# Increasing Forensics in the Audit
## *(and driving a bottom-line benefit)*

Patrick J D Taylor
CEO, Oversight Systems

Tuesday March 18, 2008

Find it. Fix it. Prove it.
Oversight™

# Agenda

- Impetus for Fraud Monitoring

- Pervasive Architecture

- Persistent and Advanced Data Analytics

- Program Management: Case Management and Compliance Work Flow

- Performance: Enterprise Dashboard

- Policies for Reporting and Compliance Evidence

# 3 Keys for Fraud Monitoring

1. Analyze

2. Resolve

3. Document

# PCAOB:
# "Improve Fraud Detection"

▸ January 2007 PCAOB report, "Observations on Auditors' Implementation of PCAOB Standard Relating to Auditors' Responsibility with Respect to Fraud"

  ◦ Management override of control is cited as an area of risk that should be more proactively addressed by audit firms

  ◦ Forensic in the audit is recommended to decrease risk of fraudulent financial reporting

# Investors want "Cooking Controls"

○ "While much of the commentary about control reporting has been concerned with compliance costs, evidence suggests that important goals of reporting on controls are not being fully achieved:
**a) There appears to be insufficient emphasis on controls that prevent senior management from fraudulently manipulating financial reporting (cooking controls)."**

Find it. Fix it. Prove it.

Oversight ™

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

# SEC: "ICFR is Insufficient"

- "ICFR also can be circumvented by collusion or *improper management override*. Because of such limitations, *ICFR cannot prevent* or detect all misstatements, whether **intentional** *errors or fraud*. …it is *possible to design into the process safeguards* to reduce, though not eliminate, this risk."

Find it. Fix it. Prove it.

Oversight ™

ISACA®
Serving IT Governance Professionals
*San Francisco Chapter*

# PCAOB – Audit Standard 5

- Focus on a top-down, risk-based approach to compliance and specifically fraud risk in General Ledger
  - Controls over journal entries
  - Period-end adjustments
  - Significant or unusual transactions
- Auditors may use management's monitoring activities as evidence
  - Competence
  - Completeness
  - Documentation

# COSO Controls Framework



- Identifies control failures and management override of controls
- Properly remediated exceptions are an effective control
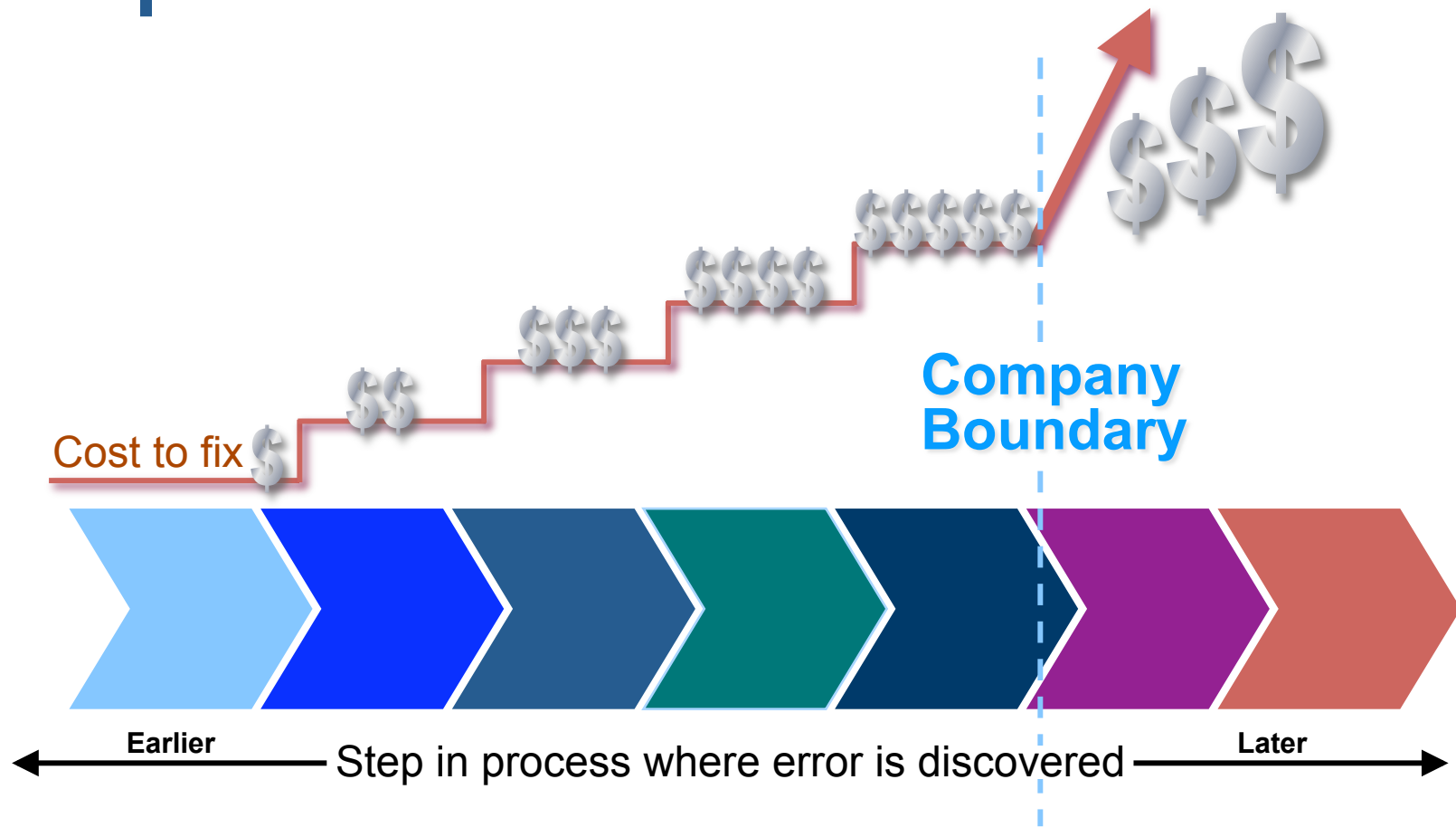- The only "Cooking Control"
- Benefits beyond compliance

# Continuous Auditing is Coming

▶ "By 2010, auditors will expect regulated organizations to detect fraud by performing transaction monitoring on a continuous basis, and 60% of regulated firms will have such an automated process in place (0.8 probability)."
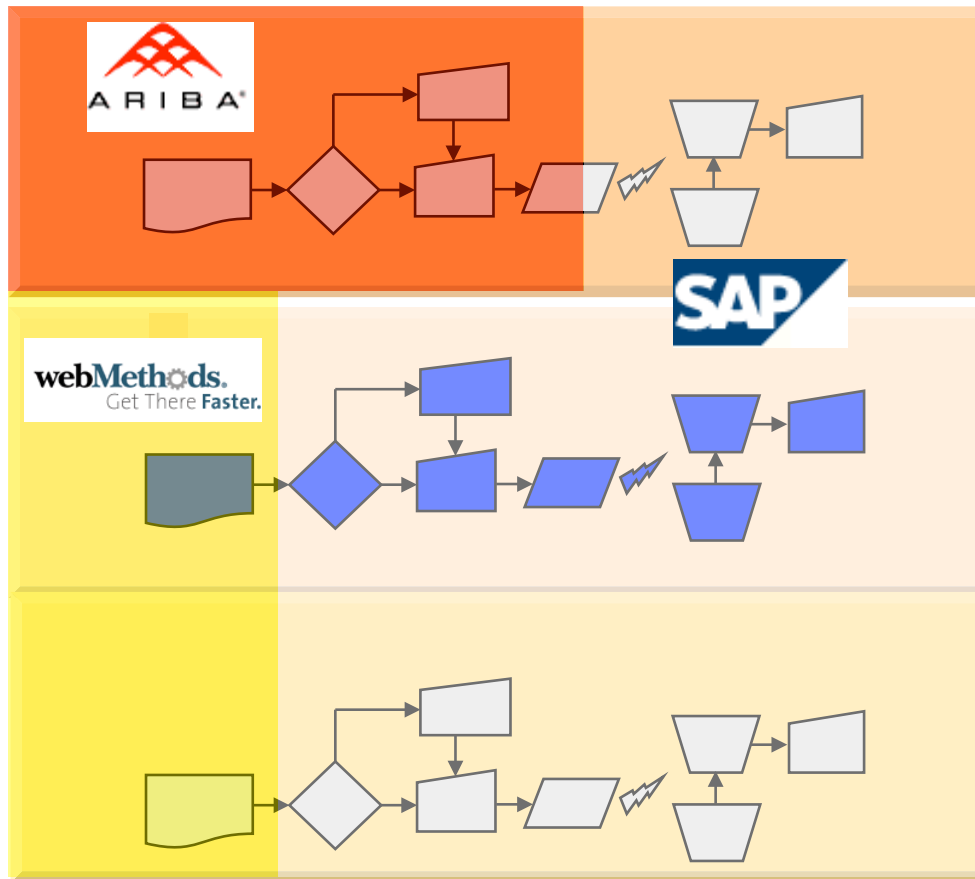
– Gartner
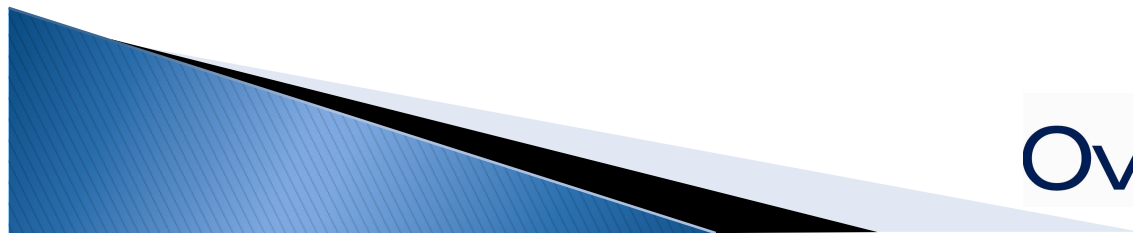
# Agenda

