ORACLE
CloudWorld

# Automate ERP Security and Controls with Embedded Data Science

September 2023

# Intro

## Sam Nyirenda

Director, Internal Controls,
Kelsey-Seybold

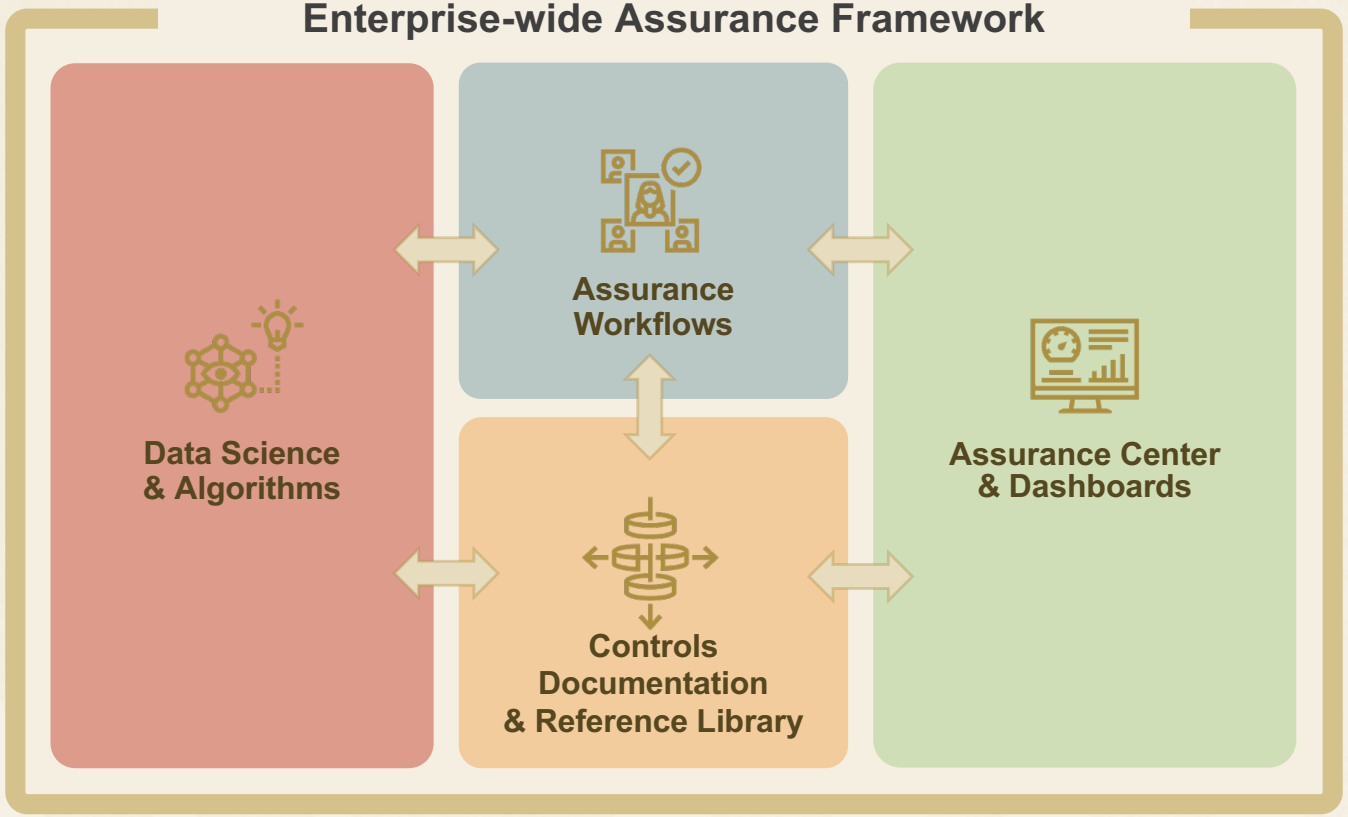
## Manjit Dokal

Director, ERP Systems,
Lyell

## Sid Sinha

VP Product, Fusion Risk Mgmt. Cloud
Oracle

# Connected system of data-driven internal controls




## Daily Assurance

- Certify and assess faster with embedded analytics
- Shift from yearly/quarterly to a daily assurance cycle

## One Connected System

- Promotes risk ownership in line 1
- Align all stakeholders (3 lines)

## Best Practice

- Designed for Oracle Apps
- Shared dashboards for monitoring and reporting across P2P, O2C, R2R & H2R

# Data Science & Algorithms

## Pre-built data science foundation - typically costs $ millions to build and operate

**Ingestion** ▶ **Enrichment** ▶ **Refine Models** ▶ **Deploy Algorithms** ▶ **Act on Results**

Oracle Fusion ERP & HCM Cloud

### Security & Transaction Data

**User & Security Data**
All user accounts, job roles, duty roles, privileges, security context data access sets, BU, Ledger, etc.

- 6000+ Privileges
- 90+ Access Entitlements with 580 key privileges

**Setup, Configuration & Master Data**
Examples: suppliers, items, payables setups, payment terms, payroll definition, etc.

- 2500+ Config Attributes
- 61 Config Business Objects

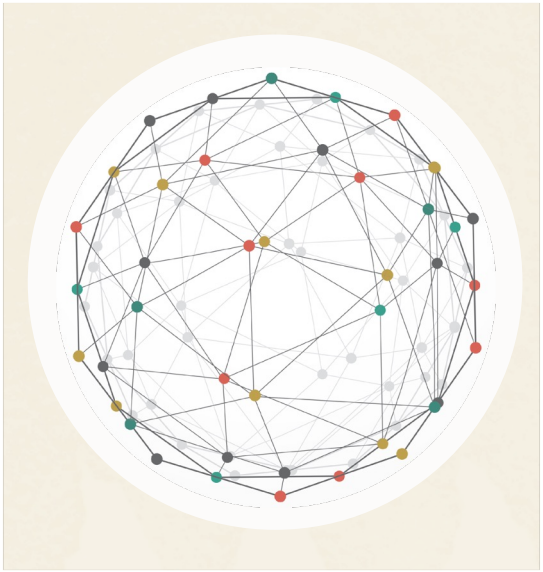
**Audit Policy Trail Data**
Old and new values for key setups including suppliers, customers, compensation plan, etc.

