Data Analytics / Continuous Controls Monitoring (CCM)

Parm Lalli, *Director*, Sunera, LLC
Professional Techniques – T22

Purpose

To help you and your organization analyze the feasibility of implementing and utilizing data analytics.

We will discuss:

- The challenges of data analytics
- The benefits of data analytics
- How to approach data analytics
- How to staff a data analytics program

Agenda

- Background
- Data Analytics Overview
- Types of Data Analytics
- Benefits of Data Analytics
- Challenges
- Applying Data Analytics
- CCM Documents Required
- Data Analytics Project Team
- Sunera Approach
- Examples

ISACA Study on CCM

- 10 Fortune 500 organizations were involved
- Identify challenges faced by organizations
- Top Data Analytics tools used
  - ACL
  - Idea
  - Arbutus
  - Tableau
- Group of 10 shared knowledge and agreed upon analytics
- 7 recommendations made

Analytic Definitions

Data Analytics (DA)	• <u>Management or Internal Audit</u> derive insight from operational, financial, and other forms of electronic data internal or external to the organization. • Insights can be historical, real-time, or predictive and can also be risk-focused (e.g., controls effectiveness, fraud, waste, abuse, policy/regulatory noncompliance).
Continuous Auditing (CA)	• Collection of audit evidence and indicators by an <u>Internal Auditor</u> on information technology (IT) systems, processes, transactions, and controls on a frequent repeatable, and sustainable basis.
Continuous Control Monitoring (CCM)	• Feedback mechanism used by <u>Management</u> to ensure that controls operate as designed and transactions are processed as prescribed. This monitoring method is the responsibility of Management and can form an important element of the internal control environment.

Data Analytic Opportunities

Reports / Summaries / Process Improvement:
Summarizes the data for planning, reconciliation or sample selection.
Examples: Vendor Spend, Accounts Payable by Business Unit

Control Based:
Clearly defined objectives that are more fact-based / black & white than the fraud & error based testing.
Examples: User Access, Employee Terminated in HR but Active in SAP, Authorization Limits

Fraud / Error Based:
Use fuzzy matching and advanced logic to identify potential fraud or errors or identify potential cash recoveries.
Examples: Duplicate Payments , Duplicate Expense Claims, T&E

Predictive / Forecasting:
Uses advanced algorithms to use inputs provided by the user to predict future events. Accounts for changes in weather and other special events that may have skewed comparative period results.
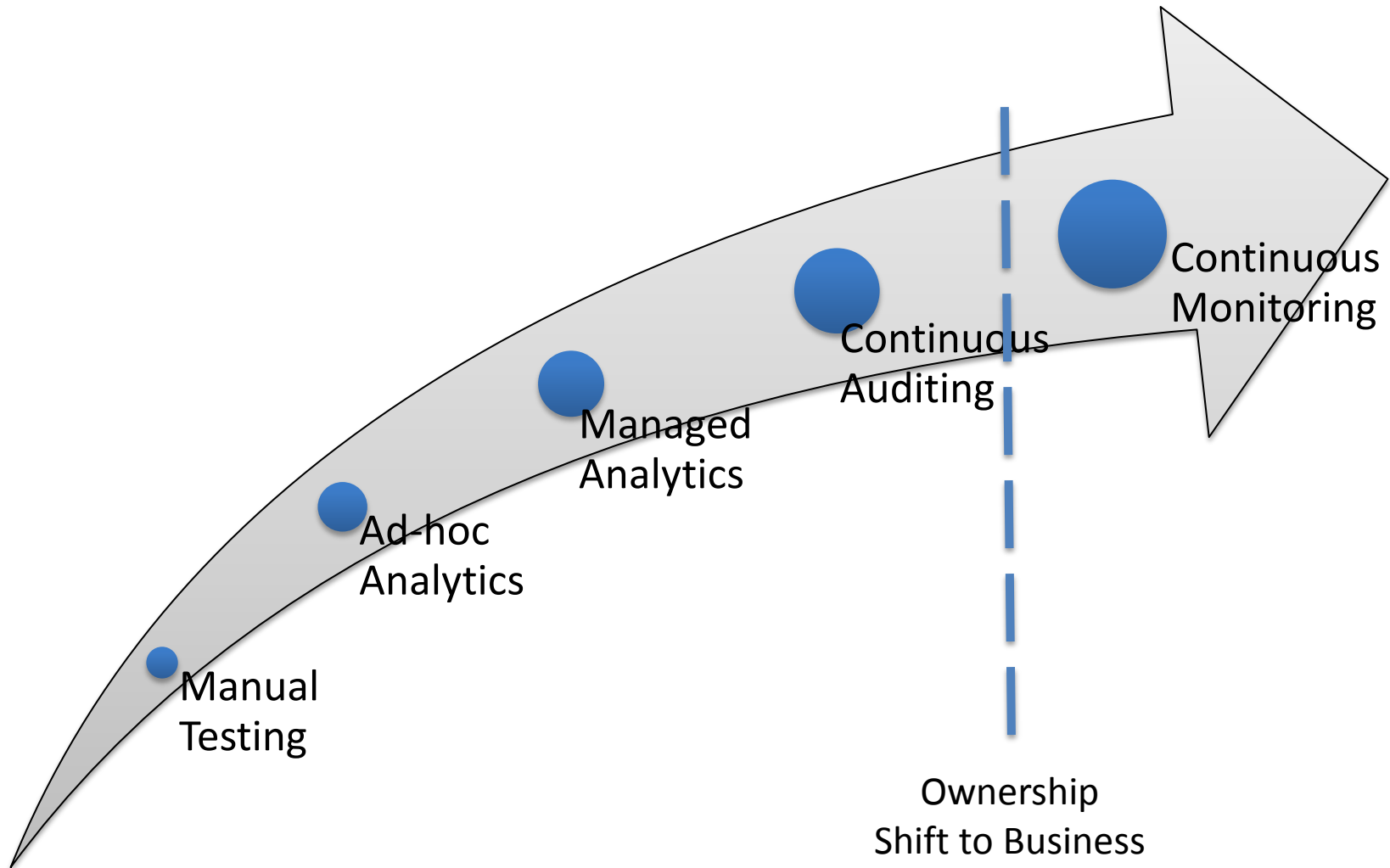**Examples:** Sales Trends

