Case Studies: Streamlining ERP Security and Assurance with Data-Driven Controls

PAN 3998

Panelists

Tina Winkler

*Global Process Manager,
Haemonetics Inc*

Anand Desai

Compliance Lead, Equinix

Richard Kadeg

*Vice President, Information
Technology, Houlihan Lokey*

Ashwat Panchal

*Vice President, Internal Audit,
Skechers USA*

Moderator: Aman Desouza
Risk Cloud Product Strategy

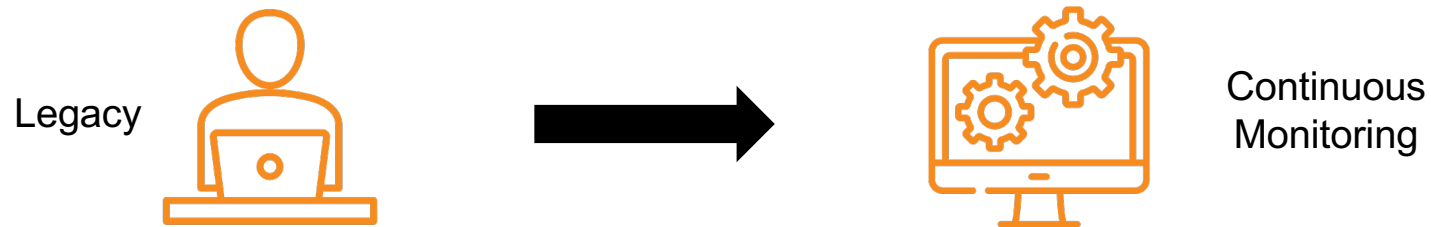![Equinix logo]

Oracle Risk Cloud

Introduction: Who are we

Equinix (NASDAQ: EQIX)

- World's digital infrastructure company^{TM}.
- Founded in 1998
- **10,000+** Customers
- **71** Markets
- **32** Countries
- **6** Continents

EQUINIX

Need for Continuous Monitoring: Motivation

Legacy

Continuous
Monitoring

**Reliance on Manual Controls**

- Manual extraction for key SOX controls
- Do more to prove completeness and accuracy
- Dependency on IT resources
- Lack of audit trail

Continuous Monitoring

- Minimize manual intervention
- Improved visibility into transactional risk
- Proven solution with low maintenance
- Systematically record user activities
- Scalable

EQUINIX

Need for Continuous Monitoring: Business Needs

ERP can get complex with the drivers being, and not limited to:
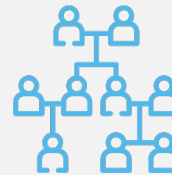
Introduction of new modules

- Users can now see more than what the previously did
- Do more than what they could in the legacy system