- 16,255+ Audit trail Attributes
- 298 Audit trail Business Objects

**Transaction Data**
Examples: PO, invoices, expenses, payroll, payments, journal entries, timecard, sales orders, etc.

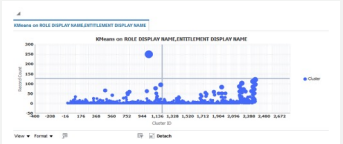
- 4100 Transaction Attributes
- 54 Transaction Business Objects

### Oracle Risk Graph



### Analysis Engine

**Statistical Techniques**



**Graphical Workbench**

**Library of 200+ Models**

**Sam Nyirenda**

Director, Internal Controls,
Kelsey-Seybold

# Challenges for External Auditors

40% of the external audits reviewed had deficiencies (PCAOB 2022 report)

- Audit opinion did not have sufficient evidence
- Gone up 6% from 2021

External audit deficiency related to:

- Design and operating effectiveness of internal controls
- Accuracy and completeness of data
- Reports used in substantive testing

*Question:* What is the Internal Audit deficiency rate?

- Note that external auditors are relying on assessment by internal audit

## Challenges for Internal Auditors

SoD nightmare: “dreaded” December

- Manual SOD tasks using spreadsheets
- Sort and categorized 6000 rows of data manually!
- Emails to 50+ managers → Typical response: “Looks good”

Lack of access to transaction and configuration data

- Sampling not as convincing as testing the entire population

Difficult to share data and results in a timely manner

- Investigate after the fact – 3 to 4 months after!

# Kelsey Seybold Clinic

Houston's Premier Multispecialty Clinic – Over **28 Specialties**

**37 Locations** and Growing Throughout Houston

More than **600 Physicians** and Allied Health Professionals

Kelsey-Seybold Clinic®

Health Plan – Kelseycare Advantage – **over 140K members**

**Pharmacy services**

**Lab services**

# Criteria for selecting Oracle Risk Management

**Seamless integration with Oracle Cloud ERP, HCM & SCM**

- Collaborated with the system implementation team in the design and customization of the security roles – which was vital in deployment of the access system based on the principles of least privilege and the resolution of SOD incidents
- Designed and implemented annual user access certification within the GRC – Ensures that assignment of roles follows the company policy and audit ready
- Implement continuous monitoring of access and transactions through advanced access and financial controls respectively
- Monitor exceptions on dashboard and resolve issues using an incident workflow

**Single platform to coordinate and collaborate with other stakeholders such as IT security**

- Collaborate with IT security in the automation and monitoring of system access including privileges access
- Minimize uncontrolled open-ended access and unnecessary exposure of critical and sensitive data.
- Collaborate with IT security in resolution of access incidents
- Collaborate with IT security in enforcing change management and computer operations policies and procedures
- Monitor changes to sensitive ERP Configurations and Master Data including the preservation of the audit trail.

# Criteria for selecting Oracle Risk Management

**Document manual controls for applications outside Oracle – e.g., Epic**

- Cataloged manual controls in Risk Cloud and utilizes the assessment workflow to document design and operating effectiveness
- Improve security and collaboration by replacing unsecured spreadsheets, emails and documents
- Document control issues and mitigation plans

**Collaborate with the business in resolving access and transaction issues**

- The internal controls team works with the business to resolve transaction or access issues before the issue is closed in the tool

## What was implemented using Fusion Risk Management

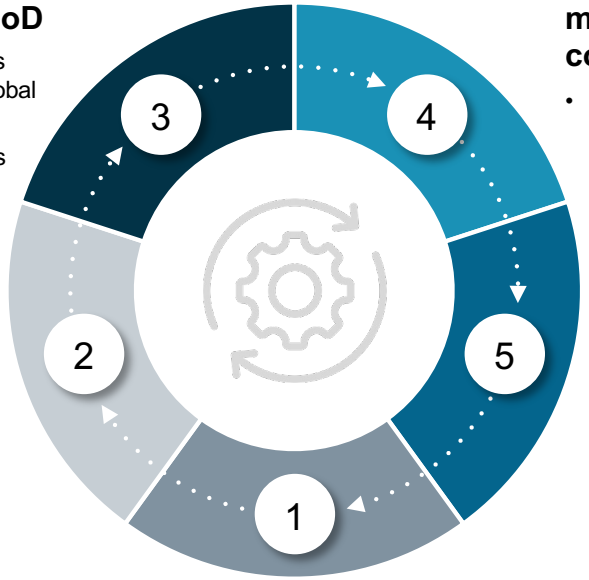
# Number of Automated Internal Controls

**Automated controls for sensitive access and SoD**

- 210 GT Custom AAC Controls spanning ERP & HCM, 10 Global Conditions
- Access Certification workflows

**Automated controls to monitor transactions and configuration changes**

- 140 AFC Controls (Oracle seeded + GT Custom)




**Activate Fusion Audit Policies**

**Dashboard and reporting Oracle (OTBI)**

- Custom GT Dashboard covering (AAC, AFC & FRC)

**Document Internal Controls (Risk & Control Matrix)**

- 218 Kelsey Seybold Controls
  - Entity- Financial Close & Reporting, ITGC, Treasury & Cash – 82
  - Managing Benefits & Payroll – 15
  - Procure to Pay – 87
  - Revenue - 34

## What was implemented using Fusion Risk Management

# Business Process Coverage

### Automated Controls to Monitor Sensitive Access and SoD

- **Monitoring & Incident Management:**
  - ERP- General Ledger, Fixed Assets, Accounts Payable, Cash Management, Accounts Receivable, Expenses, Projects
  - HCM - Human Capital Management, Payroll, Compensation, Recruiting, Benefits
  - SCM – Procure to Pay Processes