▸ Impetus for Fraud Monitoring

▸ **Pervasive Architecture**

▸ Persistent and Advanced Data Analytics

▸ Program Management: Case Management and Compliance Work Flow

▸ Performance: Enterprise Dashboard

▸ Policies for Reporting and Compliance Evidence

Find it. Fix it. Prove it.

Oversight ™

ISACA®
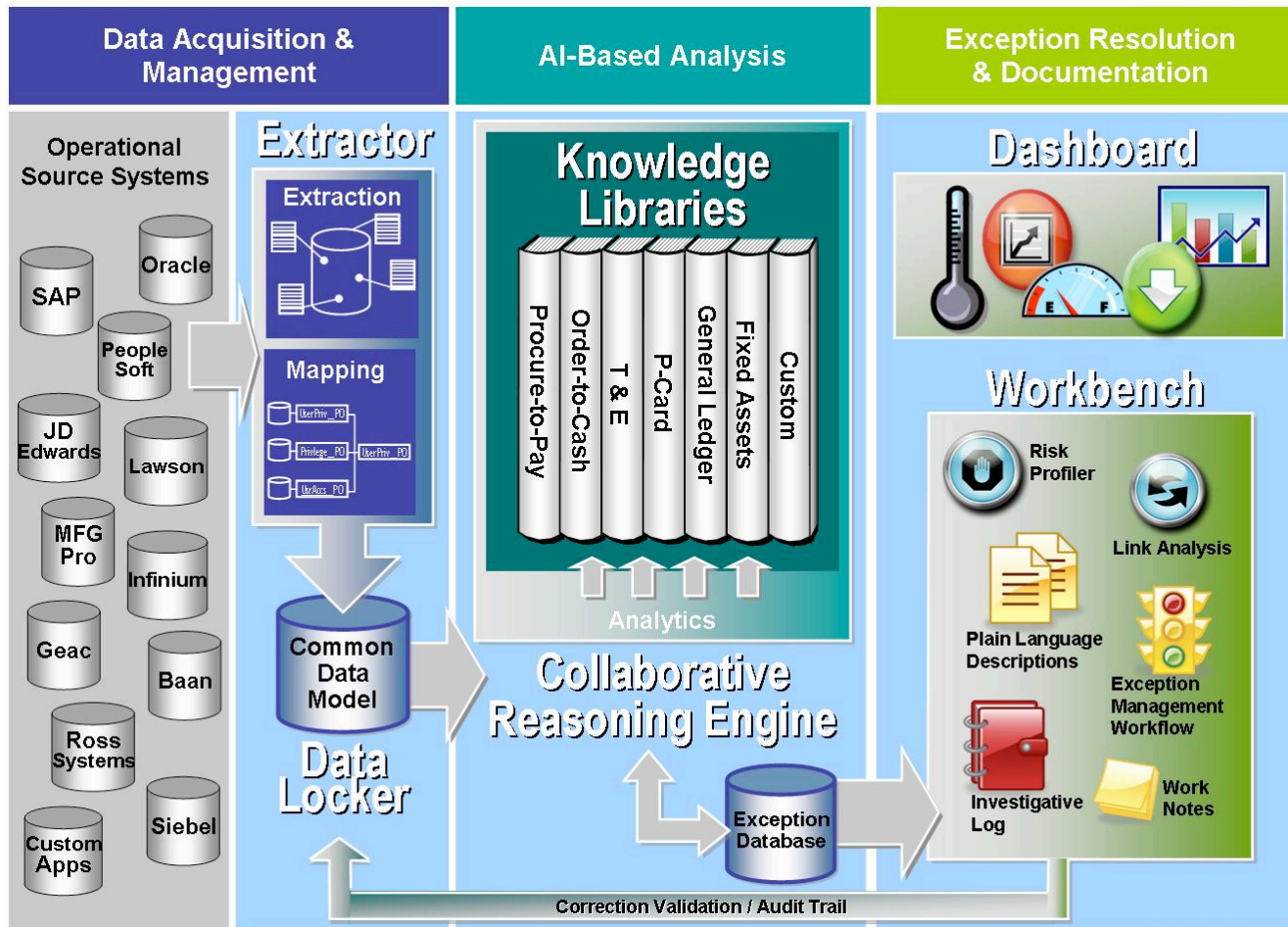Serving IT Governance Professionals
*San Francisco Chapter*

# Multi–application Solution Stack



The average $1B company has:
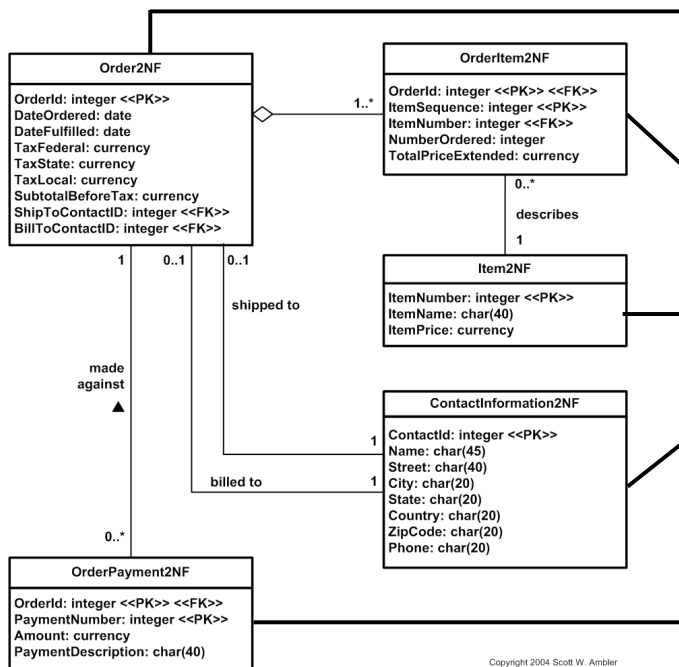
- 2.7 ERP Systems

- 40+ financial apps

# Pervasive Architecture

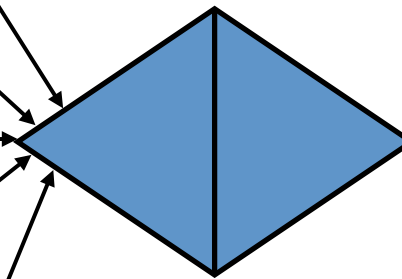# Organize and Store Data in a Business View