Quarterly releases

- Myriad of privileges and data security policies
- Releases requiring privilege validations
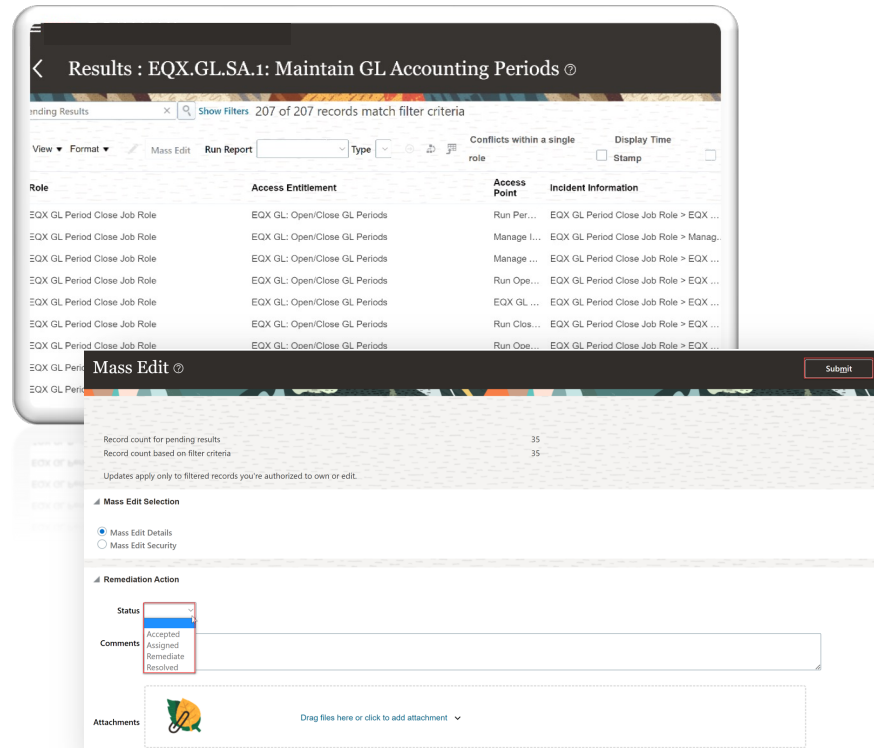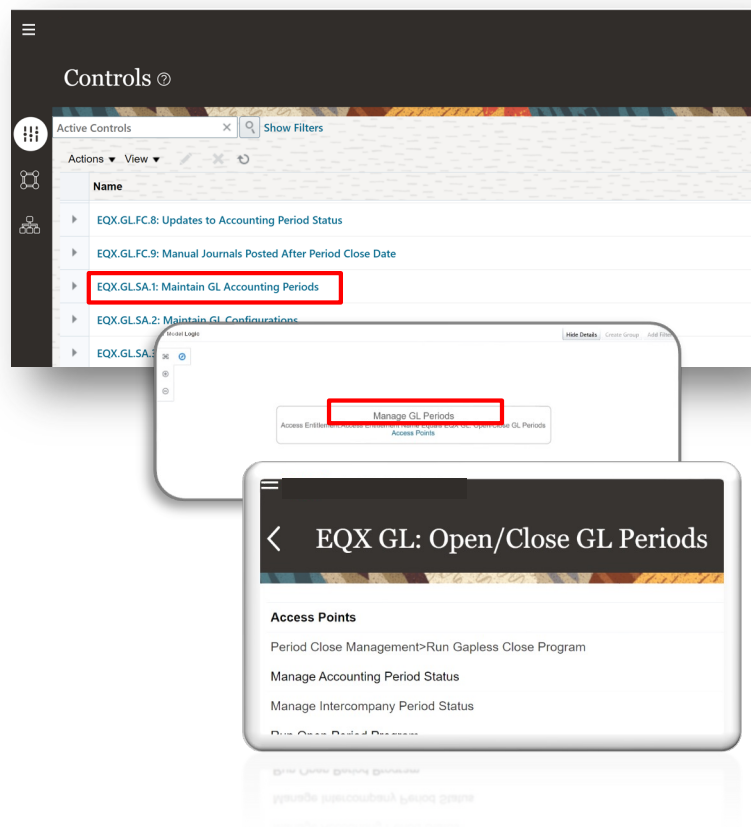
Expansion/Re-org.

- Users with elevated, conflicting access
- Bot accounts
- The list goes on…

Continuous Monitoring solution

- Detect frequent changes to role design
- Access violations
- Transactions
- Provide actionable insights

EQUINIX

Access Controls

Sample Access Rulesets & Incident Management

Transactions and Configuration Controls

Sample Rulesets & Incident Management

*Dependency on audit objects that is made available

© 2022 Equinix

EQUINIX

Key Takeaways: Risk Cloud Journey

Goal: Monitor user access and role changes for segregation of duties(SOD), and changes to audited configuration and operational data. Below is the approach of how we were able to achieve governance and compliance.

Better engagement with stakeholders
Internal/External

Configured Roles
Specific to Cloud – Load Import FBDI
Controlled role provisioning

Reduction in manual effort
Dropped the review cycle by ~50%.

APPROACH

Access Controls
Simplified approach, SOX relevant, role design

Standardized Review
Privileged access review, impact assessment

Configuration and Transaction Controls
Risk based approach: monitor key transactions, configurations

EQUINIX

Where to Start?

