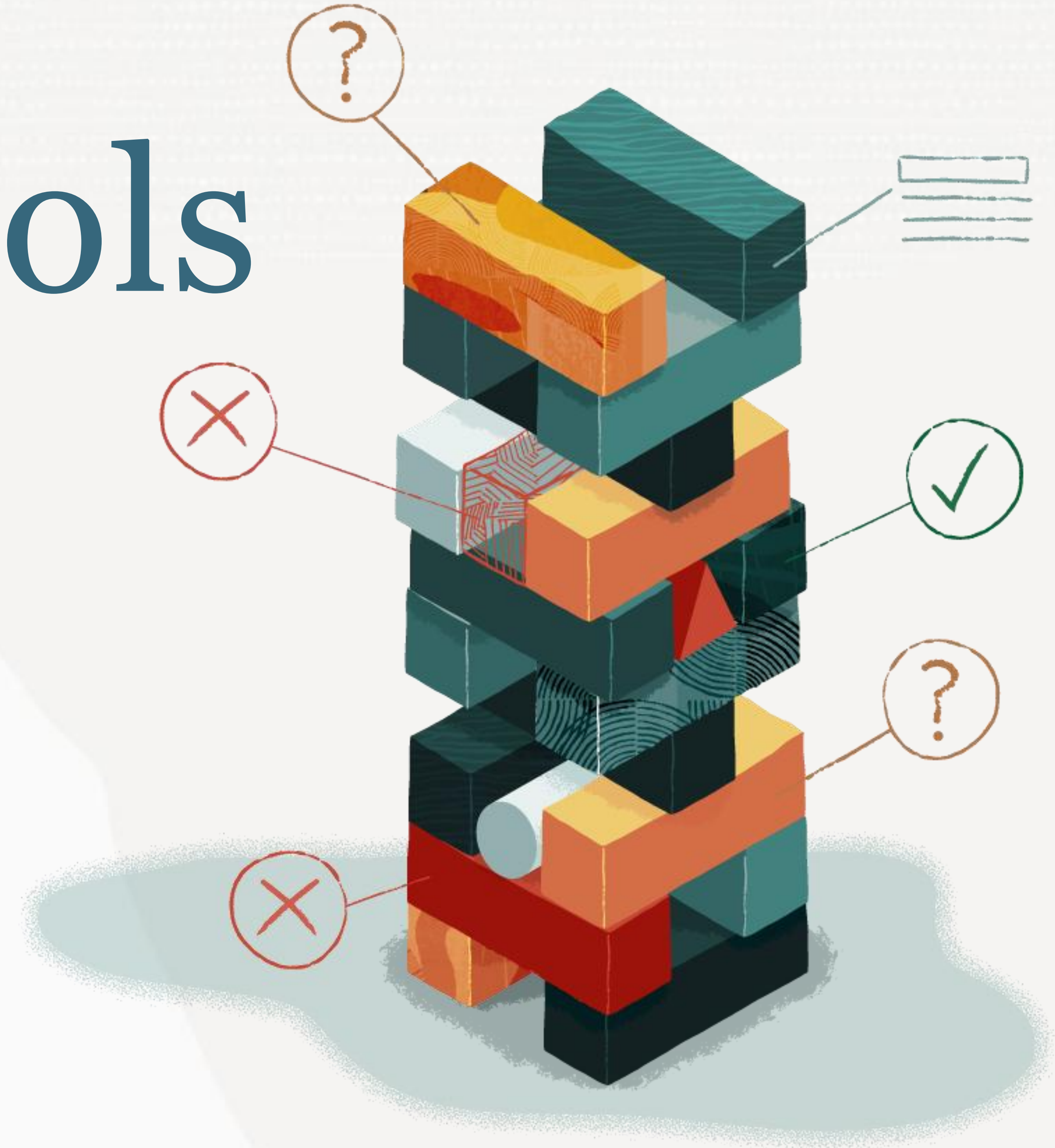
ORACLE

Advanced HCM Controls



A fully integrated Risk Management Solution within Oracle Cloud HCM

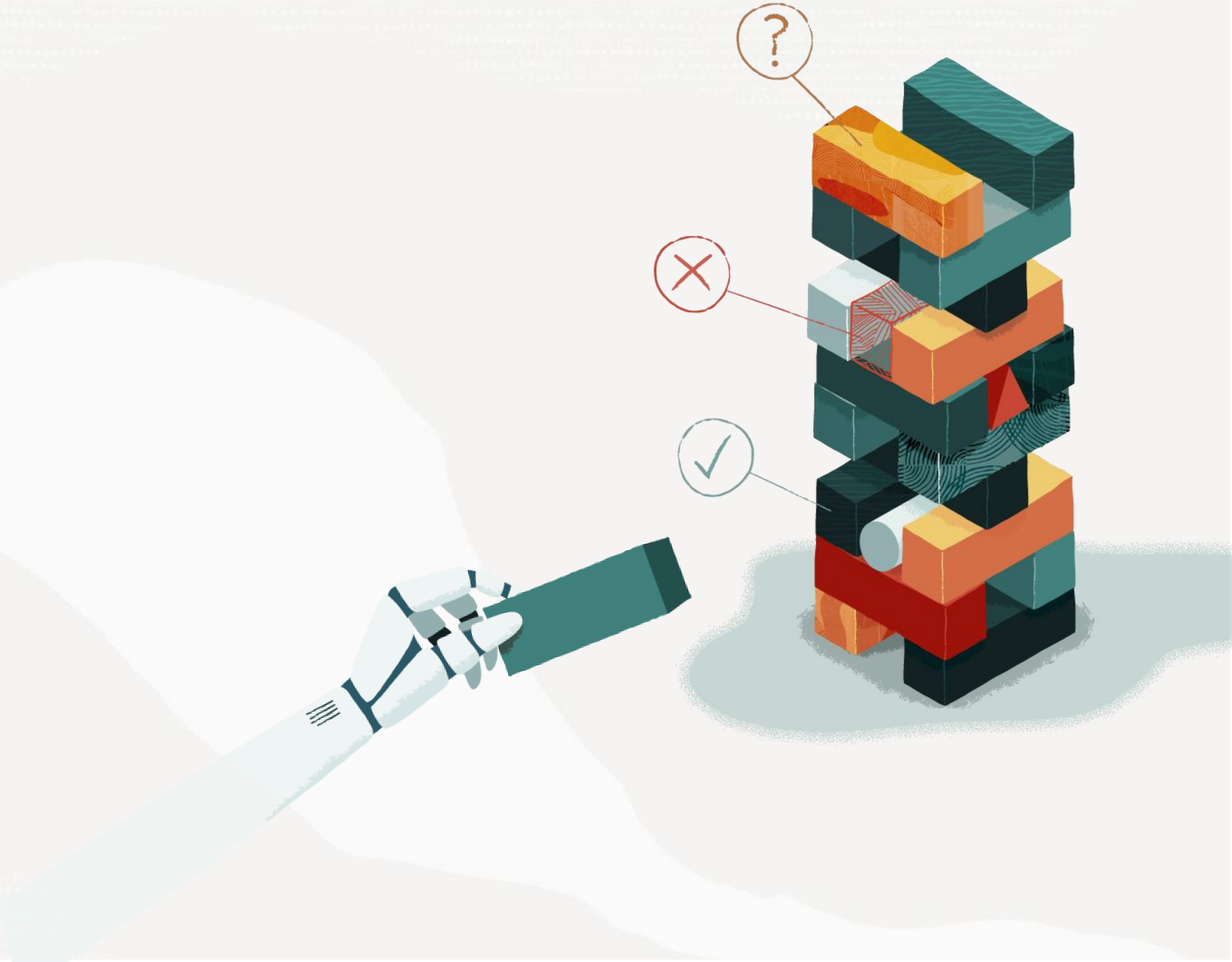
Cloud computing is fundamentally changing all business applications

How do we prepare for this emerging challenge?