## ERP Data Model



**Order2NF**

OrderId: integer <<PK>>
DateOrdered: date
DateFulfilled: date
TaxFederal: currency
TaxState: currency
TaxLocal: currency
SubtotalBeforeTax: currency
ShipToContactID: integer <<FK>>
BillToContactID: integer <<FK>>

**OrderItem2NF**

OrderId: integer <<PK>> <<FK>>
ItemSequence: integer <<PK>>
ItemNumber: integer <<FK>>
NumberOrdered: integer
TotalPriceExtended: currency

**Item2NF**

ItemNumber: integer <<PK>>
ItemName: char(40)
ItemPrice: currency

**ContactInformation2NF**

ContactId: integer <<PK>>
Name: char(45)
Street: char(40)
City: char(20)
State: char(20)
Country: char(20)
ZipCode: char(20)
Phone: char(20)

**OrderPayment2NF**

OrderId: integer <<PK>> <<FK>>
PaymentNumber: integer <<PK>>
Amount: currency
PaymentDescription: char(40)

1..*
0..*
describes
1
shipped to
made against
billed to
1
1
1
0..1
0..1
0..*

Copyright 2004 Scott W. Ambler

## Business Entity Model
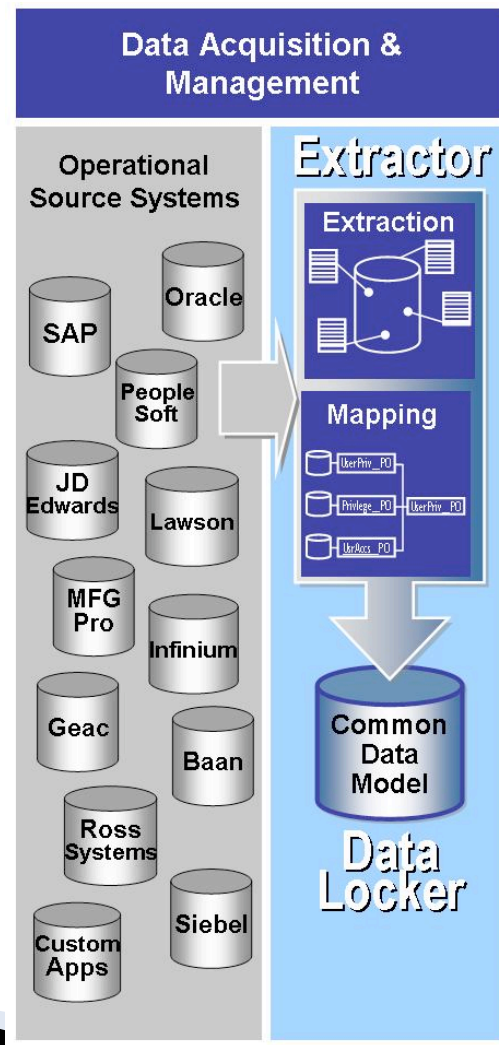
# Audit Data Warehouse: Key Step for Fighting Fraud

- Data mapping is addressed through common data models
  - Center for Audit Quality (www.thecaq.com):
    Common Data Model for General Ledger
  - XBRL-GL
- Audit Data Warehouses
  - Single repository to record transaction history
    - Available for management, internal audit and external auditors
  - Leverage heterogeneous data acquisition and mapping – design analytics for business process issues without being limited by applications
- Key Fraud Fighting Capabilities
  - Extraction logging and control totals for information integrity
  - Highly secure with independence from IT infrastructure
  - Revision history to provide evidence of concealment

Find it. Fix it. Prove it.

Oversight™

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

# Keys for a Flexible Audit Data Warehouse



- ▸ Avoid software installation on application servers (ABAP program required for SAP to get accurate extractions)

- ▸ Data extracted by precisely-crafted read requests; performance impact <one user

- ▸ Mappings to source systems in XML files for fast implementations and easy maintenance

# Agenda

▸ Impetus for Fraud Monitoring

▸ Pervasive Architecture

▸ **Persistent and Advanced Data Analytics**

▸ Program Management: Case Management and Compliance Work Flow

▸ Performance: Enterprise Dashboard

▸ Policies for Reporting and Compliance Evidence

# Simple Duplicates are Easy

▸ Most financial applications stop identical documents

# Finding the Real Problems is Harder

▸ **Symbolic Reasoning – analysis at the document level**
  ◦ The Order numbers are similar; Line item details match; Order dates are close

# GL Fraud: 33% of SEC Actions

- Cooking the Books
  - 1/3 of all SEC enforcement fraud schemes involve manipulation of financial statement items – Deloitte Forensic Center
  - Means ICFR have been failed
    - Manipulation of Assets
    - Manipulation of Expenses
    - Manipulation of Reserves
    - Manipulation of Liabilities

# Finding the Unusual Journal Entries

▸ Risk represented by a combination of attributes
  ◦ Time of day, week and month
  ◦ Large dollar adjustments in one transaction or accumulated in many transactions
  ◦ Isolated in one account or accumulated across accounts
▸ Evaluated according to each user's
  ◦ Activity compared to normal vouchering participation
  ◦ Timing and frequency of entries
▸ Journal Vouchers – the Devil is in the Details
  ◦ Needles in a haystack

# Business Benefit

- Error identification falls out of the analysis
  - Inappropriate end states for accounts
  - Basic debit/credit typos
- Early identification of problematical trends
- Simplifies the process for closing the books

# Scru Chains

| | Debit | Credit |
|---|---|---|
| Sales | | $100 |
| AR | $100 | |
| Cash | $100 | |
| AR | | $100 |
| AP | $100 | |
| Cash | | $100 |
| AP | | $100 |
| PPE | $100 | |

# The Fraud Unfolds

|        | Debit  | Credit |
|--------|--------|--------|
| Sales  |        | $100   |
| AR     | $1X0   |        |
| Cash   | $100   |        |
| AR     |        | $1X0   |
| AP     | $100   |        |
| Cash   |        | $100   |
| AP     |        | $100   |
| PPE    | $100   |        |

# The Fraud Unfolds

| | Debit | Credit |
|---|---|---|
| Sales | | $100 |
| AR | $~~1~~00 | |
| Cash | $~~1~~00 | |
| AR | | $1~~0~~0 |
| AP | $100 | |
| Cash | | $1~~0~~0 |
| AP | | $100 |
| PPE | $100 | |

Find it. Fix it. Prove it. ™

Oversight

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

# The Fraud Unfolds

|  | Debit | Credit |
|---|---|---|
| Sales | | $100 |
| AR | $~~X~~00 | |
| Cash | $~~X~~00 | |
| AR | | $1~~X~~0 |
| AP | $~~X~~00 | |
| Cash | | $1~~X~~0 |
| AP | | $1~~X~~0 |
| PPE | $100 | |

# Disguising the Path

| | Debit | Credit |
|---|---|---|
| Sales | | $100 |
| AR | $60 $40 | |
| Cash | $70 $30 | |
| AR | | $50 $50 |
| AP | $90 $10 | |
| Cash | | $45 $55 |
| AP | | $100 |
| PPE | $20 $80 | |

# Disguising the Path

|  | Debit | Credit |
|---|---|---|
| Sales | | $100 |
| AR | ~~$60~~ $40 | |
| Cash | ~~$70~~ $30 | |
| AR | | ~~$50~~ $50 |
| AP | ~~$90~~ $10 | |
| Cash | | ~~$45~~ $55 |
| AP | $20 | ~~$100~~ |
| PPE | $80 | |

# Fraud Chain Analytics

- Challenging search problem
  - Sales/AR to AR/Cash to Cash/AP to AP/PPE equals 4 links
    - A "real" chart of accounts could support much longer chains
  - The number of parallel links geometrically expands the search space
    - 70+30 = 2 parallel links
    - 30+30+40 = 3 parallel links
- Compute and compute some more

# Revenue Recognition Fraud

- 41% of all SEC enforcement fraud schemes (Source: Deloitte)
  - 35% Fictitious revenue
  - 16% Swaps, round tripping or barters
  - 12% Transactions not shipped
  - 12% Contingencies
  - 13% Inappropriate reserves
  - 12% Incomplete delivery