1
Access Monitoring

Access Controls, User Access Certification

- Segregation of Duties (SOD) and Sensitive Access (SA)

- Embed role and user level SOD testing during implementation

- Role based User Access Review/Certification workflow

2
Activity Monitoring

Configuration, Transaction Controls

- Monitor changes to configurations e.g., Enablement of JE Approval workflow

- Monitor changes to key transactions e.g., Duplicate Invoices

3
Compliance Workflow

Financial Report Compliance

- End-to-end workflow to automate internal audit assessments, financial reporting certifications and compliance mandates

EQUINIX

Comprehensive coverage for Security, IT and Financial Controls

Data Analysis & Algorithms

Business Apps · Oracle Fusion ERP & HCM Cloud — Security, Configuration, Audit Trail, Transaction

Risk Graph Data Store — 20,000+ Attributes with Relationships

Analysis Engine — Statistical Techniques · Graphical Workbench · Library of 200+ Models
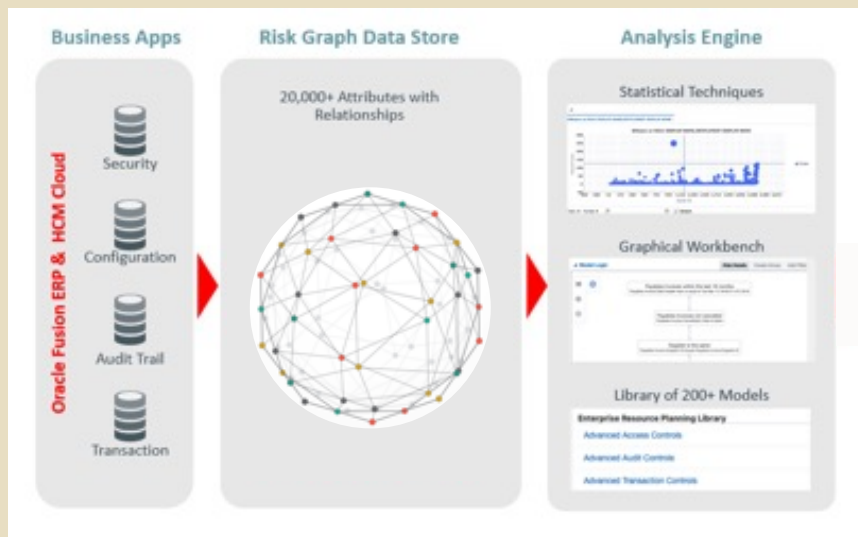
Solution Areas | *Use Cases*

Risk Based Access
- Advanced Access Requests
- Role Design Dashboard

Actual SOD Monitoring
Access Certifications
- SOD/Sensitive Access Report
- Daily Access (SOD, RU, SA) Assurance
- Periodic & Continuous certifications

Transaction & Configuration Monitoring
- Procure to Pay Assurance
- Record to Report Assurance
- Order to Cash Assurance
- Hire to Retire Assurance

Internal Controls
- Internal Controls Repository
- Certification & Testing Workflow

Benefits and business value by stakeholders

Management, CFO, CAO

- *Increase investor & lender confidence with better financial & cybersecurity controls*
- *Increase productivity by replacing drudgery of compliance with data-driven automation*
- *Lower external audit fees*
- *More resilient to change (M&A) and disruptions (pandemic) with better monitoring of operations*

Fusion Cloud
ERP, HCM, SCM
Risk Management

External Audit Team

- *Ensure higher quality audit and reduces costs*
- *Save time with self-service access to the latest documentation, data and controls monitoring results*

Process Leads (Line 1)
Control Owners

- *Certify controls with confidence*
- *Assurance of policy compliance and authorized access*
- *Minimize manual effort and time spent on lower-value compliance tasks*
- *Prevent audit surprises and disruptions*

Risk & Controls Team (Line 2)
Financial Governance, SOX

- *Enhance exec and board level reporting*
- *Faster certification and testing cycle*
- *Enhance relationships with process owners with data-driven insights*
- *Standardize and automate control and governance processes*
- *Automate routine external audit requests for documentation, audit testing and controls monitoring results*
- *Eliminate need for 3rd party SOD analysis*

Fusion IT Team (Line 2)
Security Admin

- *Enforce security and access rules without adding friction to the business*
- *Assurance that ITGC controls for user access, configurations are effective*
- *Design and test (both functional and data access) in roles*
- *Eliminate need for large audit data extracts and related governance*
- *Better prepared to stop and respond to data breaches*

Internal Audit (Line 3)