A Mature Data Analytics Overview

- Self-contained on dedicated server

- Fully automated and scheduled

- Alerts to business unit managers or stakeholders of results

- Clear and concise documentation
  - For all scripted analytics
  - For setup and configuration

A Mature Data Analytics Overview (cont.)

- Training provided to any and all individuals involved, including new hires

- Ongoing review of existing analytics and possible new analytics based on new business processes

- Maintain a change log for any addition or removal of scripts or changes to configuration

Data Analytics Lifecycle

Manual Testing

Ad-hoc Analytics

Managed Analytics

Continuous Auditing

Continuous Monitoring

Ownership Shift to Business

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Critical Success Factors

- Business buy-in

- IA Executive Management support

- Analytic optimization
  - Minimize false positives for quicker buy-in
  - Quick wins – Low hanging fruit

- Data identification & access

- Coordination with existing analytic efforts going on in the business
  - Work together and eliminate redundancy

Common CCM Tools

A number of tools are available. The right choice will depend on each company's business requirements and will include how well the proposed tool will integrate with existing systems and tools.

- ACL
- SAP or Oracle GRC
- Approva
- Oversight
- Actuate BIRT
- Actuate e.Reports
- Cognos 8 BI Report Studio
- Crystal Reports
- InformationBuilders WebFOCUS
- JasperServer/iReport
- Microsoft SQL Server Reporting Services
- MicroStrategy Report Services
- SAS Web Report Studio

Gartner February 2009: Critical Capabilities for Business Intelligence Reporting

Types of Data Analytics

Types of Data Analytics

- **Ad Hoc Analysis**
  - Time consuming
  - Data typically supplied by IT
  - Up to 50% more budgeted time required
  - Difficult to repeat tests if not documented
  - Exploratory type analysis

- **Repeatable Analysis**
  - More skills required than ad hoc testing
  - Pre-defined scripts created to perform same tests over and over again
  - More consistent and can be run more frequently
  - Data may be supplied, but imports are automated
  - Good documentation for the scripts/analytics

Types of Data Analytics (cont.)