# Finding the Unusual Revenue

- Fictitious and overstated revenue
  - Anomalies in the revenue recognition details
    - Shipments processed against invalid/incomplete sales orders
    - Invoices inconsistent with shipment documents
    - Intra-divisional transfers booked as sales
- Identify patterns of revenue transactions for review
  - Patterns of cross period bookings and returns
  - Channel stuffing

# Business Benefits

- Preventing Lost Revenue
  - Unearned discounts taken by (or given to) customers
  - Trade allowance gaming
- Customer satisfaction
  - Incorrect shipments – costly in $ and reputation
  - AR days sales outstanding (DSO) reduction

# Defining the Usual & Unusual

▸ Structural & Knowledge Based Approaches
  ◦ Critical fields are malformed or missing
  ◦ Apparent duplications
  ◦ Second-order anomalies (e.g. JE compared to sales order)

▸ Statistical Approaches
  ◦ Numerical outliers
  ◦ Timing and frequency anomalies
  ◦ Discrete valued outliers
  ◦ Combinations of above

▸ Similarity Comparisons
  ◦ Account numbers – 123456 resembles 1230456

# Transaction Monitoring –
# What Drives the Cost?

- The quantity of exceptions
  - True positives generate an ROI
  - False positives are an obvious cost
  - Repeat positives are a hidden cost
    - Analysis over a 30 day window once per day can identify the same exception (true or false) 30 times
- Effort per exception
  - Interpreting the reasons why
  - Evaluating related information in order to adjudicate
  - Assigning for correction
  - Validating the correction
  - Documenting the reconciliation

# False Positives can Choke Continuous Monitoring

▸ Temporal Reasoning: transaction relationships thru time

◦ Recurring is part of a pattern
◦ Similar amount
◦ Same vendors

**Jan 1** **Feb 2** **Mar 1** **Apr 4** **May 2** **Apr 3** **May 1**

Find it. Fix it. Prove it.

**Oversight**

**ISACA®**
Serving IT Governance Professionals
*San Francisco Chapter*

# Journal Entry Valid

**New Manual Journal Entry** → **JE Valid**

- Name Present
- JE Acctg Period Valid
- JE Trans Source Present
- JE Over Limit
- JE Split
- JE Currency Present
- JE Trans Type Present
- JE Descript Present
- JE Balanced
- JE SoD

→ **Conclusion**

# Integrity Checks vs Tests
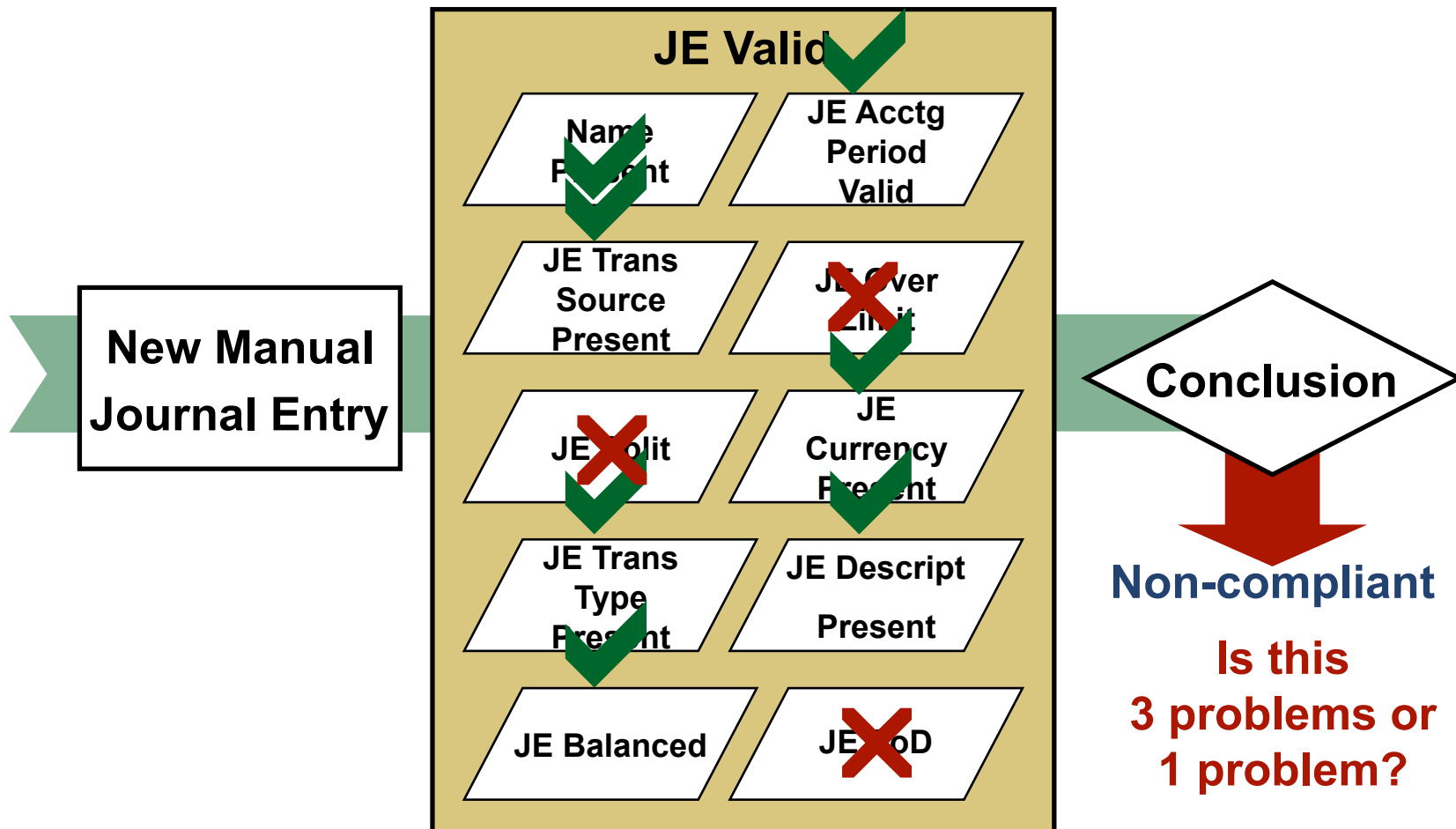


New Manual Journal Entry

JE Valid

- Name Present
- JE Acctg Period Valid
- JE Trans Source Present
- JE Over Limit
- JE Split
- JE Currency Present
- JE Trans Type Present
- JE Descript Present
- JE Balanced
- JE CoD

Conclusion

Non-compliant

Is this
3 problems or
1 problem?

Find it. Fix it. Prove it.

Oversight™

ISACA®
Serving IT Governance Professionals
San Francisco Chapter
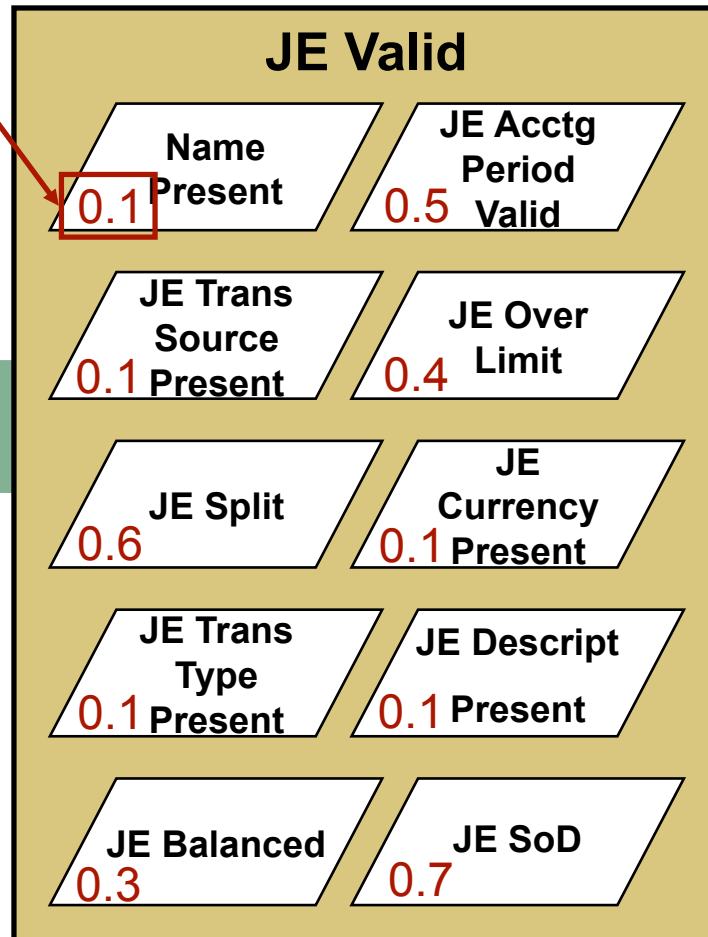
# Fraud Scoring