### Automated Controls to Monitor Transactions and Configuration Changes

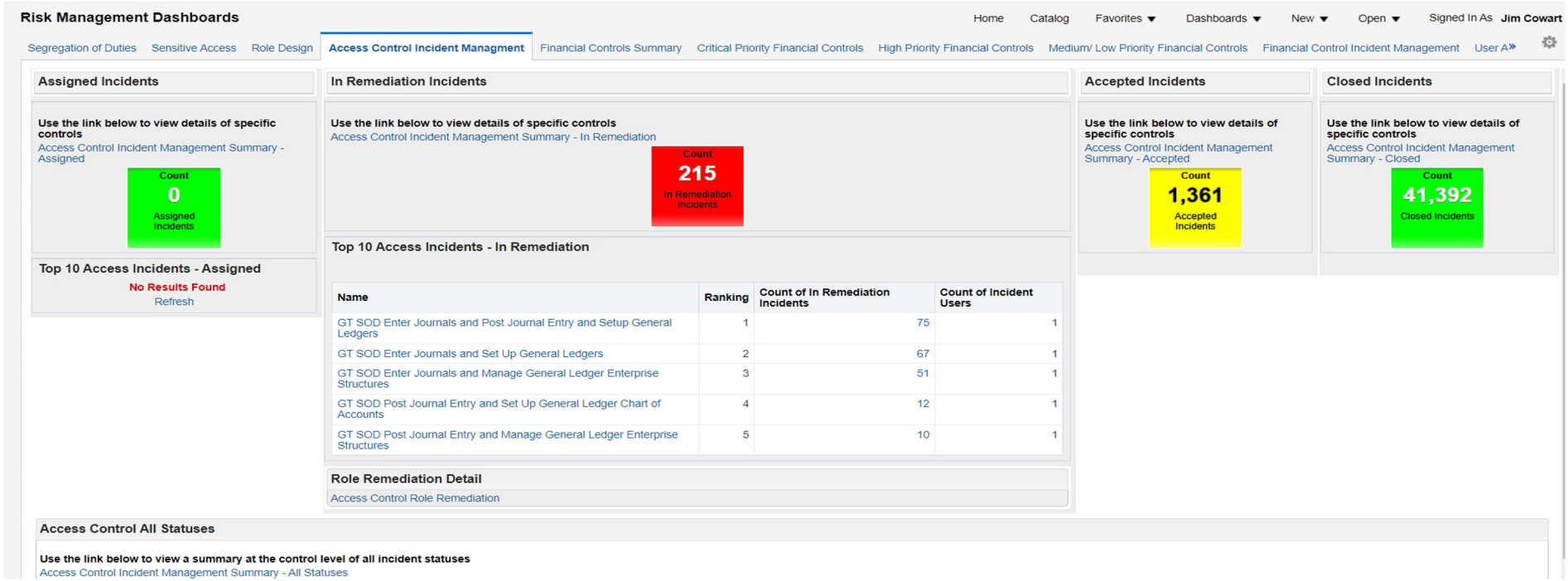
- **Monitoring & Incident Management:**
  - ERP:
    - **Configuration Monitoring Controls:**
      - General Ledger, Fixed Assets, Accounts Payable (Invoices & Payments), Accounts Receivable, System Administration
    - **Transaction Monitoring Controls:**
      - General Ledger, Fixed Assets, Accounts Payable (Invoices & Payments), Accounts Receivable, Expenses, Supplier & Customer Mgmt, System Administration
  - HCM:
    - **Configuration Monitoring Controls:**
      - Human Capital Management
    - **Transaction Monitoring Controls:**
      - Human Capital Management, Payroll, Compensation

### Document Internal Controls (Risk & Control Matrix)

- Major Process Areas:
  - Entity- Financial Close & Reporting, ITGC, Treasury & Cash
  - Managing Benefits & Payroll
  - Procure to Pay
  - Revenue

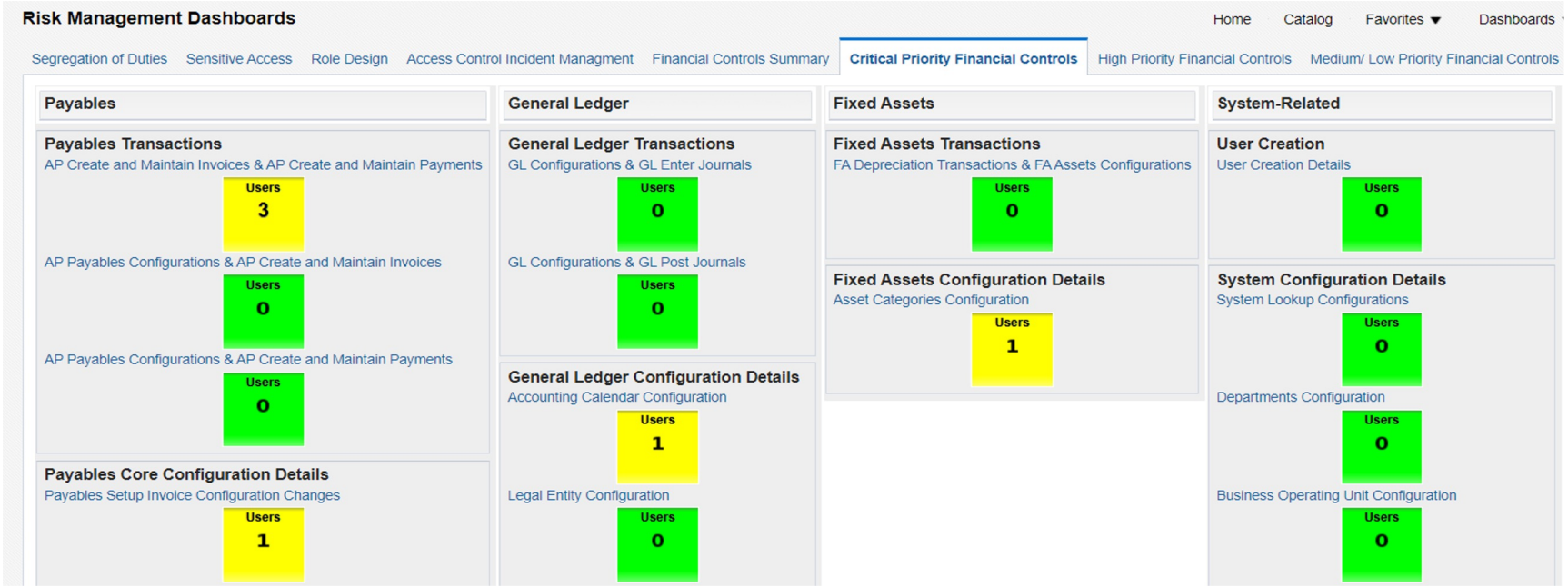
# Kelsey-Seybold Dashboard for Sensitive Access and SoD Controls

Covers lifecycle - provision, de-provision, monitoring sensitive access and user certification



# Kelsey-Seybold Dashboard for Financial Controls

100% of data analyzed for for SOD, Configurations, and transactions (no sampling)




- Continuous monitoring of current state of transactional/financial control incidents, i.e What are people doing with the system privileges they have? (changing config, modifying financial data, etc..)
- Centralized platform to view the full lifecycle of transactional/financial control incidents that have been reviewed and how these incidents were resolved, i.e. Accepted, Remediated, Monitoring