- **Centralized Analysis**
  - Development, storing, and running of repeatable analytics is centralized
  - A single, powerful server is set up for the repeatable analytics
  - Data imports are all automated
  - Standards in place for developing tests and scripting
  - Source data and results are stored on server
  - Better security for data files and result files
  - Great deal of documentation on tests, scripts, data, and sample logic

- **Continuous Auditing**
  - Process of performing audit related tasks in a continuous manner
  - Continuous risk and control assessments types of testing
  - Compliance (SOX) control testing
  - Security event monitoring

Types of Data Analytics (cont.)

- Continuous Controls Monitoring (CCM)
  - Very skilled and experienced individuals are able to script and implement
  - All analytics and data imports are fully automated
  - No interaction from end users required
  - Allows for notifications to be sent to business unit managers about identified exceptions
  - May involve a web dashboard interface, workflow, remediation tracking, and heat maps
  - Better role based security for reviewing results
  - May provide management with areas for improvement with internal controls
  - A better likelihood of identifying fraudulent activity
  - Acts as a very good deterrent system

Benefits of Data Analytics

Benefits of Data Analytics

- Access data from many disparate sources
- Independent of the systems and people being audited
- 100% transaction coverage with unlimited file sizes
- Read-only data access to ensure the integrity of the data
- Audit trails are available to identify steps taken
- Scripting/batching capabilities to capture test logic (like macros)
- Very fast to run and produce results
- Easier to comply with the provisions of Section 404 of the Sarbanes-Oxley Act

Benefits of Data Analytics (cont.)

- Close control loopholes before fraud escalates
- Quantifies the impact of fraud
- Cost-effective
- Acts as a deterrent
- Can be automated for continuous monitoring
- Provides focus based on risk and probability of fraud
- Direct pointers to critical evidence
- Support for regulatory compliance
- Logs for review and evidence
- Scalability – Build on what you need
- External audit reliance

Data Analytics Automation Benefits

- Validates effectiveness of internal controls
- Identifies occurrences of potential fraud
- Identifies transactional errors
- Identifies segregation of duties violations
- Identifies process deficiencies
- Utilizes a technology driven process

Data Analytics Automation Benefits (cont.)

- Tests 100% of transactions as opposed to sampling
- Accesses data across disparate systems and geographies
- Provides prompt notification of control breakdowns
- Quantifies exposure of business risk
- Provides an auditable history of compliance tests and follow-up activities
- Enables better allocation of skilled audit/technical resources within the organization

Challenges

What Are the Challenges

- Implementing change

- Changing culture for the organization

- Defining what CCM can accomplish

- Gathering large volumes of data in multiple applications

- Understanding data and processes

- Monitoring of manual controls

- Relying on reporting

- Implementing costs

- Integrating with multiple compliance frameworks and into the existing IT environments

HOW DO YOU MAXIMIZE YOUR INVESTMENT IN CCM?

Applying Data Analytics

Where to Apply Data Analytics

What controls are eligible for automated testing?

- Electronic data is available and accessible.

- Access to data through an automated process is possible.

- Rules can be documented or captured within test logic.

- Internal controls and compliance controls are eligible.

What are the ideal conditions for automated testing?

- Large number of controls are in place.

- Large volumes of data are available.

- Multiple systems and data sources are available.

- Data is at multiple locations.

- Fraudulent activities are caught prior to a transaction reaching the end of a process.

Approach – IA Analytics

1. ## Internal discussion to identify data analytic integration points
   o   Review annual audit plan
   o   Review individual audit programs
   o   Review "Test Bank" for Standard Analytics

<Step 2-4 Determined after Step 1>

2. ## Identify & obtain data sets
   o   Understand Data Sources
   o   Validate / Reconcile Obtained Data