# Fraud Scoring



New Manual Journal Entry

JE Valid

| | |
|---|---|
| Name Present 0.1 | JE Acctg Period Valid 0.5 |
| JE Trans Source Present 0.1 | JE Over Limit 0.4 |
| JE Split 0.6 | JE Currency Present 0.1 |
| JE Trans Type Present 0.1 | JE Descript Present 0.1 |
| JE Balanced 0.3 | JE FoD 0.7 |
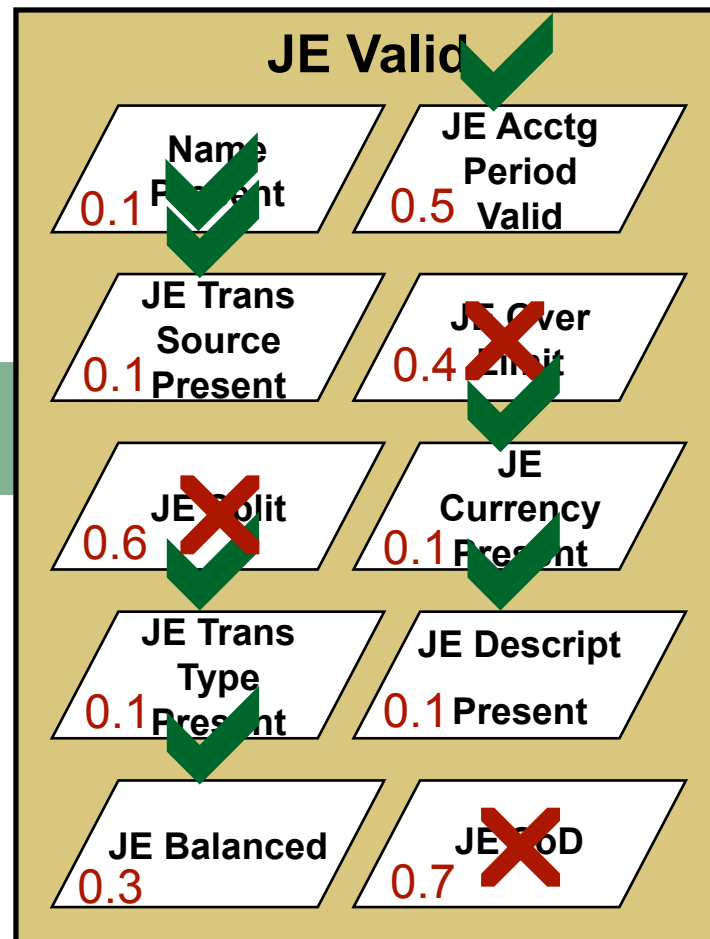
Conclusion

**92.8% confidence of 1 non-compliant transaction**

# Eliminate Duplicate Payments and Rework

- Invalid Vendor
- Duplicate Vendor
- Ghost Vendor
- Vendor Change Change-back
- Vendor Maint SOD

- Receipt/PO SOD

- Payment for 0
- Payment without Voucher
- Payment Payee differs from Vendor
- Payment to Ghost Vendor
- Payment to Employee
- Payment Detail Mismatch
- Payment/PO SOD

- Payment Duplicate
- Payment Line Duplicate
- Payment Line Exceed Voucher
- Payment Line Without Voucher
- Payment Line/Voucher Mismatch
- Payment Line for Duplicate Voucher
- Payment/Voucher SOD

Vendor Maintenance → Requisition → PO → Goods Receiving → Invoice Voucher → Payment → Recovery

- Invalid PO
- PO to Inactive Vendor
- PO to Invalid Vendor
- PO to Ghost Vendor
- Duplicate PO
- PO/Vendor SOD

- Invalid Voucher
- Voucher for 0
- Voucher to Invalid Vendor
- Voucher to Duplicate PO
- Voucher Duplicate Amount
- Voucher Duplicate Invoice
- Voucher/PO SOD

Find it. Fix it. Prove it.
Oversight �N ™

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

# Revenue Recognition

- Invalid Customer
- Duplicate Customer
- Ghost Customer
- Customer Change Change-back
- Customer Credit Invalid
- Customer Credit to Invalid Customer

- Invalid Shipment
- Shipment Differs From Customer
- Shipment Changed After Invoice
- Shipment Line Order Line Mismatch

- Cash Receipt Invalid
- Cash receipt From Invalid Customer
- Cash Receipt From Invalid or Nonexistent Customer
- Cash receipt w/o Cash Application
- Duplicate Cash receipt

Customer Maintenance → Sales Order → Order Fullfillment → Invoices Credit → Cash Receipts → Cash Applications → RMA → Return Receipts

- Invalid Sales Order
- Sales Order to Inactive Customer
- Sales Order to Invalid Customer
- Sales Order to Ghost Customer
- Duplicate Sales Order
- Order SOD
- Sales Order to Inactive Customer

- Invalid Invoice
- Invoice to Invalid or Nonexistent Customer
- Duplicate Invoice
- Invoice w/o Order
- Return Credit Duplicate
- Return Credit Invoice Mismatch

- Cash Application to Invalid Customer
- Cash Application to Invalid or Nonexistent Customer
- Duplicate Cash Application
- Cash Application Invoice Mismatch
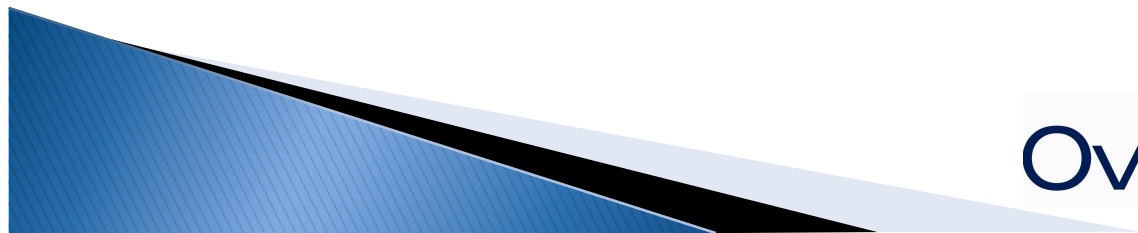
# GL Fraud Checks

## Financial Accounting and Reporting

- Journal Entry Invalid
- Journal Entry Unsupported
- Journal Entry Empty
- Journal Entry Unbalanced
- Journal Entry Over Limit
- Duplicate Journal Entry

- Chart of Accounts Account Invalid
- Chart of Accounts Contra Account
- Chart of Accounts Account Duplicate
- Chart of Accounts Change Changeback
- Calendar Reopened and Closed

Automated Journal Entries → Create Manual Journal Entries → Approve Journal Entries → Post to General Ledger → Review Trial Balance → Reconcile Accounts → Close Accounting Period

- Journal Entry SoD
- Journal Entry Override
- Chart of Accounts Override
- Scru Chains