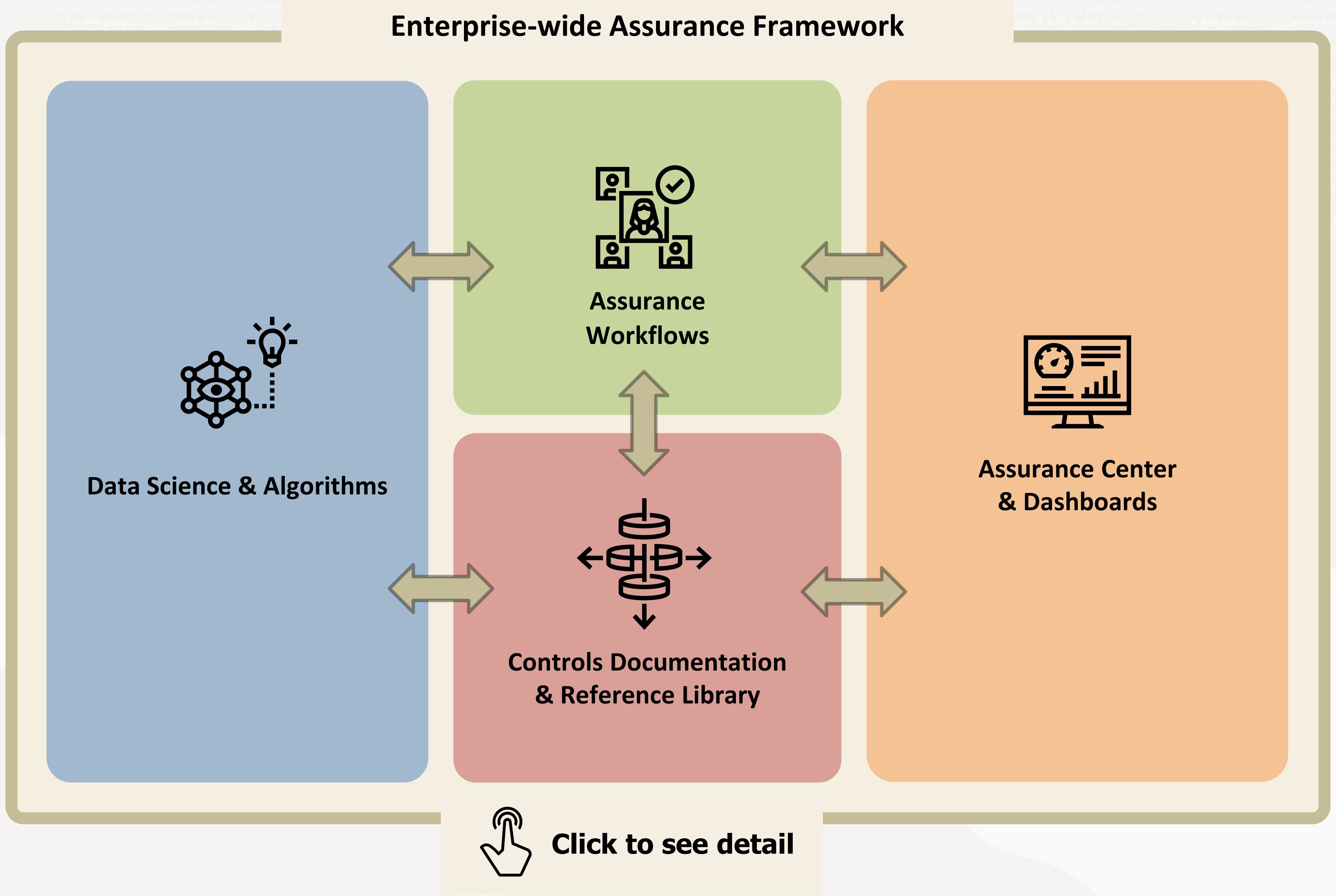
In the cloud, business processes happen much faster, are more automated and are accessed by more users who could be anywhere in the world. This shift is impacting internal controls – which also need to be faster, more frequently tested and more data-driven.

Privacy and Audit standards are responding to this new reality with new requirements for cyber security disclosures, privacy and data driven controls.

Organizations are embarking on transformation of internal controls for HCM along with other back-office applications, to provide Hire-to-Retire assurance.



Oracle Advanced HCM Controls


Enterprise-wide Assurance Framework
Data Science & Algorithms
Assurance Workflows
Controls Documentation & Reference Library
Assurance Center & Dashboards
Click to see detail

Prevent SOD violations

Monitor user access

Monitor user activity

Explore key use cases
to solve the most difficult risk & security challenges

A complete solution for security, HR & IT controls and compliance

- Embeds compliance and assurance into one solution built on data science and algorithms.
- Automates routine, labor-intensive risk tasks related to monitoring of security, configurations and transactions
- Eliminates the need to transport or move data for analysis thereby delivering assurance without exposure to integration vulnerabilities.
- Leverage AI driven monitoring to reduce compensation and payroll fraud, security breaches, and cash leakage.