- *Focus on higher risk areas by automating routine data analysis & monitoring tasks*
- *Provide practical insights to improve operations using better analytics*
- *Easier collaboration with process owners while remaining independent*
- *Better manage scope and negotiations of external audit engagements with reliance on automated internal controls*

ORACLE
CloudWorld

Thank you

Firstname Lastname, Position

emailaddress@oracle.com

+1 123.456.789

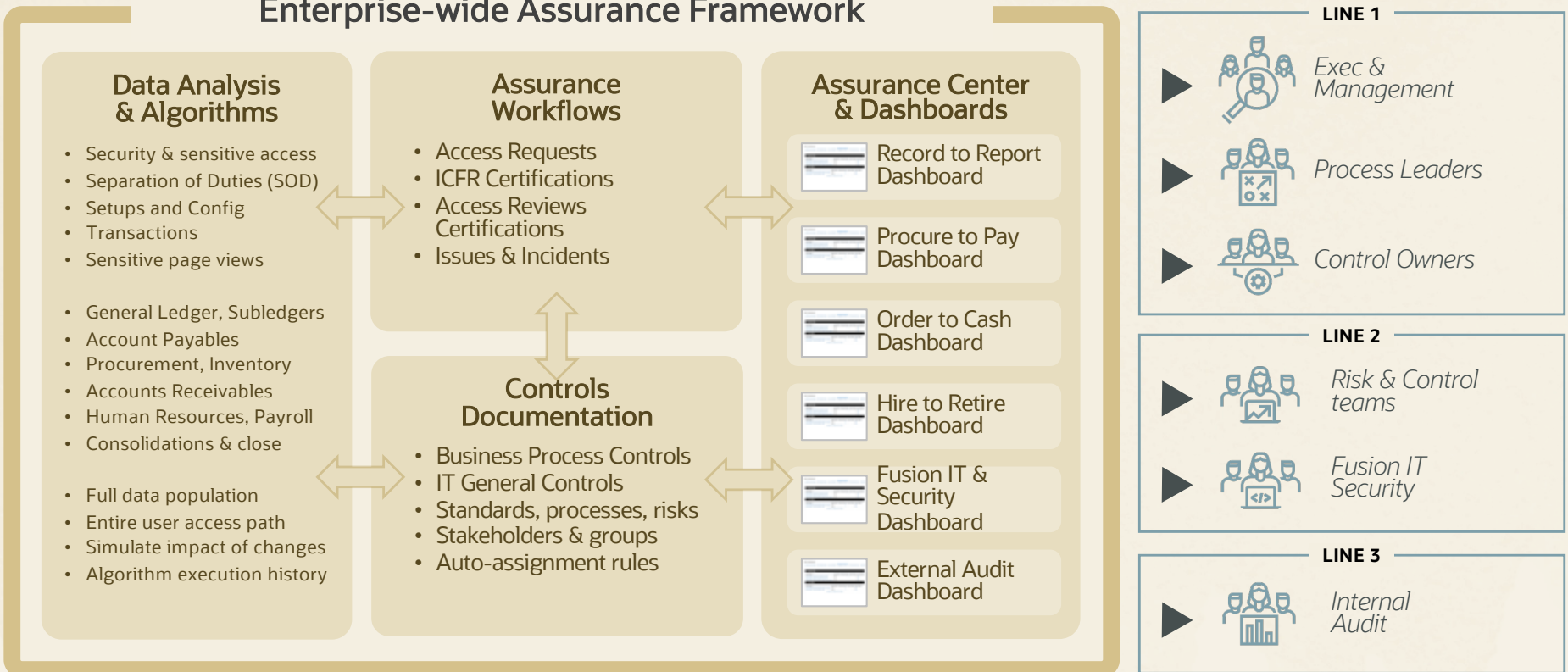| Start Before Go-live	Go-live
✓ Activate Access Controls ✓ Design Roles and User Profiles by simulating potential violations	✓ Periodic and event driving User Certifications ✓ Compliant provisioning ✓ Daily monitoring for Admin access ✓ Daily monitoring for users with SOD risk ✓ Daily monitoring for users that have committed SOD violations ✓ Daily monitoring for viewing sensitive employee data

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

Enterprise-wide Assurance Framework

Data Analysis & Algorithms

- Security & sensitive access
- Separation of Duties (SOD)
- Setups and Config
- Transactions
- Sensitive page views