# Example – Backdated Purchase Order

No Purchase Order - No Invoice Pay Policy.  100% of Invoices evaluated

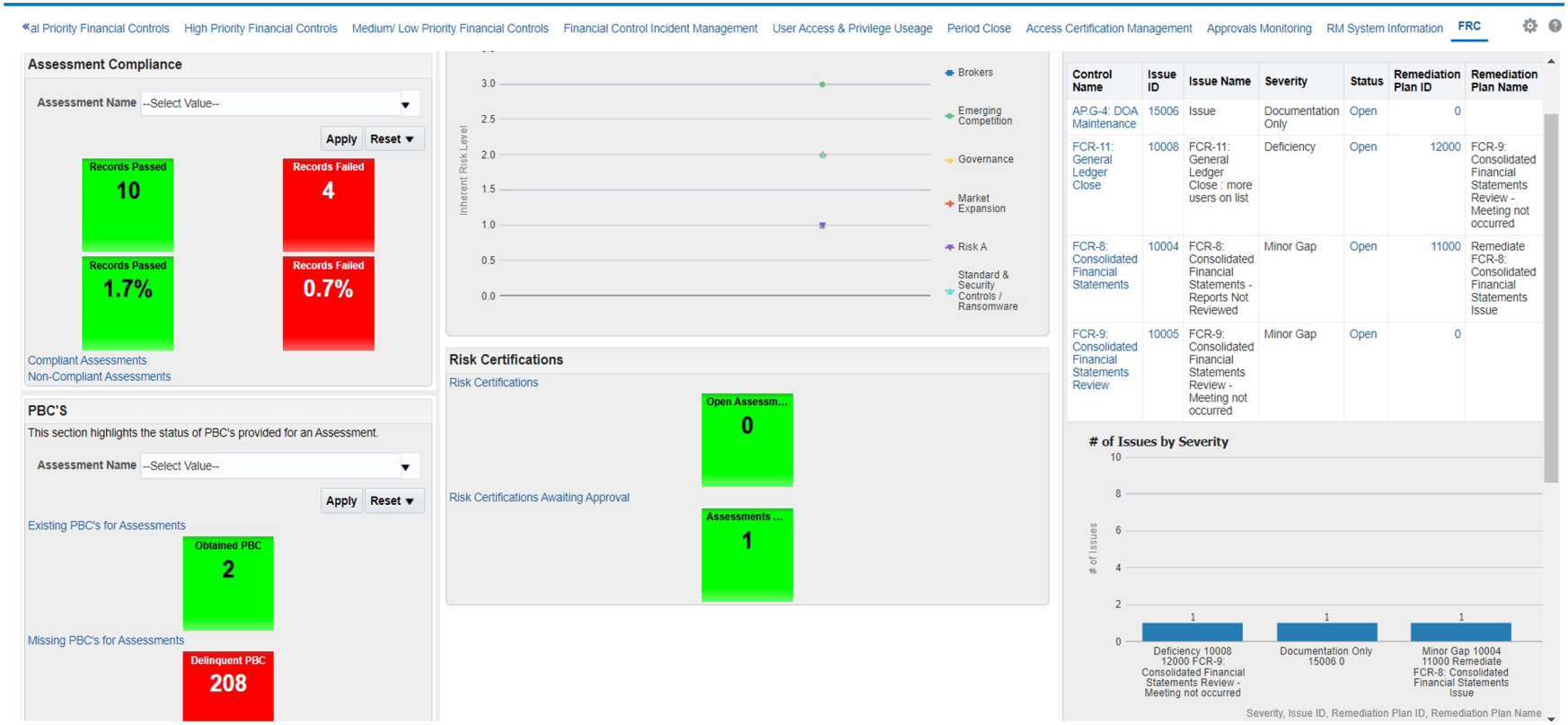
**Top 10 Financial Incidents - Assigned**

| Name | Incident Information | Ranking | Count of Assigned or In Remediation Incidents |
|---|---|---|---|
| users who created PO's | Purchase Order.Created By: FUSION_APPS_PRC_SOA_APPID | 1 | 3515.0 |
| 40010: Journals Created and Approved or Posted by the Same User | Ledger Setup: General.Name: Kelsey Seybold US | 2 | 802.0 |
| GL Open and Close Periods & GL Enter Journals | Journal Entry.Last Updated By: KAChapa@ksnet.com | 3 | 548.0 |
| GL Open and Close Periods & GL Post Journals | Journal Entry.Last Updated By: KAChapa@ksnet.com | 3 | 548.0 |
| users who created PO's | Purchase Order.Created By: K20117@ksnet.com | 5 | 512.0 |
| 30003: Backdated Purchase Orders | Supplier.Supplier Name: CARDINAL HEALTH 108 LLC | 6 | 388.0 |
| users who created PO's | Purchase Order.Created By: BJGary01@ksnet.com | 7 | 385.0 |
| Manage Employee | Person.Created By: anonymous | 8 | 357.0 |
| 40012: Payable Invoices Approved and Created or Updated by the Same User | Supplier.Supplier Name: ALSCO INC | 9 | 331.0 |
| 40013: Payable Invoices Approved and Payment Created or Updated by the Same User | Supplier.Supplier Name: ALSCO INC | 9 | 331.0 |

## Backdated Purchase Orders

- The company has a no PO no Pay policy hence a Purchase Order is required for all purchasing transactions
- Backdated PO could indicate that a purchasing transaction was executed without a PO.
- The Internal Controls team works with the purchasing department to investigate the incident and implement mitigation measures
- Upon resolution, the incident is closed in the GRC

# Kelsey-Seybold Dashboard for Internal Controls Documentation (RCM)



# Key Takeaways

1. **Automation and efficiency of internal controls naturally leads to higher levels of assurance** and confidence that you achieved operating, reporting and compliance objectives.