Prevent SOD violations

Prevent SOD violations

Monitor user access

Monitor user activity

Manage Internal Controls

Design custom roles without SOD violations

Design Custom Roles without Separation of Duties (SOD) Violations

Accelerate HCM security configuration

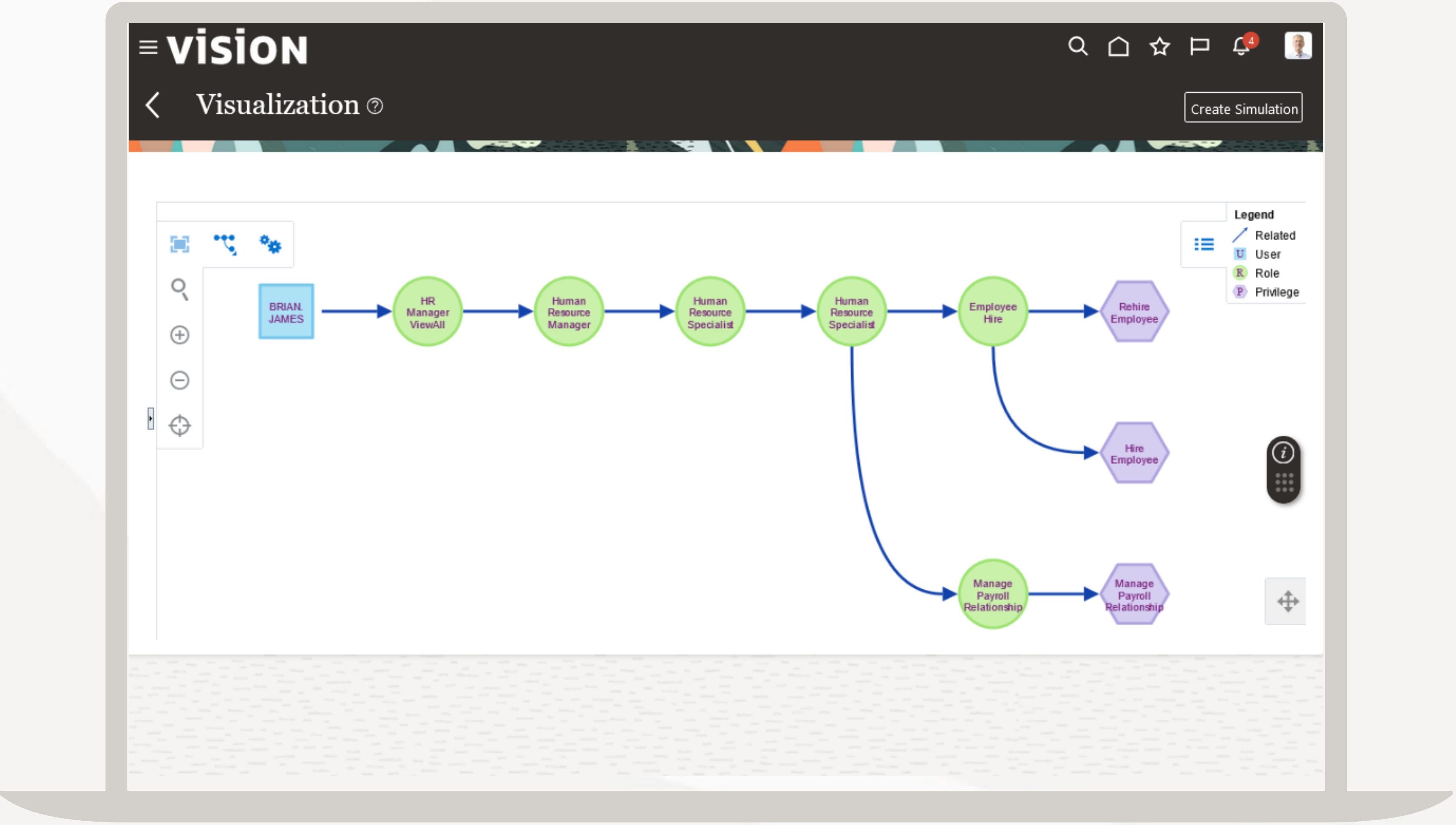
- Automate analysis of user access to identify and eliminate SOD conflicts. Ensure that roles are compliant and audit ready. Start analyzing security configurations in hours, to avoid last-moment user acceptance testing (UAT) issues, that will delay your HCM project.

Design roles without inherent risks

- Utilize visualizations and simulations to make the best design decisions. Eliminate poorly designed roles, which are the leading cause of audit findings after go-live. Building job roles without inherent risk saves thousands in unnecessary remediation.

Leverage library of pre-built security rules

- Use best-practice sensitive access and SOD rules to ensure your roles are complaint prior to go-live. View SOD results in minutes using a pre-built library of 30+ best-practice rules.



Monitor user access

Prevent SOD violations

Monitor user access

Monitor user activity

Manage Internal Controls

Monitor & Report Sensitive (Restricted) Access

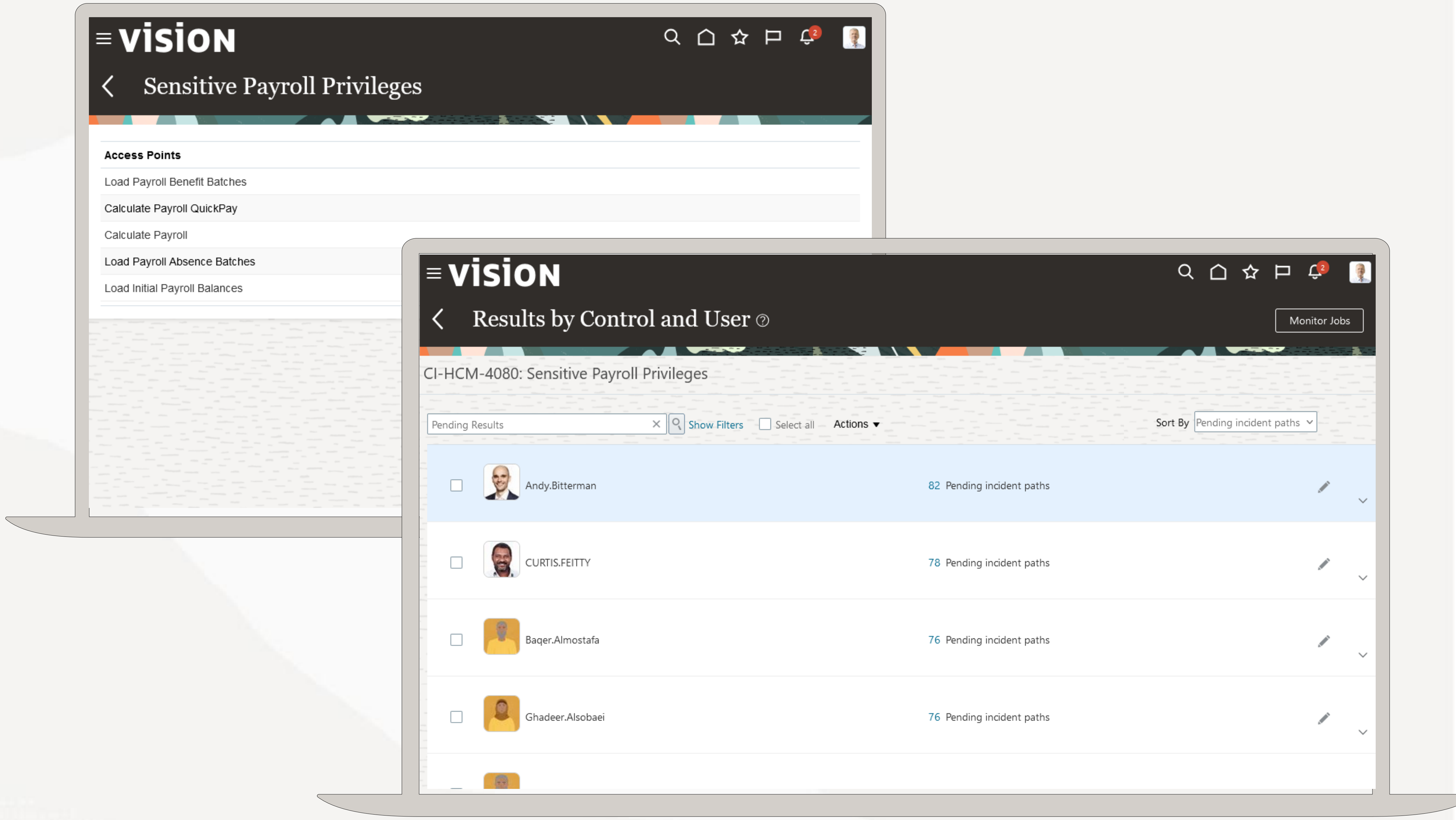
Monitor & Report Separation of Duties (SOD)

Digitize user access certification workflows

Monitor & Report Sensitive (Restricted) Access

Monitor sensitive access granted to users and activity performed with sensitive access

- Identify roles and privileges that are highly restricted and monitor users with this access.
- Monitor configuration updates and transactions performed by users with sensitive access.