- General Ledger, Subledgers
- Account Payables
- Procurement, Inventory
- Accounts Receivables
- Human Resources, Payroll
- Consolidations & close

- Full data population
- Entire user access path
- Simulate impact of changes
- Algorithm execution history

Assurance Workflows

- Access Requests
- ICFR Certifications
- Access Reviews Certifications
- Issues & Incidents

Controls Documentation

- Business Process Controls
- IT General Controls
- Standards, processes, risks
- Stakeholders & groups
- Auto-assignment rules

Assurance Center & Dashboards

- Record to Report Dashboard
- Procure to Pay Dashboard
- Order to Cash Dashboard
- Hire to Retire Dashboard
- Fusion IT & Security Dashboard
- External Audit Dashboard

LINE 1
- *Exec & Management*
- *Process Leaders*
- *Control Owners*

LINE 2
- *Risk & Control teams*
- *Fusion IT Security*

LINE 3
- *Internal Audit*

Automate ERP access requests with embedded risk analysis

Traditional Approach

Use of email or custom workflow app

Limited or no access analysis for SOD policy

Exceptions and approvals in excel

Manual granting of access

 Risk Cloud Approach
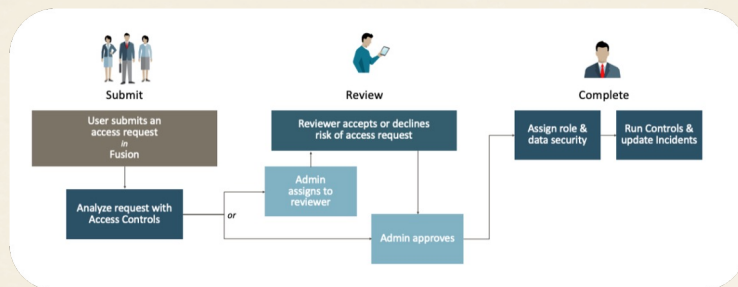
▶ Within Fusion ERP

▶ Complete and Accurate SOD risks in detail

▶ Exception and comments stored within Risk Cloud for reporting

▶ Automated – saving 100s of hours annually

≡ **VISION** ⌂ 🔔 Casey Brown

Access Request Approvals
Lucy Farrier

··· View Dashboard

Request ID
6001 ▾   🔍 Search for role name

☐ New Role Requests (0)   ☐ Pending Review (0)   ☑ Pending Approval (1)
☐ Approved (0)   ☐ Rejected (0)

1 Roles

∨ Accounts Payable Invoice Supervisor
Business Unit   2/4/23
Per mgr   **4 violations**   ···

Approvals   Data Requests   **Control Violations**   Conflicting Roles   Worker Info

Controls with Violations 4 of 44

CI-PTP-5892: Maintain Supplier Bank Accounts and Create Payments

CI-RTR-6870: Enter Journals and Post Journal Entry

CI-PTP-9802: Sensitive Payment Privileges

CI-PTP-9801: Sensitive Supplier Privileges

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 — Faster, cheaper, more accurate and relevant
Results managed using email spreadsheets	▶	Results sent to risk owner with dashboards and tracking

Optimize Security Design SOD Controls for Compliance Accepted Incidents Review Access Certification **SOD Transaction Report**

Supplier and Payables Invoices Created by Same User Invoices	Payment Process Request Created by Same User Managing Suppliers Payment Process Requests	Suppliers and Purchase Orders Managed by the Same User Purchase Orders	Customers and Receivables Invoices Managed by the Same User Invoices
132	**2**	**104**	**173**

PTP-40001 Supplier and Payables Invoices created by the same user

Identify payables invoices created in the last six months by the user who created the corresponding supplier or supplier site

Invoice Created By CHRISTIAAN.DERODE ▾

Supplier Name	Site Name	Invoice Amount	Invoice Number	Invoice ID	Invoice Date	Supplier Created By	Site Location Created By
Midtown Computer Supplies	MCS Netherlands	1,172.49	FCTR_NL411549	MATTHIJS.SNEIDER	05/13/2021	CALVIN.ROTH	CHRISTIAAN.DERODE
Lee Supplies	Lee Netherlands	701.32	FCTR_411548	CHRISTIAAN.DERODE	05/13/2021	CALVIN.ROTH	CHRISTIAAN.DERODE
JGA	JGA Netherlands	337.59	ERS-286-403544	CHRISTIAAN.DERODE	05/13/2021	CALVIN.ROTH	CHRISTIAAN.DERODE