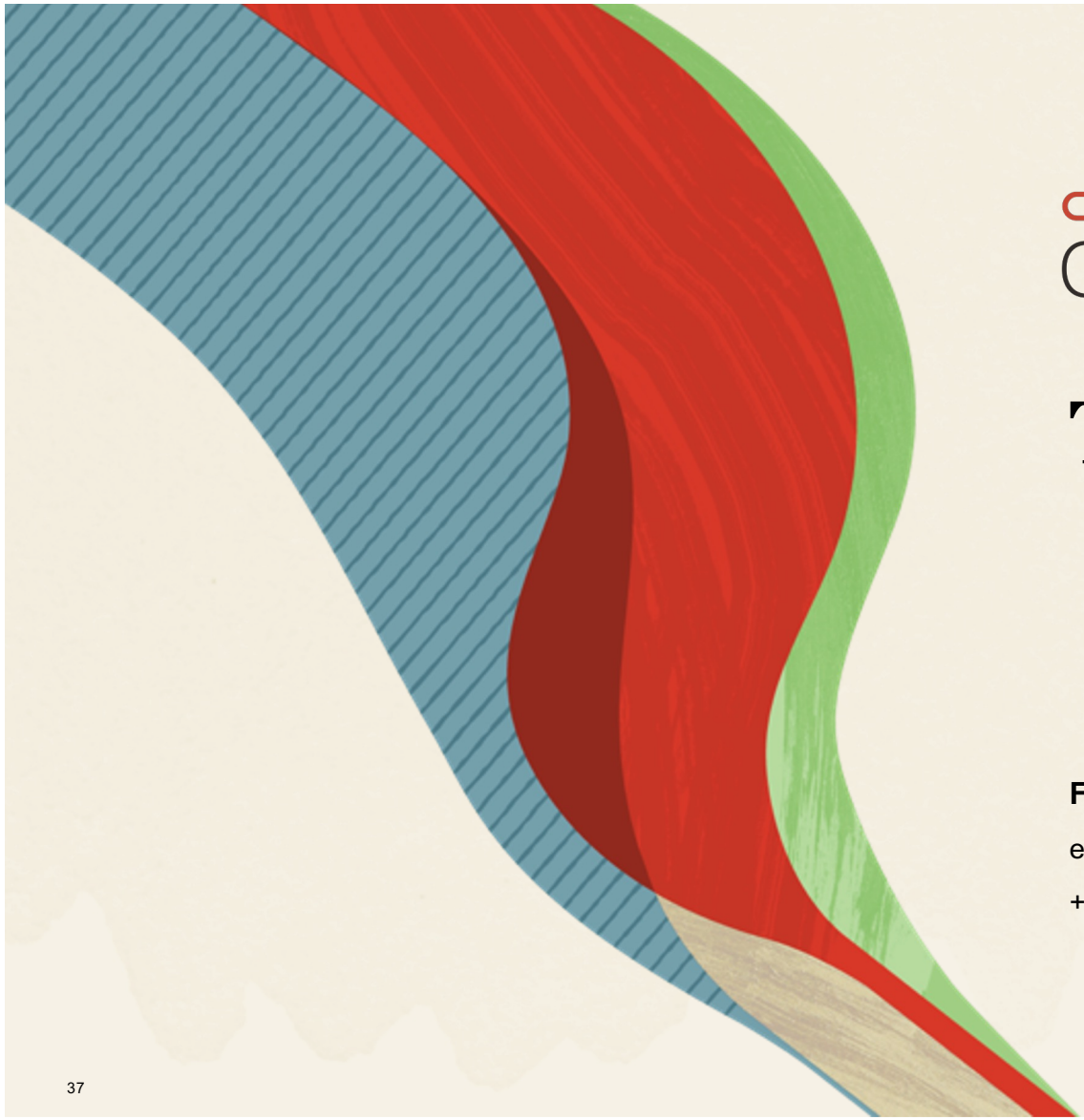
2. **New normal for reasonable assurance. Today an effective and efficient system of internal controls requires more continuous, data-driven monitoring** because cloud-based ERP & HCM transactions are increasingly automated & touchless. Less human oversight => more automated monitoring for assurance.

3. **Priority, priority, priority. Automating internal control activities and monitoring can generate a significant number of results to review**. To avoid becoming overwhelmed, it is crucial to evaluate the materiality and context of the automated results and have a simple methodology or a process to triage them – much like any other business process.

4. **Obtain buy-in from all stakeholders early because risk mgmt. inherently requires a shared vision** across different teams (IT, security, Internal Audit etc.). A single risk platform does help foster a culture of trust and collaboration.

# Takeaways

1. In the Cloud, traditional controls provide a false sense of security
2. Sampling & testing 1 or 2 times a year is inadequate for Cloud ERP
3. Audit standards are changing to data-driven security & financial controls
4. Kelsey Seybold & Lyell evaluated multiple vendors, & chose Risk Cloud to achieve:
    i. *Automated SOD and sensitive access analysis and reporting (avoid "dreaded" December!)*
    ii. *Automated monitoring of 100% of transactions & configurations changes to automate key ICFR activity*
    iii. *Align and unify Process Owners, IT Security and Audit within one system*
    iv. *Eliminate significant expenses with 3rd party SOD and audit analysis by extracting data from ERP*