Sensitive Payroll Privileges

Access Points
Load Payroll Benefit Batches
Calculate Payroll QuickPay
Calculate Payroll
Load Payroll Absence Batches
Load Initial Payroll Balances

Results by Control and User

CI-HCM-4080: Sensitive Payroll Privileges

□	Andy.Bitterman	82 Pending incident paths
□	CURTIS.FEITTY	78 Pending incident paths
□	Baqer.Almostafa	76 Pending incident paths
□	Ghadeer.Alsobaei	76 Pending incident paths

Monitor user access

Prevent SOD violations

Monitor user access

Monitor user activity

Manage Internal Controls

Monitor & Report Sensitive (Restricted) Access

Monitor & Report Separation of Duties (SOD)

Digitize user access certification workflows

Monitor & Report Separation of Duties (SOD)

Analyze enforcement of security and privacy policies

- Continuously analyze roles and user access as business functions or responsibilities evolve. Quickly identify SOD violations to refine roles and security configurations in response to ever-changing organizations.

Protect security data from exposure

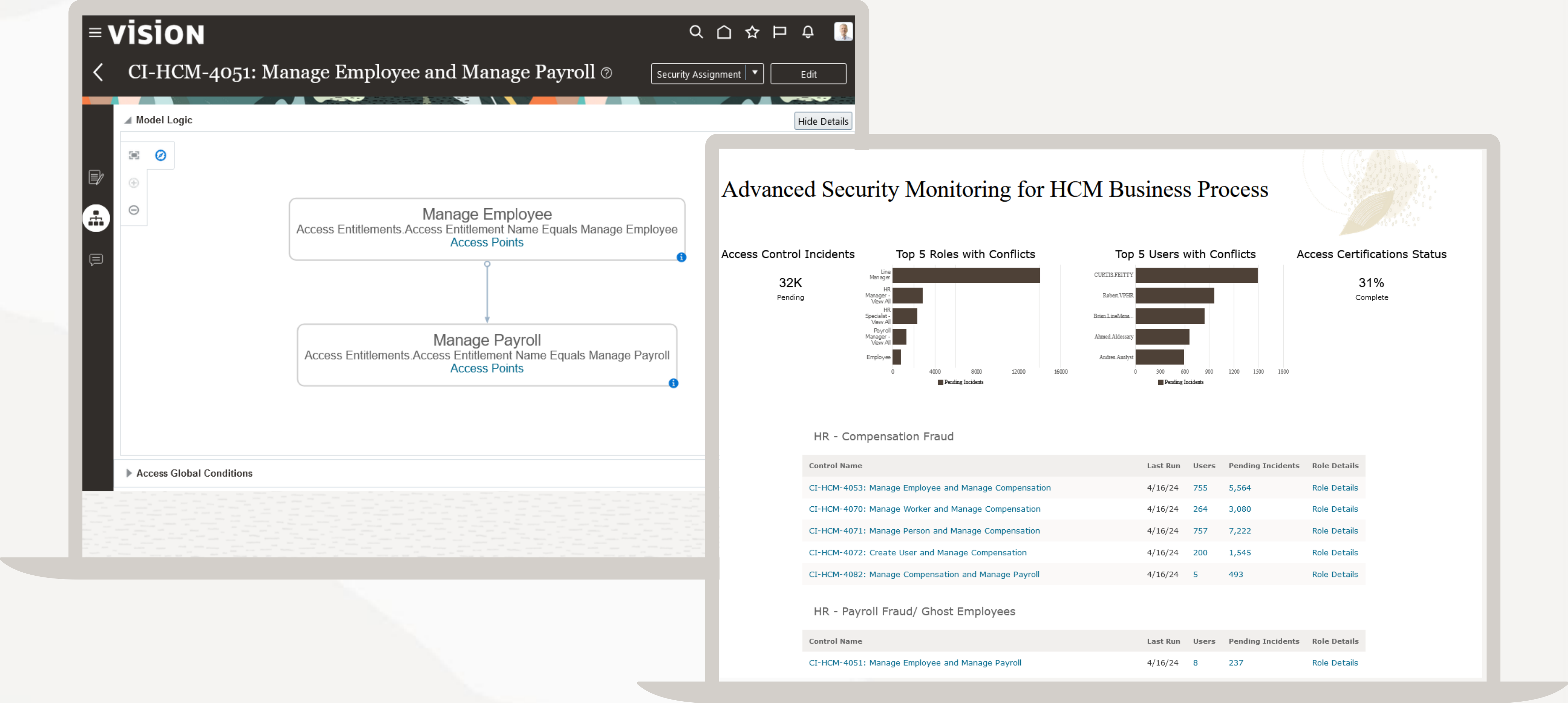
- Eliminate the need to export, copy or distribute sensitive HCM security data to third-party services. Avoid uncontrolled access and unnecessary exposure of critical and sensitive data.

Report SOD results with confidence and ease

- Rely on built-in, complete analysis of fine grain functional access. Generate compliance-driven SOD reports with confidence each quarter. Reduce audit consulting fees by over $100,000* per year.

Manage access exceptions with ease

- Monitor exceptions via dashboard and resolve issues using a simple incident workflow. Accelerate resolution of conflicts with the aid of visualizations and simulations.



CI-HCM-4051: Manage Employee and Manage Payroll

Manage Employee
Access Entitlements.Access Entitlement Name Equals Manage Employee
Access Points

Manage Payroll
Access Entitlements.Access Entitlement Name Equals Manage Payroll
Access Points

Advanced Security Monitoring for HCM Business Process

Access Control Incidents: 32K Pending

Top 5 Roles with Conflicts

Top 5 Users with Conflicts

Access Certifications Status: 31% Complete

HR - Compensation Fraud

Control Name	Last Run	Users	Pending Incidents	Role Details
CI-HCM-4053: Manage Employee and Manage Compensation	4/16/24	755	5,564	Role Details
CI-HCM-4070: Manage Worker and Manage Compensation	4/16/24	264	3,080	Role Details
CI-HCM-4071: Manage Person and Manage Compensation	4/16/24	757	7,222	Role Details
CI-HCM-4072: Create User and Manage Compensation	4/16/24	200	1,545	Role Details
CI-HCM-4082: Manage Compensation and Manage Payroll	4/16/24	5	493	Role Details

HR - Payroll Fraud/ Ghost Employees

Control Name	Last Run	Users	Pending Incidents	Role Details
CI-HCM-4051: Manage Employee and Manage Payroll	4/16/24	8	237	Role Details

* Audit firms commonly charge ~$50,000-200,000 to compile SoD reports typically done 1 to 4 times per year.