3. ## Perform exploratory analytics (pre-audit)
   o   Basic analytic steps to determine feasibility & benefit
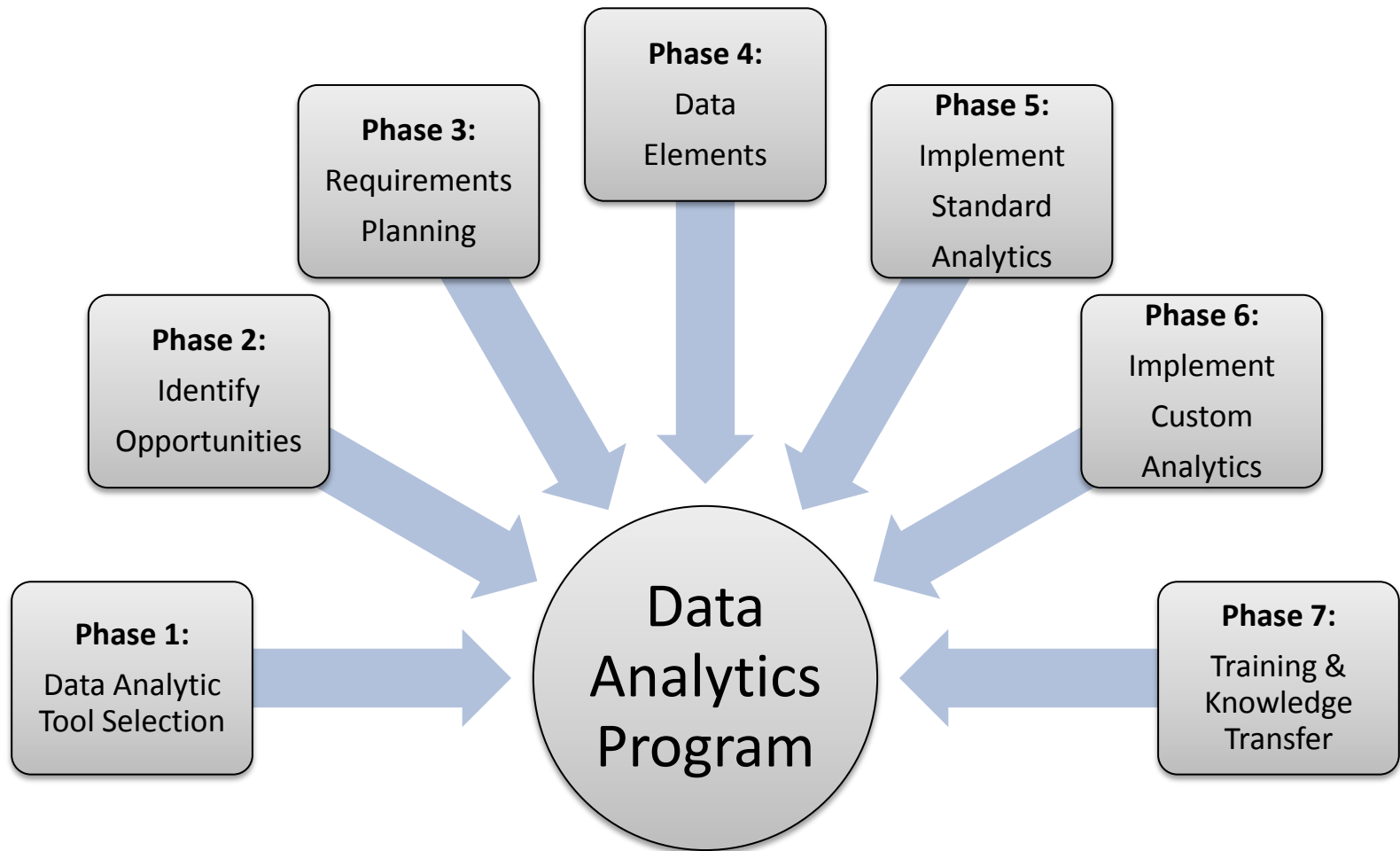
4. ## Analytic development
   o   Prepare value-add analytics for live audit

Data Analytics Steps for Mature Rollout

- **Steps for implementing continuous controls monitoring / auditing**
    1. Vendor selection and product evaluation
    2. Assess controls
    3. Scope and design system requirements
    4. Data warehouse implementation
    5. Data access requirements definition
    6. Analytics script development
    7. Results verification and review
    8. Adjusting logic, parameters, and thresholds
    9. Rollout

Data Analytics Implementation Approach

Phase 4:
Data Elements

Phase 3:
Requirements Planning

Phase 5:
Implement Standard Analytics

Phase 2:
Identify Opportunities

Phase 6:
Implement Custom Analytics

Phase 1:
Data Analytic Tool Selection

Data Analytics Program

Phase 7:
Training & Knowledge Transfer

CCM Documents Required

CCM Documents Required

- **CCM Project Checklist**
  - This document is a complete project checklist of typical CCM project tasks and responsibilities.

- **Data Analytic Tests**
  - This spreadsheet has standard analytics for many different business processes. Included are the purposes for each analytic.