PTP-40004: Payment Process Request created by the same user managing su

Identify payment process requests created in the last twelve months where the same user created payment process and created or updated supplier

Supplier Created By CASEY.BROWN ▾

Supplier ID	Supplier Name	Supplier Type	Payee Name	Payment Process Request Identifier	Payment Process Request Name	Payment Process Request Business Unit	Payment Process Request Amount	Payment Process Request Date	Payment Process Request Status	Supp Upd
300000069320926	Internal Revenue Service	TAX AUTHORITY	Internal Revenue Service	123198	200604-chk-001	US1 Business Unit	640	06/08/2020	COMPLETED	laur
300000069320926	Internal Revenue Service	TAX AUTHORITY	Internal Revenue Service	146161	201008-chk-001	US1 Business Unit	89	10/08/2020	COMPLETED	laur

PTP-40005: Suppliers and Purchase Orders managed by the same user

Identify purchase orders updated in the last six months where the same user created or updated suppliers and purchase orders

Supplier Created By CALVIN.ROTH ▾

Supplier Name	Supplier Number	Supplier Type	Purchase Order Number	Purchase Order Creation Date	Purchase Order Type	Purchase Order Status	Busines Unit Name	Purchase Order Line Number	Purchase Order Created
Amazon	1343		6225	05/05/2021	CONTRACT	OPEN	Japan Business Unit		MAKOTO.KIKUCHI
American Telephone and Telegraph	1259		162540	08/20/2015	STANDARD	CLOSED	US1 Business Unit	1	AMY.MARLIN

Fusion Risk Management example

Daily P2P assurance dashboards

Traditional Approach

☁ **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

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

Author new algorithms using a graphical workbench

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

Results managed using email spreadsheets ▶ Results sent to risk owner with dashboards and tracking

44

Features that connect and align stakeholders

Management, CFO, CAO

- *Review Assurance dashboards*
- *Review ICFR certifications*
- *Monitor exceptions*
- *Monitor remediation plans*

Fusion Cloud
ERP, HCM, SCM
Risk Management

External Audit Team

- *Restricted access to:*
  - *Review Documented Internal Controls*
  - *Replace large data extraction requests with analysis using Risk Cloud*
  - *Rely on ICFR assurance dashboards*

Process Leads (Line 1) Control Owners

- *Review Controls documentation*
- *Certify Process Controls*
- *Certify access to ERP users*
- *Review new access requests with SOD analysis*
- *Alerts for high risk transactions*
- *Alerts for high risk changes to setups and configurations*
- *Review Assurance dashboards*
  - *R2R, P2P, O2C & H2R*

Risk & Controls Team (Line 2) Financial Governance, SOX

- *Manage Controls documentation*
- *ICFR Certifications workflow*
- *Audit testing workflow*
- *Automate Business Process Controls*
  - *Data analysis for Testing activity*
  - *Data analysis for Monitoring status*
- *Automate IT General Controls*
  - *Data analysis for Separation of Duties (SOD)*
  - *Data analysis for Sensitive access*
  - *Data analysis for Restricted access*
- *Review Assurance dashboards*
  - *R2R, P2P, O2C & H2R*

Fusion IT Team (Line 2) Security Admin

- *Manage ITGC documentation*
- *Certify ITGC Controls*
- *Manage ERP access requests workflow with SOD analysis*
- *Monitor users viewing of sensitive HR data*
- *Automate security analysis for new Roles*
- *Review Assurance dashboards*
  - *IT users with admin access*
  - *IT users with Separation of Duties (SOD), Sensitive or Restricted access*
  - *High risk changes to setups & configuration*

Internal Audit (Line 3)

- *Review Internal Controls*
- *Manage remediation plans*
- *Automate data analysis for audit testing*
  - *Full data population testing*
  - *Author new algorithms*
- *Review Assurance dashboards*
  - *R2R, P2P, O2C, H2R, IT Security*