Monitor user access

Prevent SOD violations

Monitor user access

Monitor user activity

Manage Internal Controls

Monitor & Report Sensitive (Restricted) Access

Monitor & Report Separation of Duties (SOD)

Digitize user access certification workflows

Digitize user access certification workflows

Certify users' access to sensitive functions

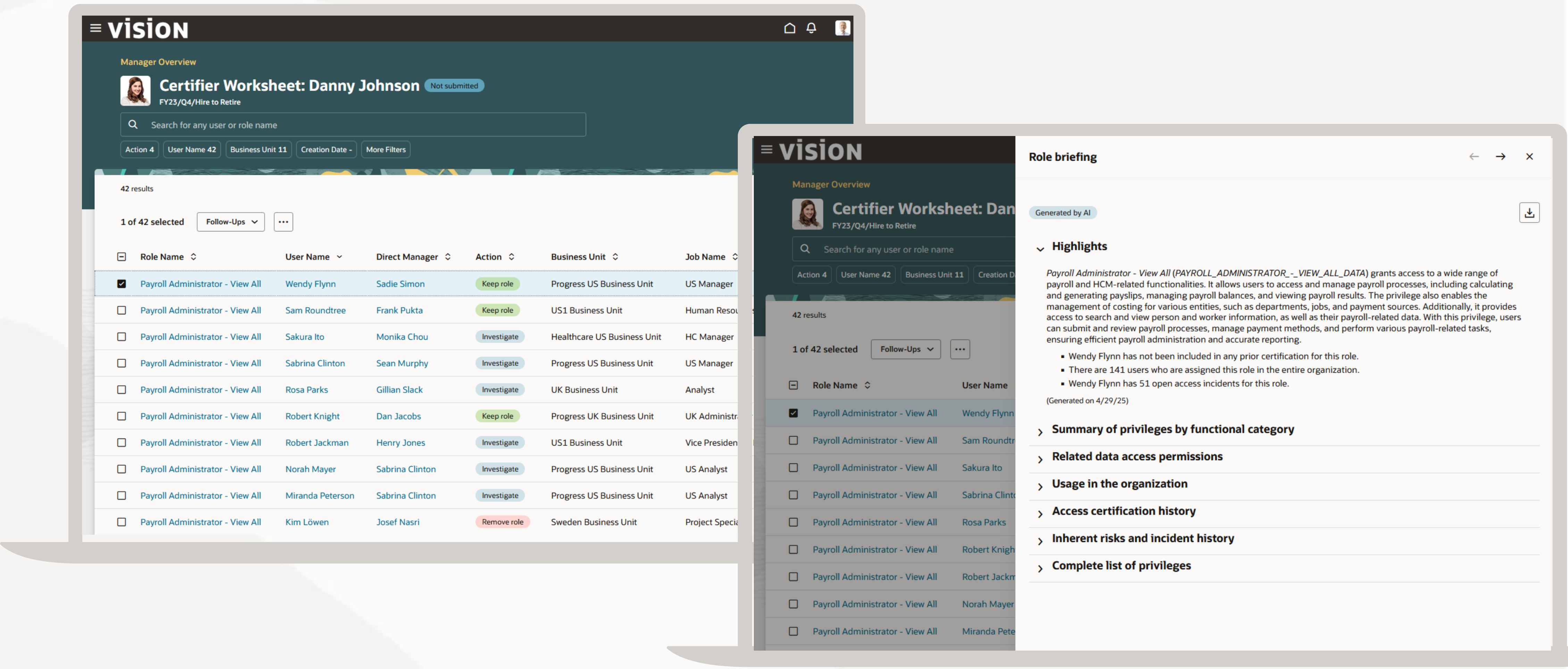
- Scope sensitive roles and ensure all users are authorized and approved. Certify users' access to sensitive data and functions, based on pre-determined audit scope and schedules. Ensures that access privileges are aligned with organizational changes & personnel moves.

Automate routing to direct manager

- Streamline workflows based on manager hierarchy and/or designated process owners. Reduce compliance fatigue and save ~250* hours of manual effort with easy-to-review worksheets.

Continuously certify new users with high-risk access

- Minimize access risk by ensuring any new user granted sensitive access is promptly reviewed and certified.



Manager Overview

Certifier Worksheet: Danny Johnson Not submitted

FY23/Q4/Hire to Retire

Search for any user or role name

42 results

1 of 42 selected Follow-Ups

⊟	Role Name	User Name	Direct Manager	Action	Business Unit	Job Name
☑	Payroll Administrator - View All	Wendy Flynn	Sadie Simon	Keep role	Progress US Business Unit	US Manager
□	Payroll Administrator - View All	Sam Roundtree	Frank Pukta	Keep role	US1 Business Unit	Human Resou
□	Payroll Administrator - View All	Sakura Ito	Monika Chou	Investigate	Healthcare US Business Unit	HC Manager
□	Payroll Administrator - View All	Sabrina Clinton	Sean Murphy	Investigate	Progress US Business Unit	US Manager
□	Payroll Administrator - View All	Rosa Parks	Gillian Slack	Investigate	UK Business Unit	Analyst
□	Payroll Administrator - View All	Robert Knight	Dan Jacobs	Keep role	Progress UK Business Unit	UK Administr
□	Payroll Administrator - View All	Robert Jackman	Henry Jones	Investigate	US1 Business Unit	Vice Presiden
□	Payroll Administrator - View All	Norah Mayer	Sabrina Clinton	Investigate	Progress US Business Unit	US Analyst
□	Payroll Administrator - View All	Miranda Peterson	Sabrina Clinton	Investigate	Progress US Business Unit	US Analyst
□	Payroll Administrator - View All	Kim Löwen	Josef Nasri	Remove role	Sweden Business Unit	Project Speci

Role briefing

Generated by AI

Highlights

Payroll Administrator - View All (*PAYROLL_ADMINISTRATOR_-_VIEW_ALL_DATA*) grants access to a wide range of payroll and HCM-related functionalities. It allows users to access and manage payroll processes, including calculating and generating payslips, managing payroll balances, and viewing payroll results. The privilege also enables the management of costing for various entities, such as departments, jobs, and payment sources. Additionally, it provides access to search and view person and worker information, as well as their payroll-related data. With this privilege, users can submit and review payroll processes, manage payment methods, and perform various payroll-related tasks, ensuring efficient payroll administration and accurate reporting.

- Wendy Flynn has not been included in any prior certification for this role.
- There are 141 users who are assigned this role in the entire organization.
- Wendy Flynn has 51 open access incidents for this role.

(Generated on 4/29/25)

Summary of privileges by functional category

Related data access permissions

Usage in the organization

Access certification history

Inherent risks and incident history

Complete list of privileges

* Compliance process – running reports, building spreadsheets, sending emails & reminders, answering questions and preparing audit reports – usually takes ~2 minutes per employee per year (x 5,000 employees = 250 hours)

Monitor user activity

Prevent SOD violations

Monitor user access

Monitor user activity

Manage Internal Controls

Monitor user activity

IT super user activity

Hire-to-Retire Assurance

Automate monitoring of changes to critical configurations.

Automate monitoring of your transactions without sampling.

Monitor user activity (configurations and transactions)

Automate risk-based analysis of setup and master data changes

- Detect breaches and evaluate risks with automated analysis of critical configuration changes across key processes such as Compensation, Payroll and Time & Labor.