- **Requirements Document**
  - This is a document that outlines the requirements to carry out a CCM initiative for a specific business process. This document includes standard tests, the purpose of each test, frequency, parameters, and source data mapping.

CCM Documents Required

- **Application Guide**
  - This document is a guide on how to use this CCM application. It includes information on how to run tests manually and change parameters. It contains information about source data and how to re-run the process in case of failure.

- **Technical Guide**
  - This document is the technical guide required by IT to rebuild the server. It contains information on how to configure the server and its related components.

Data Analytics Project Team

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

2014 Fall Conference - "Think Big"

CRISC
CGEIT
CISM
CISA

Data Analytics Project Team

- **Project Team Skills**
  - Project Manager: Managers who organize and manage all resources to complete the implementation project within the defined scope, time, and cost.
  - Business: Key owners of each business process to be monitored.
  - Audit: Process and control experts to identify areas of risk and test design.
  - IT: Key owners of the data and primary systems related to each of the processes.
  - Technical: Specialized experts to build, configure, and implement the monitoring tools.

Sunera Approach

CRISC
CGEIT
CISM
CISA

Data Analytics — Sunera Approach

- **Step 1**
  - Review existing business process risk documentation
  - Review existing analytics for efficiency and effectiveness
  - Update existing analytics for full automation

- **Step 2**
  - Conduct additional reviews of business processes and identify risk areas
  - Identify opportunities for improving process through data analytics
  - Identify analytics opportunities within specific business processes
  - Identify and verify all compensating controls

Data Analytics — Sunera Approach

- **Step 3**
  - Add risk rating for identified analytics across business units
    - High, Medium, Low
  - Quantify risk areas based on business units ($$)
  - Obtain management agreement on ratings and quantitative measures

- **Step 4**
  - Create requirements documentation
    - Data requirements from all available sources
    - Confirm test logic
    - Confirm required parameters
    - Confirm reporting fields
  - Obtain agreement and sign off on requirements document

Data Analytics — Sunera Approach

- **Step 5**
  - Obtain sample data from all required sources
    - Directly or data dump
  - Verify data based on requirements document
    - All fields present
    - No corruption of data
  - Perform data preparation

- **Step 6**
  - Create scripts for tests
  - Create Excel result sets
  - Have end user and/or business unit manager verify results
  - Tweak any tests to remove false positives

Data Analytics—Sunera Approach

- **Step 7**
  - Create scheduling for all tests
    - Daily, weekly, monthly, quarterly
  - Move all pieces into production environment
  - Verify data connections/feeds
- **Step 8**
  - Create documentation for handoff
  - Provide training to CCM stakeholders

Examples

Data Analytics Examples

Reports / Summaries

- Major Casino –
  - ➤ Pit Boss Comps
  - ➤ Credit Card Reporting Reconciliations
  - ➤ System vs Direct Report Comparison
- Global Shared Service Center – Top 10 Vendors
- CRM Data Migration – Detailed Exception Reports

Control Based

- SOX Controls – IT GCs
  - ➤ Leavers, Access Rights, System Settings
  - ➤ Segregation of Duties
- Compliance (AML, HIPAA, FCPA)
- Policy & Procedures
  - ➤ Black Car Ride Example
  - ➤ Large Fast Food Corp – T&E Audit

Fraud / Error Based

- Major Corporation - Waste & Abuse
  - ➤ Adult Entertainment – MCC Analysis
  - ➤ Double Dip – Mileage + Gas
  - ➤ Split Requisitions to circumvent appr. Limits
  - ➤ Dupe Expense (Cash + Credit)
  - ➤ Payroll to diff EE's (same bank/ address)

Predictive / Forecasting (NEW)

- NEW Hot Topic
- Rebate Estimation
- Executive Dashboard Estimates
- Recent Algorithm Developed by Sunera

Data Analytics Examples

- **Purchasing**
  - Purchase splitting
- **Purchase cards**
  - Inappropriate, unauthorized purchases
- **Travel & entertainment expenses**
  - Duplicate claims, inappropriate activity
  - Adult bars using MCC and description
- **Payroll**
  - Phantom employees
  - SSN test

Data Analytics Examples

Accounts Payable

- Questionable invoices
  - Invoices without a valid P.O.
  - Sequential invoices
  - Vendor invoice formats