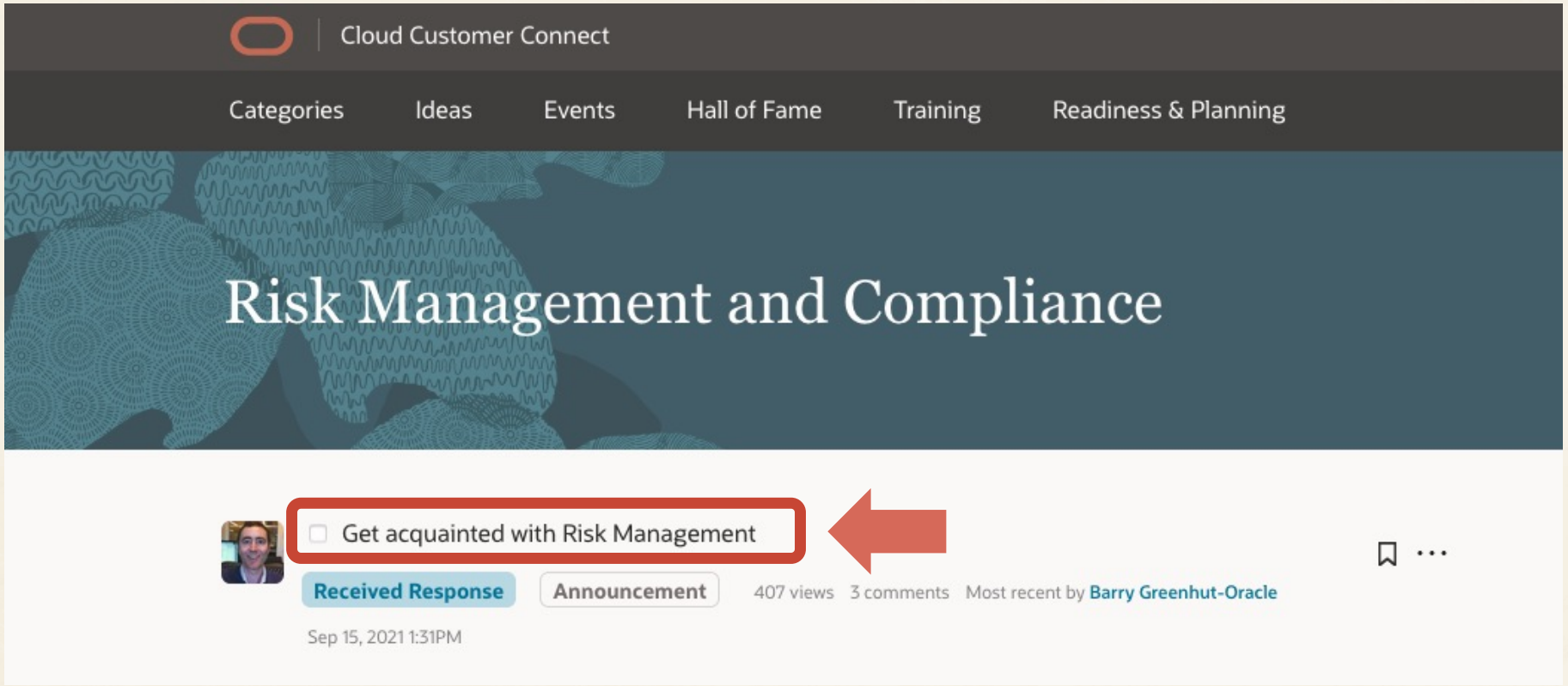
ORACLE
CloudWorld

# Thank you

**Firstname Lastname, Position**

emailaddress@oracle.com

+1 123.456.789

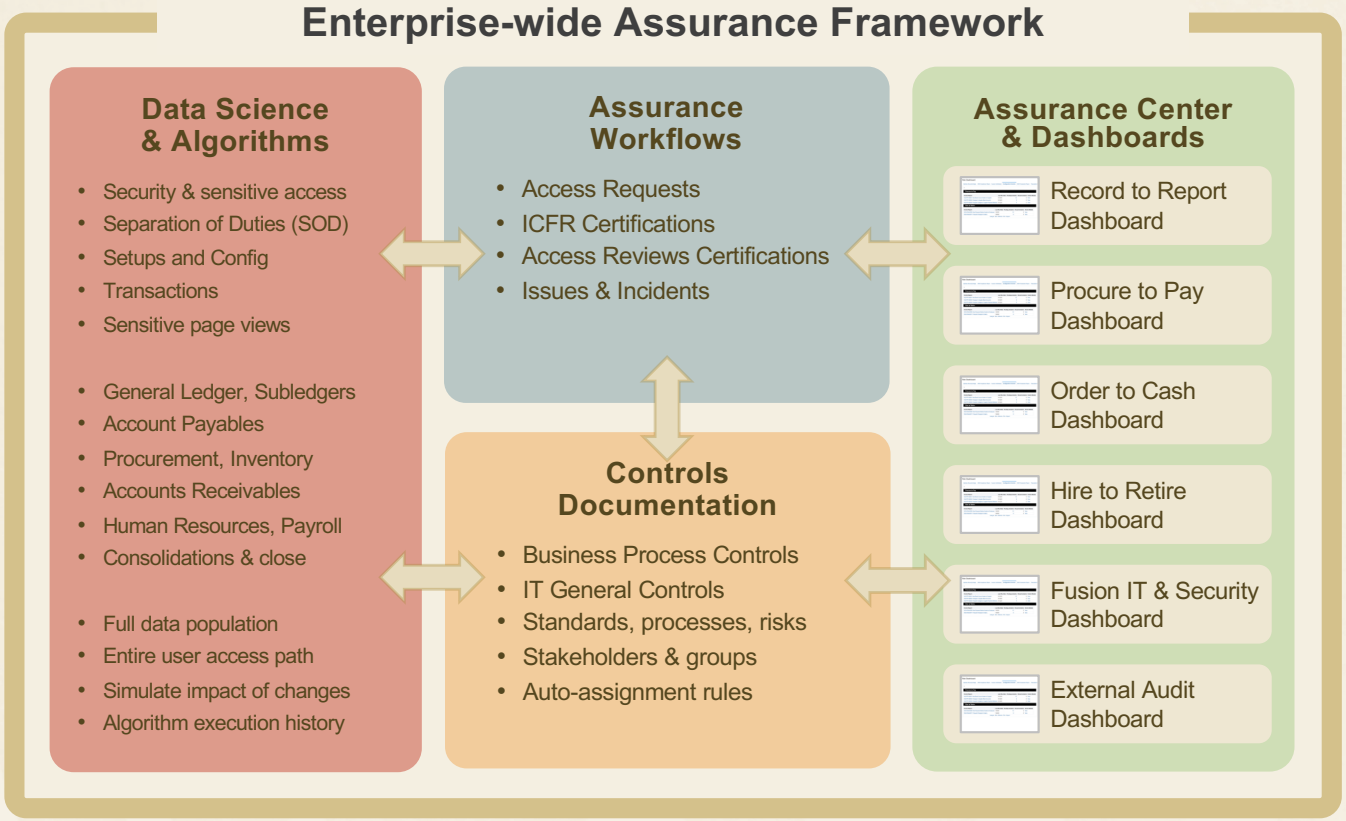



*https://community.oracle.com/customerconnect/categories/erp-risk-management*

Fusion Risk Management Cloud Vision

# One connected system of data-driven security, IT and financial controls

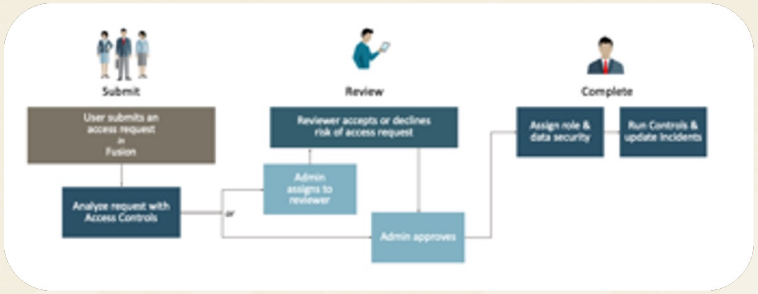


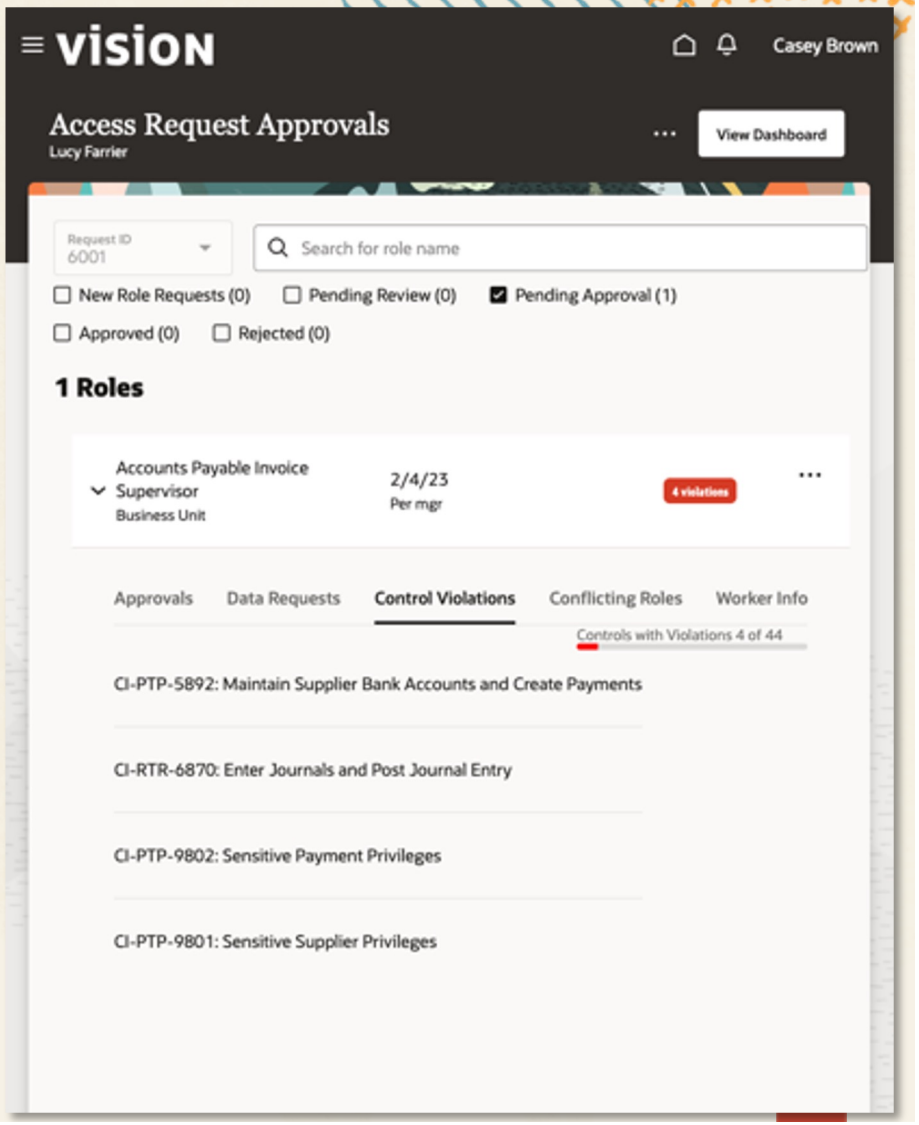

 

Fusion Risk Management example

# Automate ERP access requests with embedded risk analysis

| Traditional Approach | Risk Cloud Approach |
| --- | --- |
| Use of email or custom workflow app | Within Fusion ERP |
| Limited or no access analysis for SOD policy | Complete and Accurate SOD risks in detail |
| Exceptions and approvals in excel | Exception and comments stored within Risk Cloud for reporting |