Manage exceptions with ease

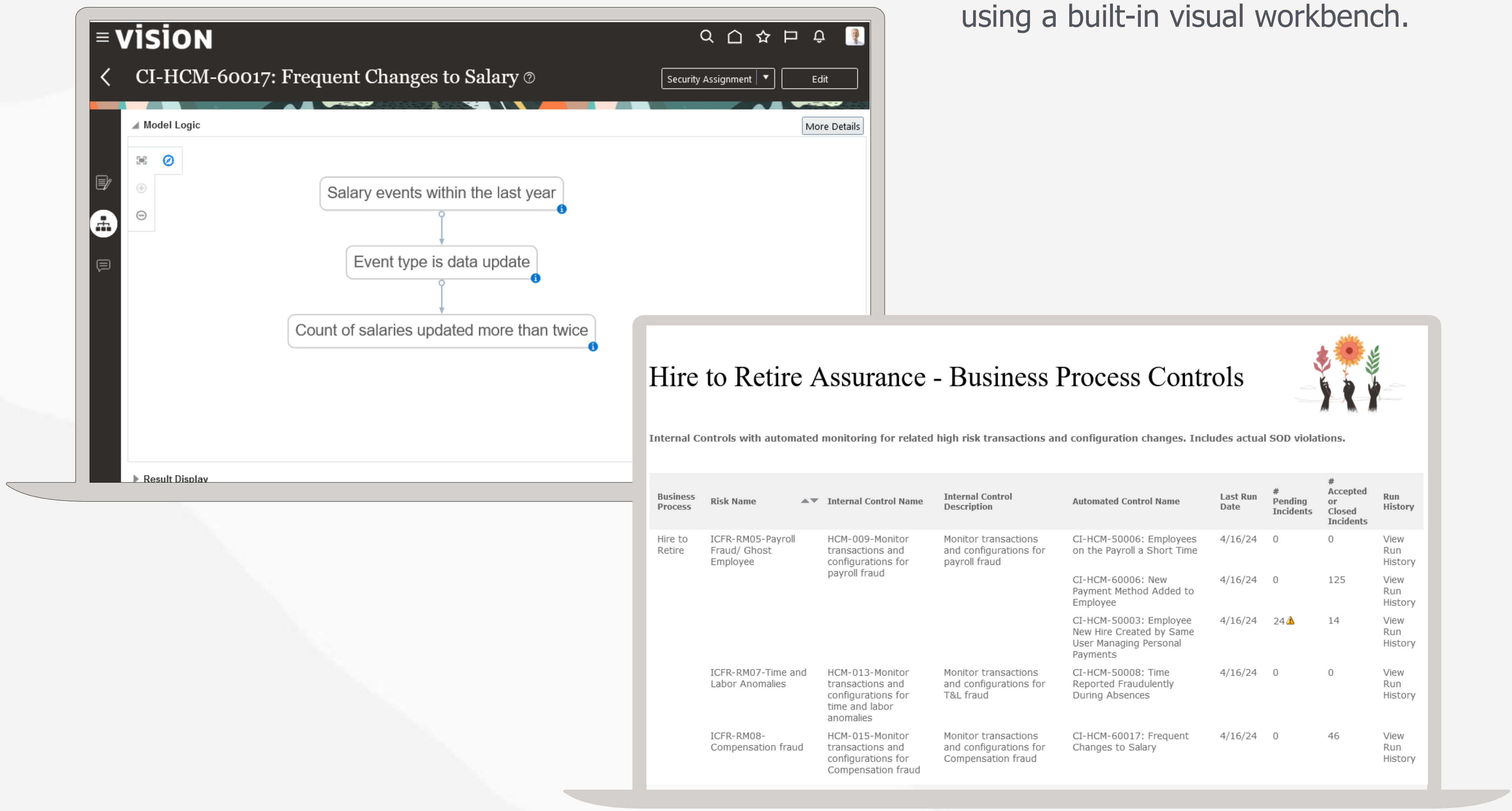
- Ensure all exceptions are routed to process owners for timely reviews (replacing emails and spreadsheets).

Analyze configurations and transactions to enforce security and privacy policies

- Continuously analyze changes and updates to critical configurations. Monitor transactions that are suspicious or violate existing policies. Evolve from sampling to continuous monitoring of HCM transactions to ensure complete oversight.

Leverage library of best-practice configuration rules

- Set up alerts for frequent changes made to employee bank accounts, payment methods, salary etc. Tailor pre-built or author new rules using a built-in visual workbench.



VISION
CI-HCM-60017: Frequent Changes to Salary
Security Assignment
Edit
Model Logic
More Details
Salary events within the last year
Event type is data update
Count of salaries updated more than twice
Result Display

Hire to Retire Assurance - Business Process Controls

Internal Controls with automated monitoring for related high risk transactions and configuration changes. Includes actual SOD violations.

Business Process	Risk Name	Internal Control Name	Internal Control Description	Automated Control Name	Last Run Date	# Pending Incidents	# Accepted or Closed Incidents	Run History
Hire to Retire	ICFR-RM05-Payroll Fraud/ Ghost Employee	HCM-009-Monitor transactions and configurations for payroll fraud	Monitor transactions and configurations for payroll fraud	CI-HCM-50006: Employees on the Payroll a Short Time	4/16/24	0	0	View Run History
				CI-HCM-60006: New Payment Method Added to Employee	4/16/24	0	125	View Run History
				CI-HCM-50003: Employee New Hire Created by Same User Managing Personal Payments	4/16/24	24⚠	14	View Run History
	ICFR-RM07-Time and Labor Anomalies	HCM-013-Monitor transactions and configurations for time and labor anomalies	Monitor transactions and configurations for T&L fraud	CI-HCM-50008: Time Reported Fraudulently During Absences	4/16/24	0	0	View Run History
	ICFR-RM08-Compensation fraud	HCM-015-Monitor transactions and configurations for Compensation fraud	Monitor transactions and configurations for Compensation fraud	CI-HCM-60017: Frequent Changes to Salary	4/16/24	0	46	View Run History