# Keys to Precisely Identify Problems
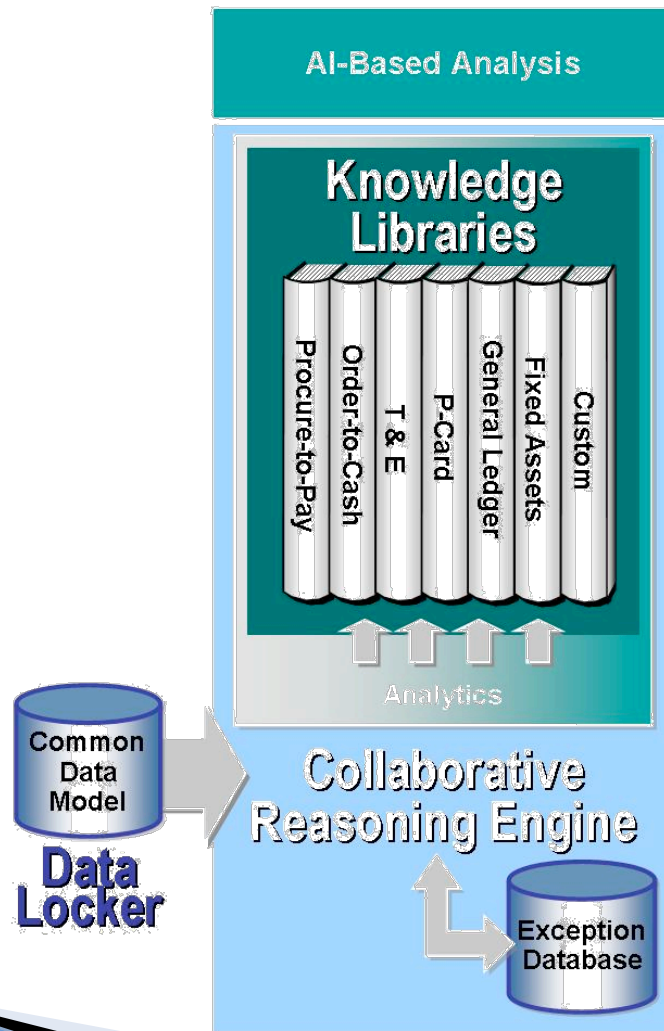


- Intelligent test compilation and scoring
- AI capabilities replicate human reasoning – unusual, similar, usual
- Analytics against an audit data warehouse are reusable across applications
- Leverage data sophisticated analytics across the business

# Agenda

- Impetus for Fraud Monitoring
- Pervasive Architecture
- Persistent and Advanced Data Analytics
- **Program Management: Case Management and Compliance Work Flow**
- Performance: Enterprise Dashboard
- Policies for Reporting and Compliance Evidence

Find it. Fix it. Prove it.

Oversight

ISACA®
Serving IT Governance Professionals
*San Francisco Chapter*

# Resolution: More than Reports



**Manual Resolution Process** **vs.** **Case Management Integrated with Continuous Auditing**

Manual Resolution Process:
- Review original report of exception…
- …identify & locate related documents
- …compare to data in individual spreadsheets
- …search customer database to validate information
- …pull reports from ERP System
- …keep detailed notes to document resolution for external audit

Case Management chart:
- Y-axis: Operations Resolution Effort / Exceptions Under Investigation
- X-axis: Elapsed Time — 1 week, 2 weeks, 3 weeks, 4 weeks
- Internal Audit oversight

Find it. Fix it. Prove it.
Oversight ™
ISACA® Serving IT Governance Professionals
San Francisco Chapter

# Elements of Efficient Resolution

▸ List of exceptions prioritized by risk
▸ Plain-language descriptions of why flagged as exception
▸ Supporting data displayed with exception, to facilitate investigation

# Prioritizing the Exceptions

▸ Calculate an aggregate confidence with Bayes Theorem

▸ Establish a priority by combining confidence and dollar value

  ◦ $1,000 exception with 90% confidence
      =  $900 priority

  ◦ $1,000,000 exception with 50% confidence
      = $500,000 priority

# Example of Plain Language Descriptions

▶ Journal Entry was created by user JMILLER that has never posted to account *1843 –Accumulated Depreciation*

▶ Journal Entry was created by user JMILLER that has never posted to account *5382 –Depreciation Expense*

▶ Journal Entry is a manual entry

▶ Manual Journal Entry posted to account *1843–Accumulated Depreciation* that typically has automated or systematic entries

# Workflow Drives Resolution

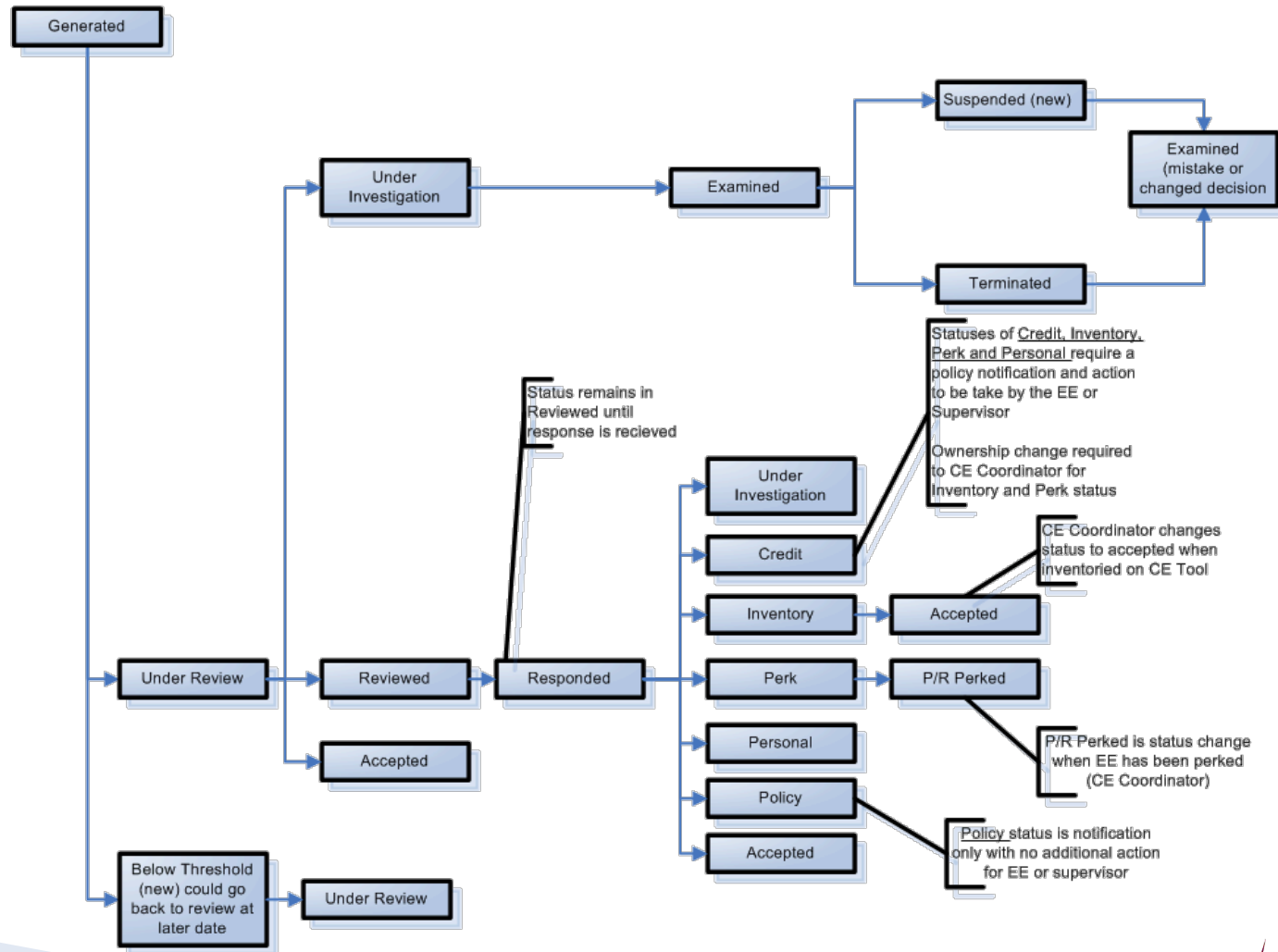| New | In Process | | Resolved |
|-----|------------|--|----------|
| | | | **Closed Conditions** |
| **Detected** | **Assigned For Review** → **Under Investigation** | | **Corrected** |
| | **Escalation** | | Correction Valid / Correction Invalid |

Single discovery of an exception (no repeats)

Configurable assignments and resolution states with an enforced workflow. Management alerts on exception status and backlogs

End state tracking for correction validation and root cause analysis

# Representative Workflow

# Exception Workflow Status

▸ Maintained with Exception description & supporting information

▸ Shows owner

▸ Reflects current status, i.e., "Review Completed"

▸ Stores notes supporting resolution status

# Agenda

▸ Impetus for Fraud Monitoring

▸ Pervasive Architecture

▸ Persistent and Advanced Data Analytics

▸ Program Management: Case Management and Compliance Work Flow

▸ **Performance: Enterprise Dashboard**

▸ Policies for Reporting and Compliance Evidence

Find it. Fix it. Prove it.