| Manual granting of access | Automated – saving 100s of hours annually |

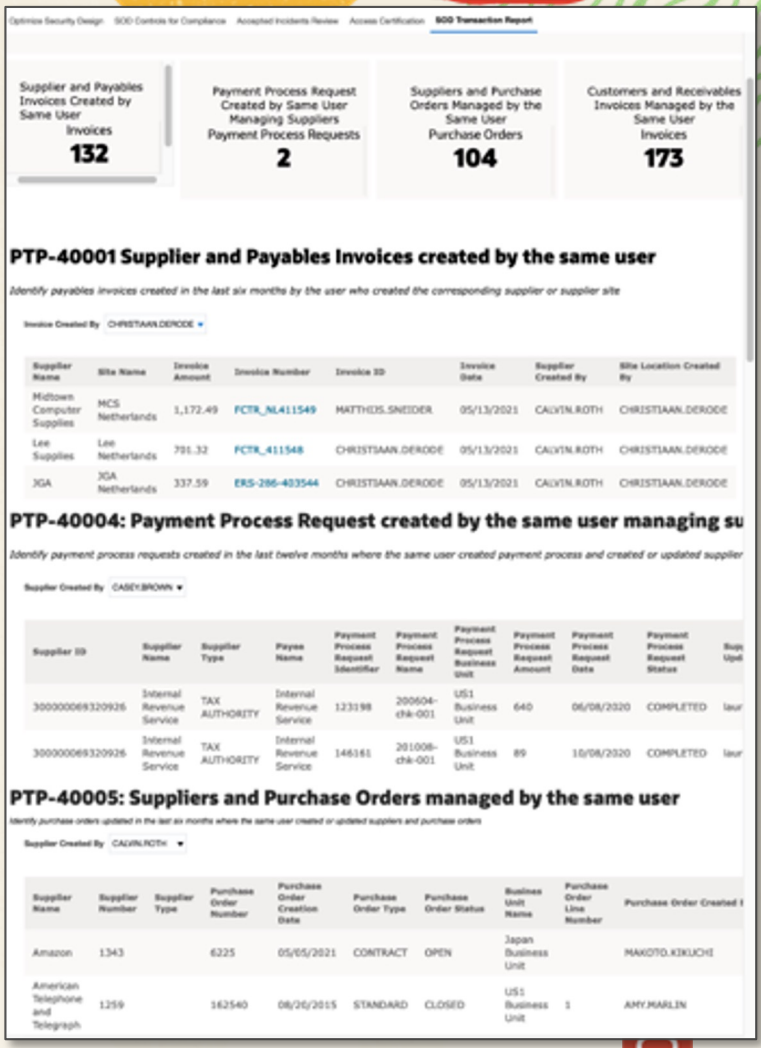


Fusion Risk Management example

# Traditional SOD Controls are inadequate; Cloud provides proof positive

| Traditional Approach | Risk Cloud Approach |
|---|---|
| Detects potential SOD risks | Detects potential & actual SOD violation |
| Analysis on access configuration data | Analysis on millions of transactions and access configuration data |
| Usually runs 1 or 2 times a year | Daily and on-demand |
| Requires extracting data using scripts | Built-in to Fusion |
| Typically costs ~$100 to 200k per year | One of many use cases<br>Faster, cheaper, more accurate and relevant |
| Results managed using email spreadsheets | Results sent to risk owner with dashboards and tracking |