Monitor user activity

Prevent SOD violations

Monitor user access

Monitor user activity

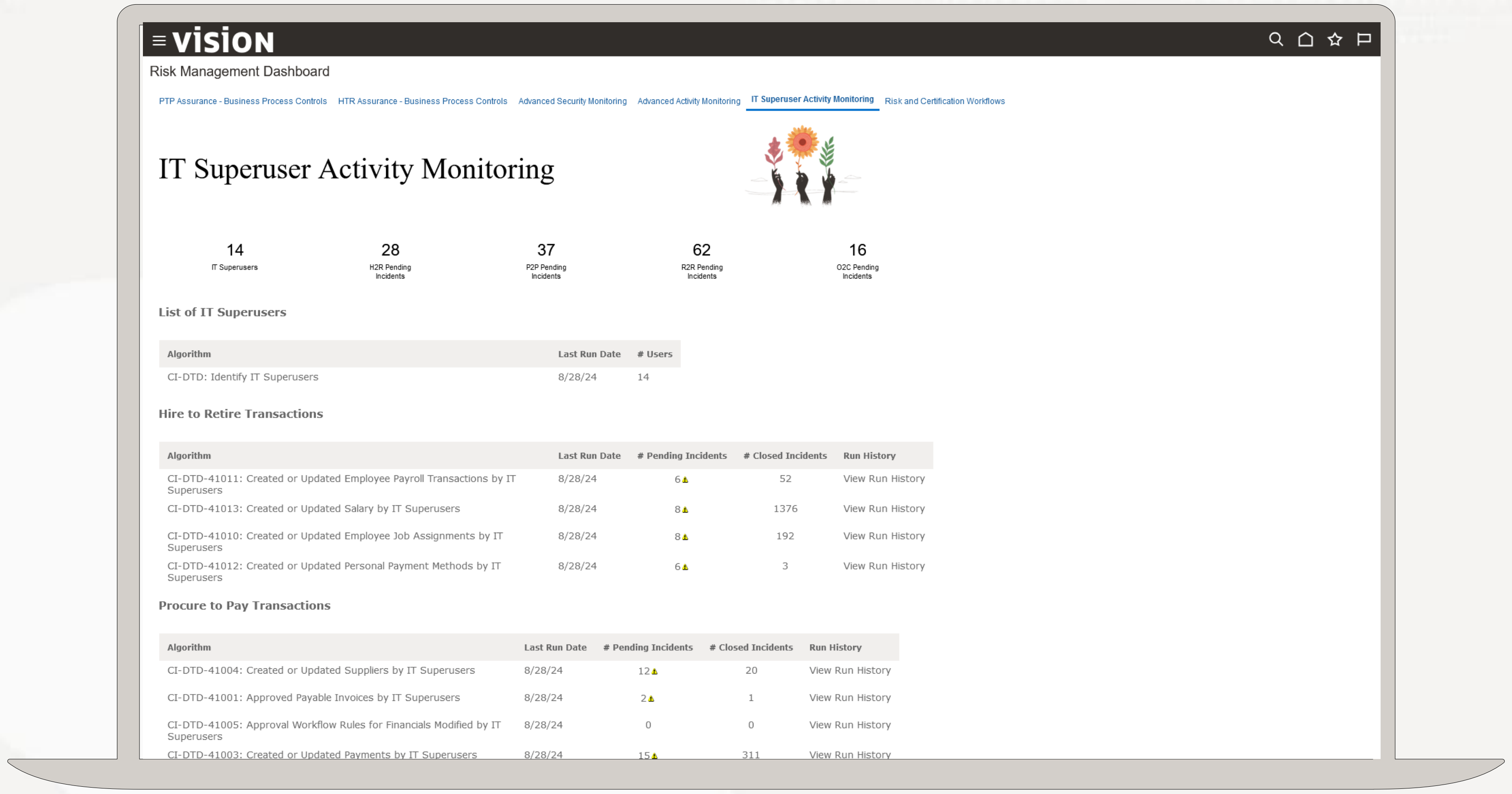
Monitor user activity

Super user monitoring

Hire-to-Retire Assurance

IT & Business Super User Monitoring

- Detect users with IT super user permissions
- Detect changes to key business transactions and master data
- Route incidents to security analysts and business owners
- Detect data breaches early



Risk Management Dashboard

PTP Assurance - Business Process Controls | HTR Assurance - Business Process Controls | Advanced Security Monitoring | Advanced Activity Monitoring | IT Superuser Activity Monitoring | Risk and Certification Workflows

IT Superuser Activity Monitoring

14	28	37	62	16
IT Superusers	H2R Pending Incidents	P2P Pending Incidents	R2R Pending Incidents	O2C Pending Incidents

List of IT Superusers

Algorithm	Last Run Date	# Users
CI-DTD: Identify IT Superusers	8/28/24	14

Hire to Retire Transactions

Algorithm	Last Run Date	# Pending Incidents	# Closed Incidents	Run History
CI-DTD-41011: Created or Updated Employee Payroll Transactions by IT Superusers	8/28/24	6⚠	52	View Run History
CI-DTD-41013: Created or Updated Salary by IT Superusers	8/28/24	8⚠	1376	View Run History
CI-DTD-41010: Created or Updated Employee Job Assignments by IT Superusers	8/28/24	8⚠	192	View Run History
CI-DTD-41012: Created or Updated Personal Payment Methods by IT Superusers	8/28/24	6⚠	3	View Run History

Procure to Pay Transactions

Algorithm	Last Run Date	# Pending Incidents	# Closed Incidents	Run History
CI-DTD-41004: Created or Updated Suppliers by IT Superusers	8/28/24	12⚠	20	View Run History
CI-DTD-41001: Approved Payable Invoices by IT Superusers	8/28/24	2⚠	1	View Run History
CI-DTD-41005: Approval Workflow Rules for Financials Modified by IT Superusers	8/28/24	0	0	View Run History
CI-DTD-41003: Created or Updated Payments by IT Superusers	8/28/24	15⚠	311	View Run History

Monitor user activity

Prevent SOD violations

Monitor user access

Monitor user activity

Manage Internal Controls

Monitor user activity

IT super user activity

Hire-to-Retire Assurance

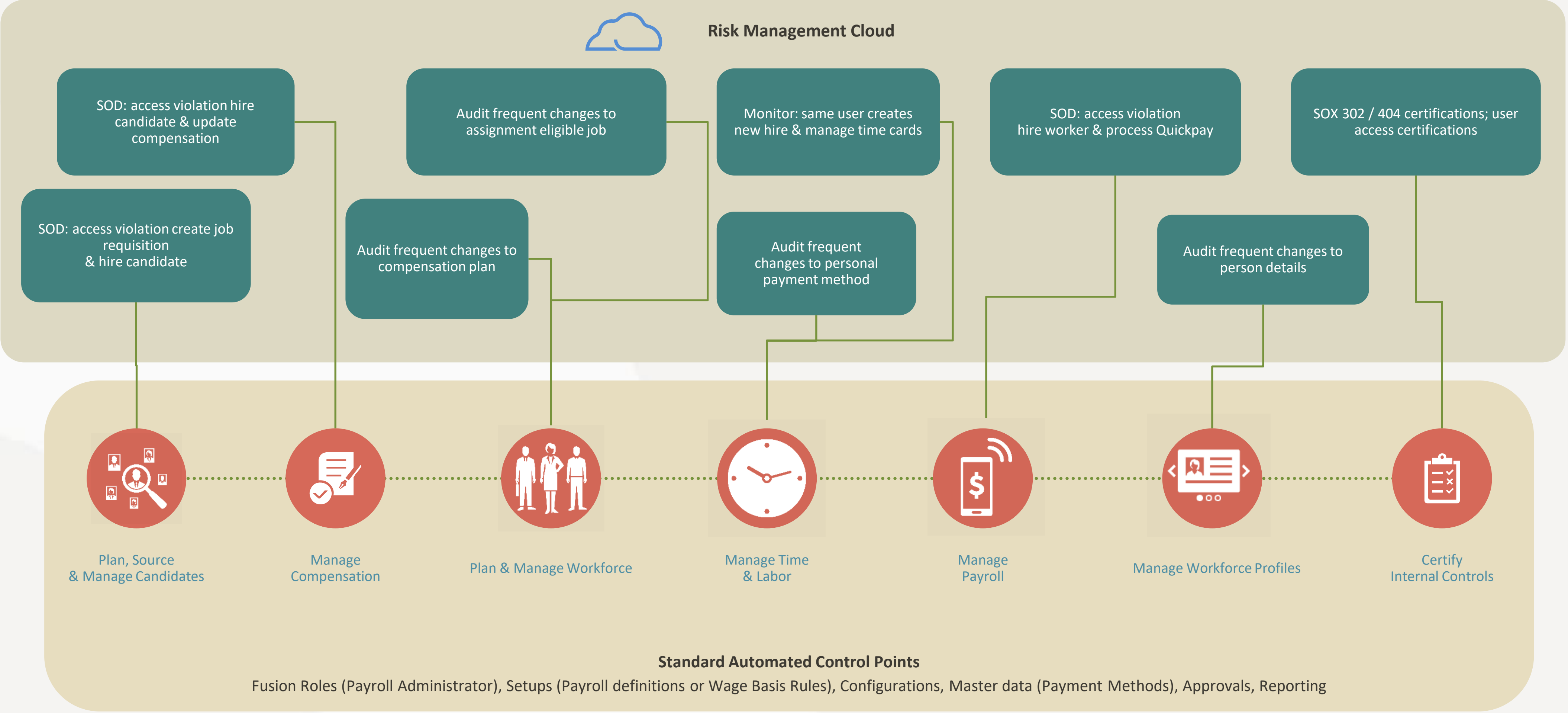
Automate monitoring of changes to critical configurations.