- Duplicate invoices
  - Multiple invoices for same item description
  - Invoices for same amount on the same date
  - Multiple invoices for same P.O. and date

- Vendors
  - Phantom vendors
    - PO Box test
  - Vendor / employee collusion
  - One time vendors or vendors not used in over a year

Examples – Non-Industry Specific

Examples - Non-Industry Specific

Purchasing

- Questionable purchases
  - P.O. / invoices with amount paid > amount received
  - Purchases of consumer items
- Split purchases
  - Similar transactions for same vendor within specific timeframe
- Inflated prices
  - Compare prices to standard price lists or to historical prices

Examples - Non-Industry Specific

Purchase Cards

- Split purchases to avoid purchasing card limits
  - Purchases processed as two or more separate transactions
  - Identified by isolating purchases from specific vendors within short periods of time
- Favored vendors for kickbacks
  - Trend analysis to compare current transaction volumes to previous time period
- Suspicious purchases
  - Transaction that occur on weekends, holiday, or vacations
  - Travel related charges not on travel expenditure reports

Examples - Non-Industry Specific

Time and Expense

- Duplicate Claims
  - Submitting claims twice
- Tracking "no receipt" claims
  - Isolate expenses without receipts and identify underlying trends through profiling techniques
- Threshold reviews
  - Track personnel exceeding thresholds
- Inappropriate activity
  - Compare expenses to travel records to ensure expenses claimed are for valid trips
- Trends by employee compared to peers
- Fuel vs. mileage claims
  - Fuel purchase location vs. branch location

Examples - Sample Logic

Data Analytics Sample Logic

Duplicates

- Exact duplicate: All fields identical within investigation period

- Almost duplicate variance, same/different duplicates

  – Purchase Order: Same vendor and similar amount

  – Payments:

    - Different vendor, same bank account
    - Same vendor, different invoice number, similar amount
    - Same vendor, same invoice, same amount, different date
    - Same vendor name, same amount, same date, different vendor ID

Data Analytics Sample Logic

Authorization Limits

- Single and multiple accumulated values exceeding limits
- Transaction amounts that exceed or are just below the authorization limit
  - Requisitions, purchase orders invoices, payments
- Accumulated transaction amounts that exceed the authorization limit
  - Split requisitions, split purchase orders, split invoices, split payments

Aging

- Single record age
  - Days difference between create date and approval date
  - Stale requisitions, stale purchase orders, stale invoices
- Multiple files aging
  - Retroactive PO vs. invoice (invoice create date prior to PO create date)

Data Analytics Sample Logic

Data Quality

- Identifying fields where critical data elements deviate from expected values and formats.
  - Invalid ID formats, missing key values, invalid characters, invalid values
  - Requisitions, purchase orders, invoices, received goods, payments

Segregation of Duties (SOD)

- SOD security table level
  - Comparing roles within ERP security tables to a conflict matrix
- SOD at transaction level
  - Single record create / modify vs. approve
    - Requisitions, purchase orders, invoices, payments
  - Multiple files
    - Create / modify PO vs. create / modify / approve vendor master update
    - Create / modify PO vs. receive ID for goods received
    - Create / modify PO vs. create / modify invoice

Data Analytics Sample Logic

Numeric Pattern Matching

- Benford digital analysis: exceptions which reveal themselves as digital anomalies.

    - Higher than expected PO amount of $49,000, bypassing controls on amounts over $50,000

- Numeric sequence or gaps: exceptions which reveal themselves in a numeric sequence or gap.

    - Invoice number sequences (suspect invoices)

- Transactions with even dollar amounts based on a divisor number, minimum transaction count and threshold value.

    - Expense report amounts with even dollar values

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Data Analytics Sample Logic

String Pattern Matching

- Name mater (% word match)
  - Word exclusion lists to remove common words like: the, company, and, etc.
  - Invoices:
    - Employee vendor name match (phantom vendor)
    - Prohibited vendors
- Address match (numeric or alpha numeric match)
  - Match on zip / postal code plus numeric digits from address field
  - Match on alpha-numeric values from the address field (no spaces or special characters)
  - Invoices: Employee vendor address match (phantom vendor)
- Soundslike match (phonetic match)
  - SOUNDEX algorithm
  - SOUNDLIKE algorithm
  - Payroll: similar employee names
  - T&E: Different expense cards assigned to employees with similar names