Fusion Risk Management example

# Daily P2P assurance dashboards

**Traditional Approach**

Custom excel or BI reports requiring regular extraction of production data with SQL scripts

Results managed using email spreadsheets

**Risk Cloud Approach**

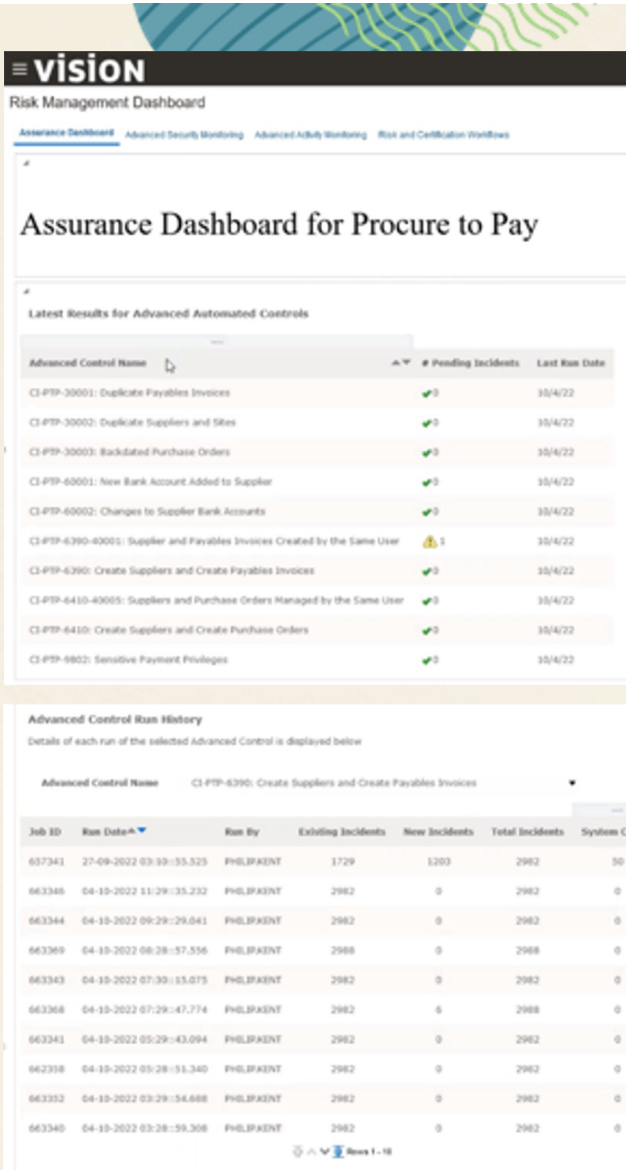
Activate library of seeded P2P algorithms e.g.:

- Backdated POs
- Duplicate Invoices
- Duplicate Suppliers and Sites
- Invoices for One-Time Suppliers with Similar Names
- Frequent changes to Bank Accounts
- Contract Payment Terms Different than Invoices
- Changes to Supplier Bank Accounts on a Weekend

Author new algorithms using a graphical workbench

Track execution history of each algorithm including related findings and number of records that were examined

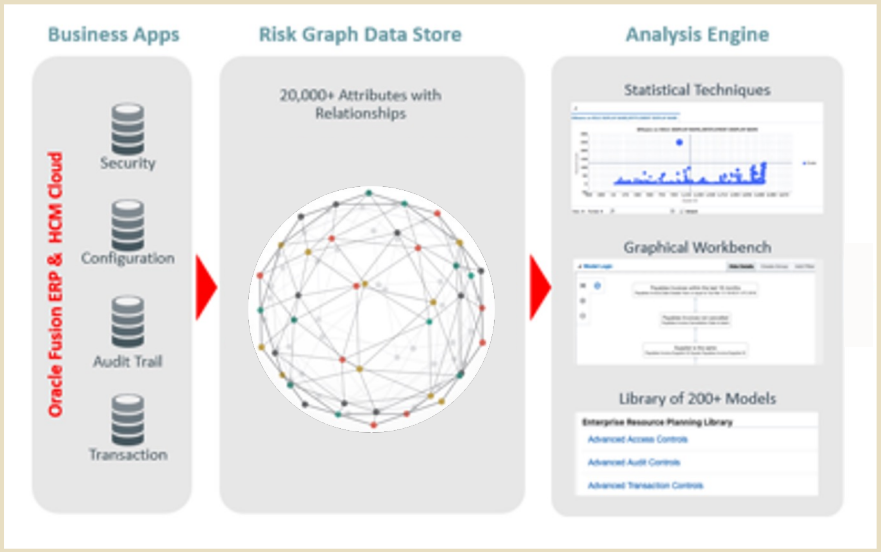
Results sent to risk owner with dashboards and tracking



Fusion Risk Management solutions

# Comprehensive coverage for Security, IT and Financial Controls

## Data Analysis & Algorithms




| Solution Areas | Use Cases |
|---|---|
| Risk Based Access | • Advanced Access Requests<br>• Role Design Dashboard |
| Actual SOD Monitoring<br>Access Certifications | • SOD/Sensitive Access Report<br>• Daily Access (SOD, RU, SA) Assurance<br>• Periodic & Continuous certifications |
| Transaction & Configuration Monitoring | • Procure to Pay Assurance<br>• Record to Report Assurance<br>• Order to Cash Assurance<br>• Hire to Retire Assurance |
| Internal Controls | • Internal Controls Repository<br>• Certification & Testing Workflow |

## Start Before Go-live

Activate Access Controls

Design Roles and User Profiles by simulating potential violations

## Go-live

Periodic and event driving User Certifications

Compliant provisioning

Daily monitoring for Admin access

Daily monitoring for users with SOD risk

Daily monitoring for users that have committed SOD violations

Daily monitoring for viewing sensitive employee data