Automate monitoring of your transactions without sampling.

Hire-to-retire assurance

Automate monitoring of changes to critical configurations & transactions

- Audit payroll and compensation related transactions
- Control and monitor access to sensitive employee data
- Reduce exposure of sensitive data and privacy risk
- Manage exceptions with ease



Risk Management Cloud

SOD: access violation hire candidate & update compensation

SOD: access violation create job requisition & hire candidate

Audit frequent changes to assignment eligible job

Audit frequent changes to compensation plan

Monitor: same user creates new hire & manage time cards

Audit frequent changes to personal payment method

SOD: access violation hire worker & process Quickpay

Audit frequent changes to person details

SOX 302 / 404 certifications; user access certifications

Plan, Source & Manage Candidates

Manage Compensation

Plan & Manage Workforce

Manage Time & Labor

Manage Payroll

Manage Workforce Profiles

Certify Internal Controls

Standard Automated Control Points

Fusion Roles (Payroll Administrator), Setups (Payroll definitions or Wage Basis Rules), Configurations, Master data (Payment Methods), Approvals, Reporting

Overlay of **Hire-to-Retire** business process with illustrative examples of access, configuration and transaction controls.

Benefits and business value for finance, HR, IT, and security functions

Line 1

CFO / CAO / CHRO

Increase investor, lender and employee confidence with better financial, cybersecurity & privacy controls.

Increase productivity by replacing drudgery of compliance with data-driven automation.

Lower external audit fees.

Improve resilience through change (M&A etc) and disruptions (pandemic etc) with automated monitoring of operations.

Process Leaders/Control owners

Certify controls with confidence.

Provide assurance for policy compliance and authorized access.

Minimize manual effort and time spent on lower-value compliance tasks.

Prevent audit surprises and disruptions.

Line 2

Fusion IT & Cybersecurity

Provide assurance that ITGC controls for user access, configurations are effective.

Design and test roles for excessive access (both functional and data). Enforce security and access rules without adding friction to the business.

Eliminate the need for large audit data extracts and related governance.

Monitor for data breaches and configuration drift.

Financial governance/ Compliance (ICFR/SOX)/ Internal Controls

Accelerate Certification & testing cycles.

Collaborate with process owners using data-driven insights.

Standardize and automate control and governance processes.

Automate routine external audit requests.

Eliminate need for 3rd party SOD analysis.

Line 3

Internal Audit

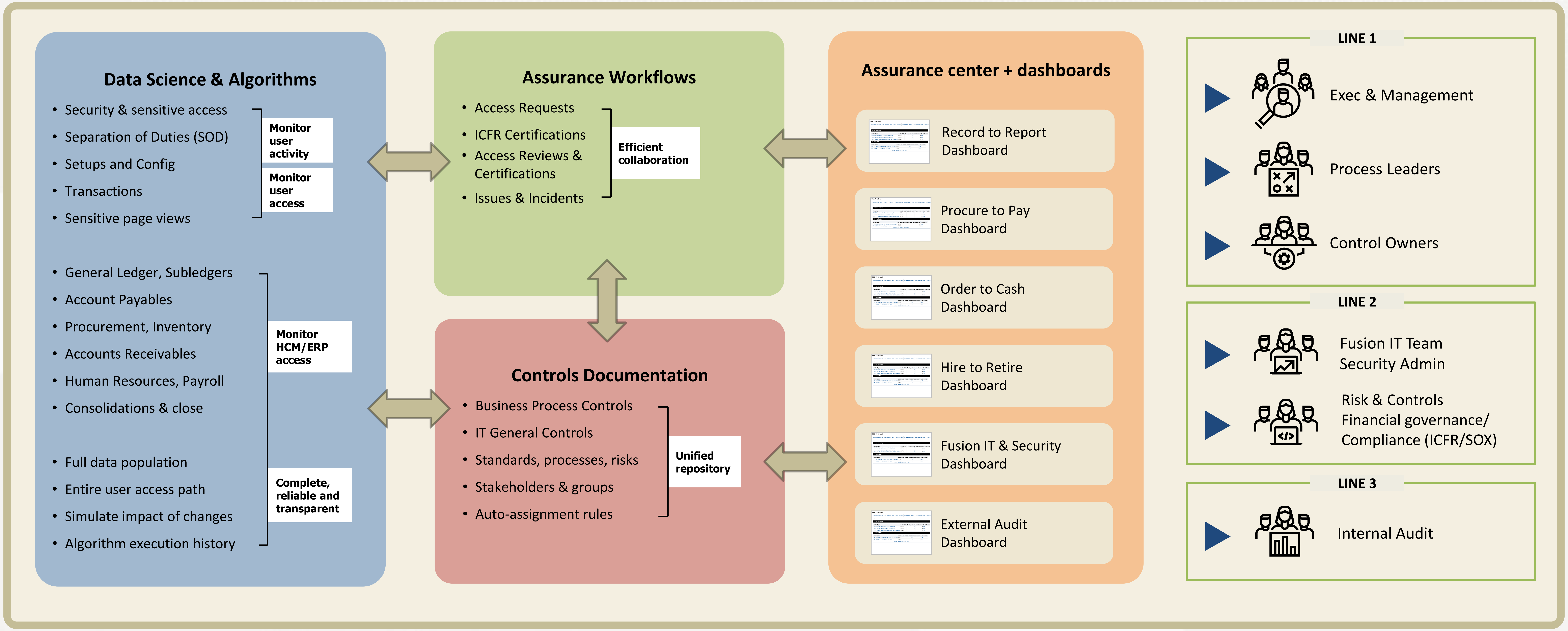
Focus on higher risk areas by automating routine data analysis & monitoring tasks.

Provide practical insights to improve operations using better analytics.

Collaborate with process owners while remaining independent.

Use automated internal controls to reduce scope and streamline external audit engagements.

Enterprise-wide Assurance Framework



Data Science & Algorithms

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

Monitor user activity

Monitor user access

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

Monitor HCM/ERP access

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

Complete, reliable and transparent

Assurance Workflows

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

Efficient collaboration

Controls Documentation

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

Unified repository

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

- Fusion IT Team Security Admin
- Risk & Controls Financial governance/ Compliance (ICFR/SOX)

LINE 3

- Internal Audit

Learn More

Request a Demo

Back to main menu