Oversight

ISACA®
Serving IT Governance Professionals
*San Francisco Chapter*

# Risk–Based Dashboard Views

- At–a–glance management tool
- Reveals backlogs
- Tracks error rates
- Identifies exception trends by user, department, account, amount, etc.
- Use relevant information to drive resolution
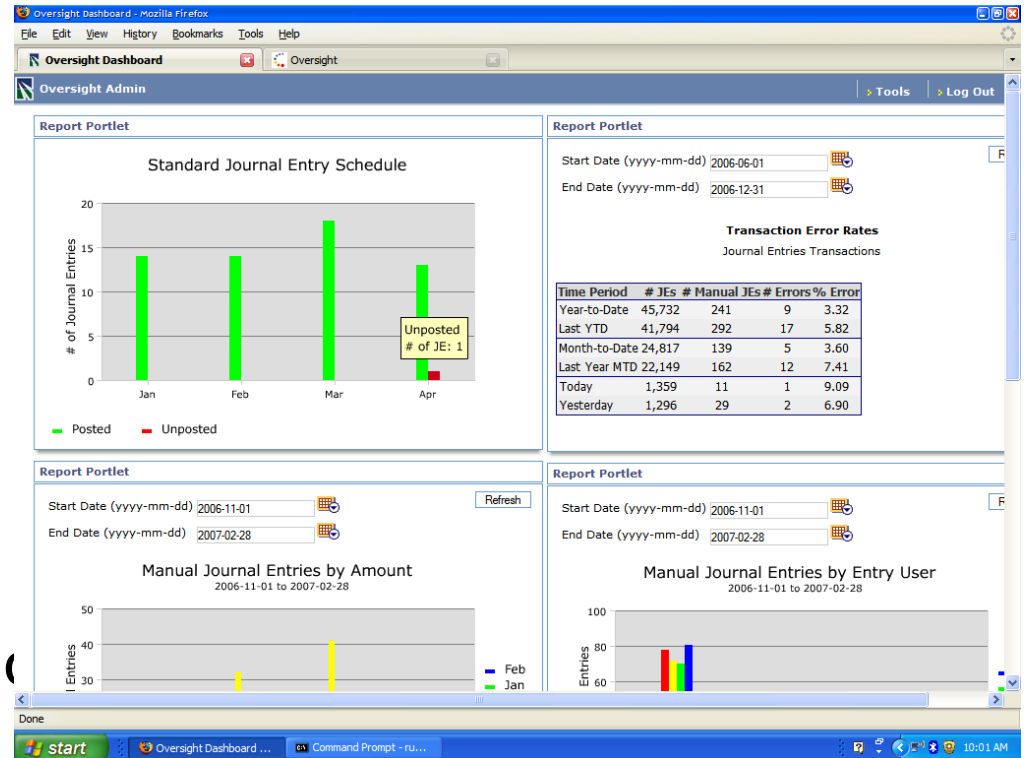
# Exception Handling Management

- Drive exception resolution through a defined process
  - Resolve each issue once and only once
  - Automatically assign to specific users/roles
  - Stages and states of process are configurable
  - Enforce mandatory process flow
- Alerts for exception handling process
  - Excessive backlog based on volume
  - Resolution that exceed time limits
  - Correction Detection validates that changes were made in the source system(s)
- Prove resolution
  - All resolution activities are permanently recorded in a secure journal
  - Reports on exceptions by
    - Error types; Person(s) handling; and Resolution state

# Agenda

▸ Impetus for Fraud Monitoring

▸ Pervasive Architecture

▸ Persistent and Advanced Data Analytics

▸ Program Management: Case Management and Compliance Work Flow

▸ Performance: Enterprise Dashboard

▸ **Policies for Reporting and Compliance Evidence**

# Prove It with a Secure Journal

▸ Journal automatically tracks and associates with exception:
  ◦ Exception ownership/assignment
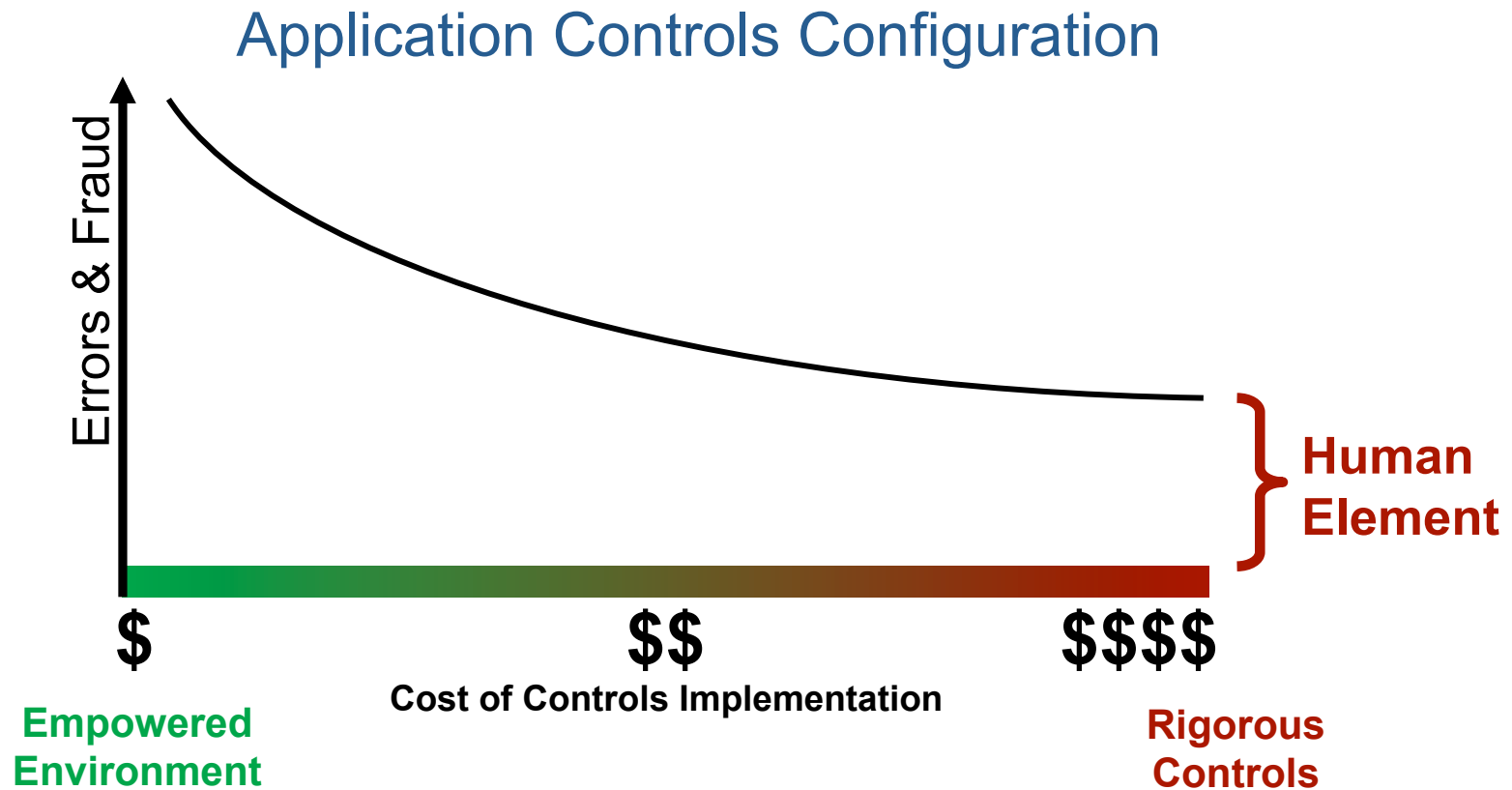  ◦ State changes
  ◦ Notes
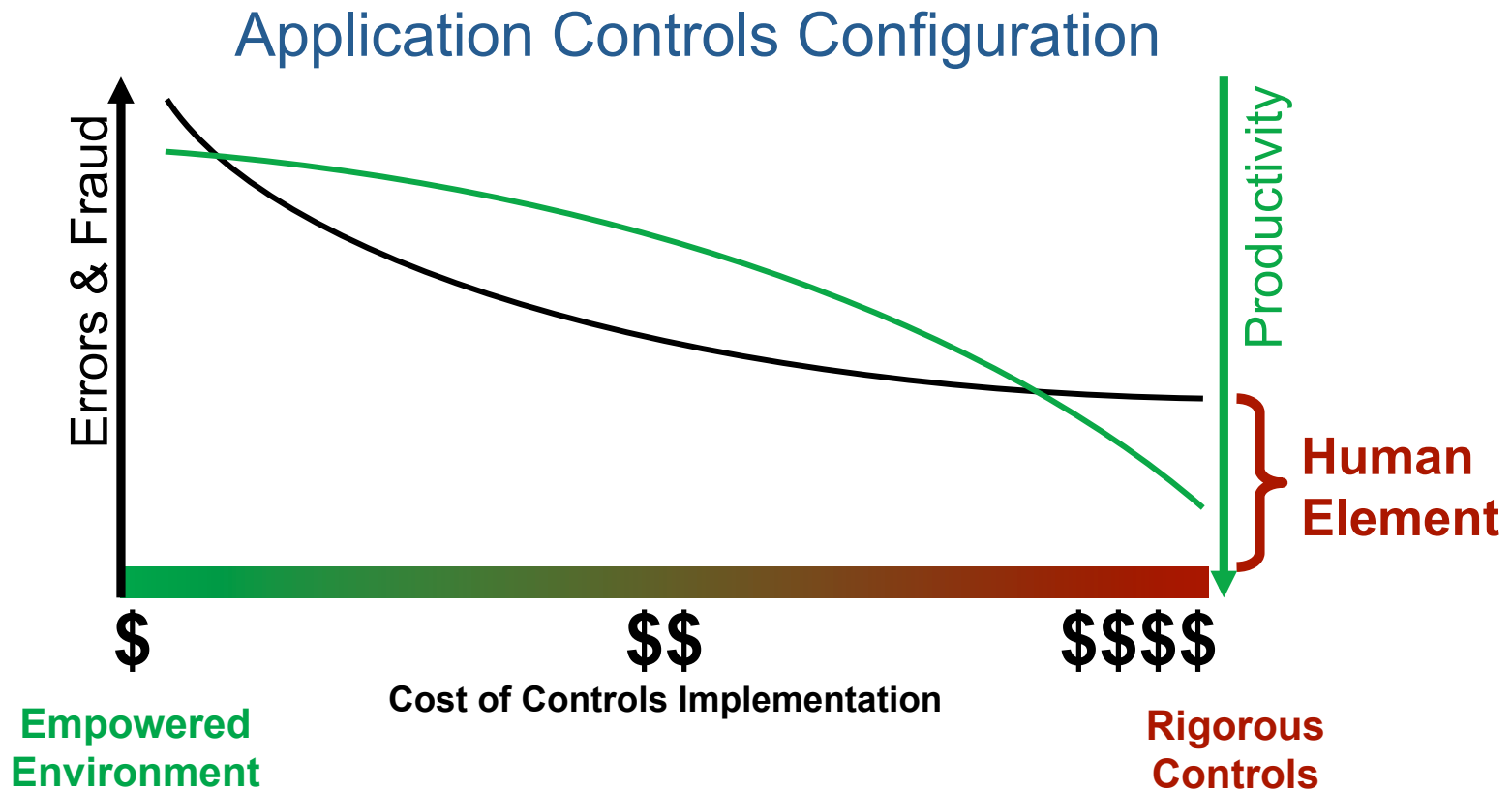▸ Provides secure permanent storage