Data Analytics Rollout Options

- Insource
  - Internal resources plan and deploy all CCM initiatives
- Outsource
  - External experts perform all activities required for CCM rollout
  - Provide documentation and training to client staff for maintenance of the program
- Co-source
  - External experts provide the knowledge and expertise and work with client staff
  - Shares the work of developing and creating test
  - Provides guidance
  - Performs reviews of client work conducted and provides feedback / insight
  - Conducts coaching sessions
  - Provides ongoing support and advice

Sunera & Your Speaker

CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"

About Your Speaker

Parm Lalli, CISA, ACDA

Parm is a Director with Sunera and leads the national data analytics practice. Parm has over 13 years of data analytics, audit, and controls experience with Sunera and other IT consulting firms. This experience includes leading multiple data analytics and CCM initiatives; installing, implementing, and configuring ACL Audit Exchange; and being involved in work on IT general controls, application controls, internal audit, IT risk assessment, process improvement advisory, operational audit, Sarbanes-Oxley Act (SOX), and National Instrument 52-109. Parm has also been involved in conducting vulnerability assessments and penetration testing for clients. Parm has a great deal of experience with CAAT's tools, performing data analytics, and developing Continuous Controls Monitoring applications for many different business processes. He has over 13 years experience with ACL Software. Parm is a Certified Information Systems Auditor (CISA) and ACL Certified Data Analyst (ACDA).

Parm also has over 10 years experience with Arbutus Software and implementing and configuring Arbutus for clients CCM needs. Parm was involved in a major feasibility study by ISACA on the concepts of Continuous Controls Monitoring (CCM) and what organizations need to do and/or have in place to kick of such an initiative.

Prior to joining Sunera, Parm worked in Compliance Audits, IT Risk Assessments, Vulnerability and Penetration testing, Data Analytics, and IT Audits with similar firms. Parm also worked at PwC in the Advisory group performing Revenue Assurance consultancy with the Telco Industry. Prior to that, Parm worked with ACL for over 5 years where he led Data Analytics and Continuous Controls Monitoring projects. Parm is a Certified Information Systems Auditor (CISA) and ACL Certified Data Analyst (ACDA).

Sunera Snapshot

Professional consultancy with core competency in:

- Internal Audit − IT Audit − Regulatory Compliance − PCI
- Information Security − Data Privacy − IT Strategy & Risk
- Finance & Accounting − Interim CFO/Controller − Training

Offices across the **United States** and **Canada**

The nation's largest independent provider of **technology risk consulting**

A **PCI Qualified Security Assessor** and Approved Scanning Vendor (QSA & ASV)

Certified **SAP integration partner** with specific expertise in SAP security, GRC, and controls

The only authorized **reseller of ACL** products in North America, solidifying our reputation as a market leader in Continuous Controls Monitoring

Delivered **thousands of projects** for **hundreds of organizations** across all major industries and sectors. Adept in servicing the Fortune 1000 but very adaptable to smaller organizations and government entities

Trained and **certified professionals** with appropriate oversight utilizing proven, pragmatic methodologies to ensure quality results

Solution-oriented teams that tailor projects to client needs, complementing clients' internal capabilities

Track record of projects achieving anticipated benefits, on-time, and within budget. Results driven by **rigorous project management discipline** and finance and IT capabilities

Registered with NASBA to **offer CPEs** for our external Internal Audit and ACL training courses.

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Data Analytics Training Option

Sunera Training Offers:

- **2 or 3 day training classes**
    - Training is hands-on and classes are tailored to meets your participants' skill levels (beginner, intermediate, advanced).
    - We customize the training by integrating your company's data into the seminar, so your employees get to work with realistic company scenarios.
    - Sunera is registered with the National Association of State Boards of Accountancy (NASB) as a sponsor of continuing professional education on the National Registry of CPE sponsors and offers CPE credits to those who attend and completed the training.
    - Training is provided by a Sunera Director or Principal Level Associate with multiple years and project experience using ACL.
    - We are planning on offering a training course in Calgary in October pending sufficient interest.
    - Training (classroom instruction) can be provided to organizations directly.

Contact Information

For additional information on Sunera's services, visit our website at **www.sunera.com** or contact:

Parm Lalli
Director
(949) 204-4550
plalli@sunera.com