# Keys to Efficient Resolution
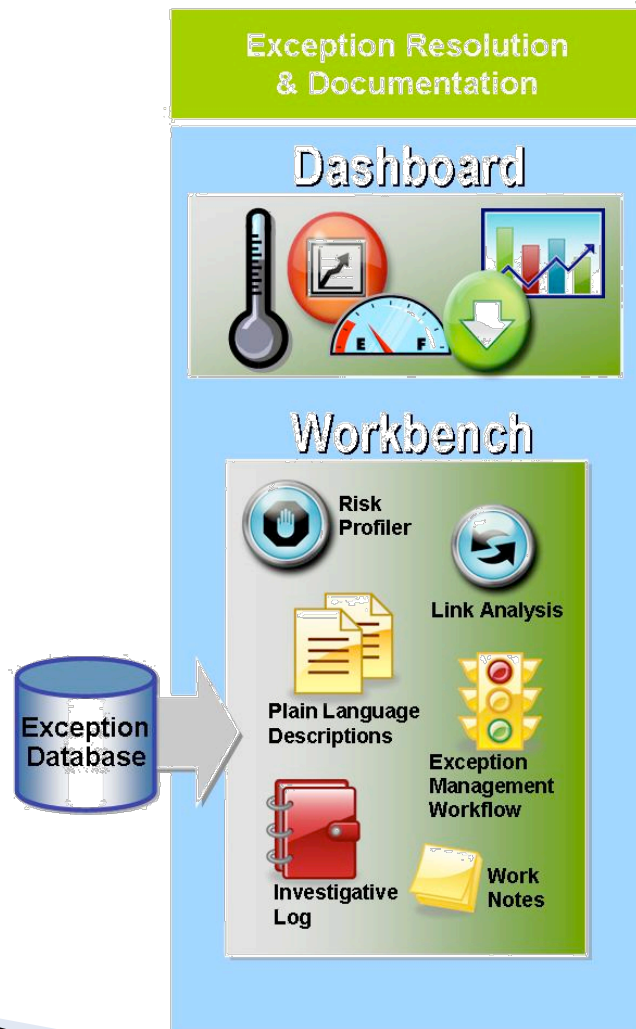


- Dashboard – management level view of compliance and facilitates root cause analysis
- Workbench supports efficient investigation of exceptions
- State model records a single instance of each exception
- Comprehensive workflow drives a process
- Permanent journal records all activity to "prove" exceptions were resolved
- Corrections are validated against the source applications

Find it. Fix it. Prove it.
Oversight ™

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

# Controls and Error/Fraud Prevention

## Application Controls Configuration



Errors & Fraud (y-axis)

Cost of Controls Implementation (x-axis)

$  $$  $$$$

Empowered Environment

Rigorous Controls

Human Element

Find it. Fix it. Prove it.

Oversight

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

# Controls and Error/Fraud Prevention



Application Controls Configuration

# Next Generation Cost of Compliance

$$
\begin{array}{rl}
 & \text{Lowered \$ for Preventive Controls} \\
+ & \text{Efficient Monitoring Controls} \\
+ & \text{\$ Saved with Error Correction} \\
\hline
= & \text{Bottom Line Return on Compliance}
\end{array}
$$
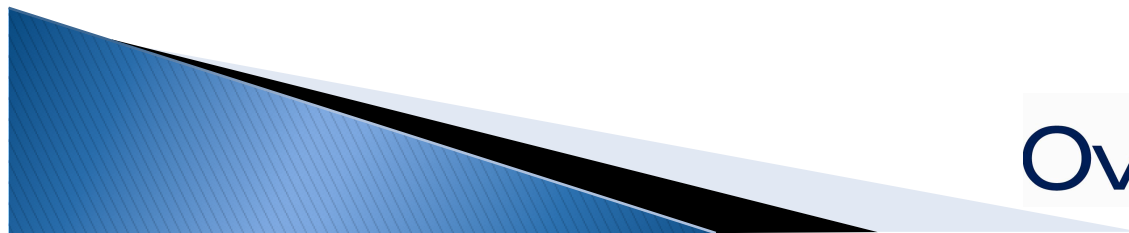
# 3 Keys for Fraud Monitoring

1. Analyze

2. Resolve

3. Document

# Oversight Contact Information

Oversight Systems, Inc.
5500 Interstate North Parkway NW
Suite 300
Atlanta, GA 30328

770-984-4650

www.OversightSystems.com