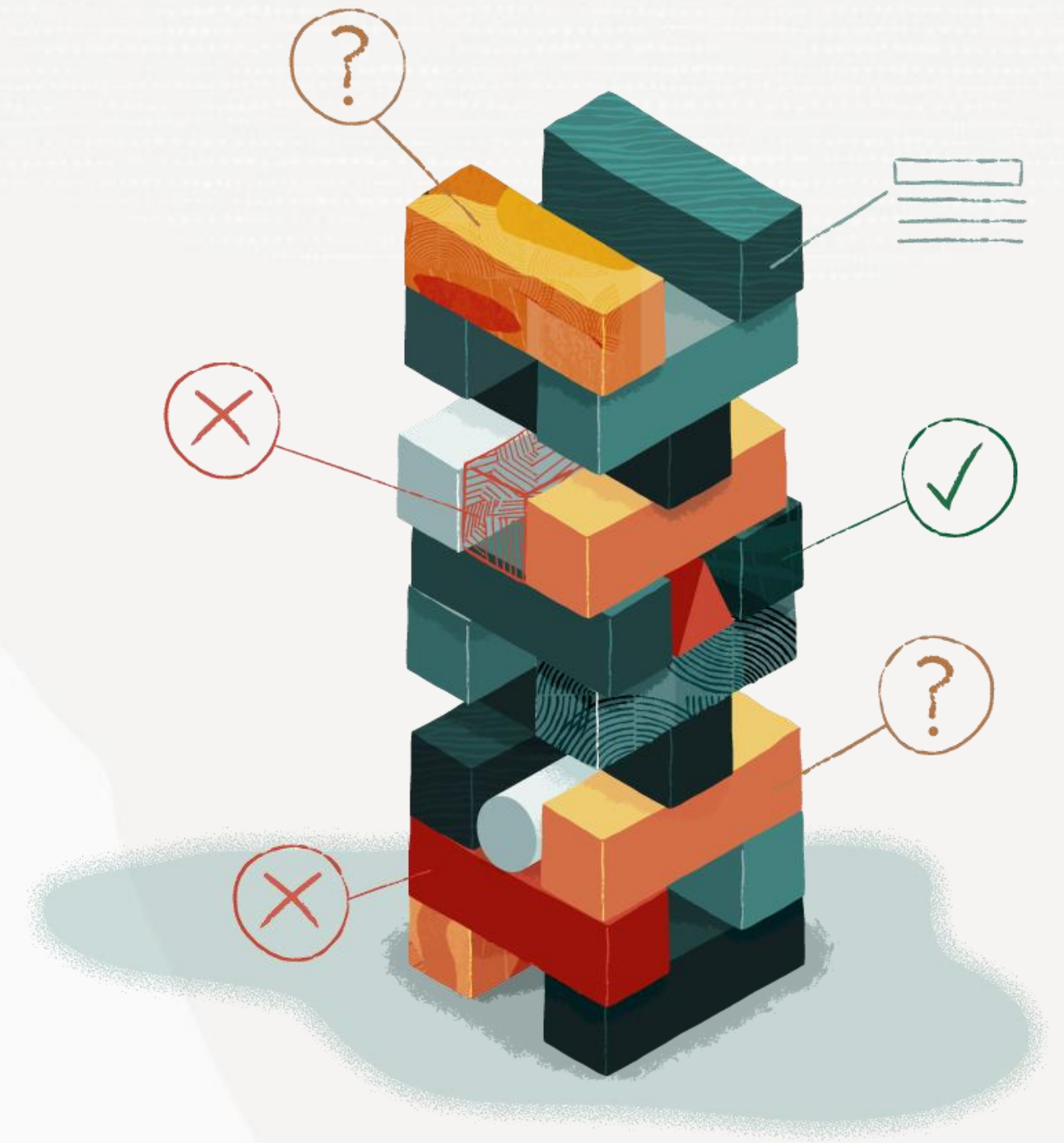ORACLE

Oracle Cloud Risk Management

A fully integrated suite within
Oracle Cloud ERP
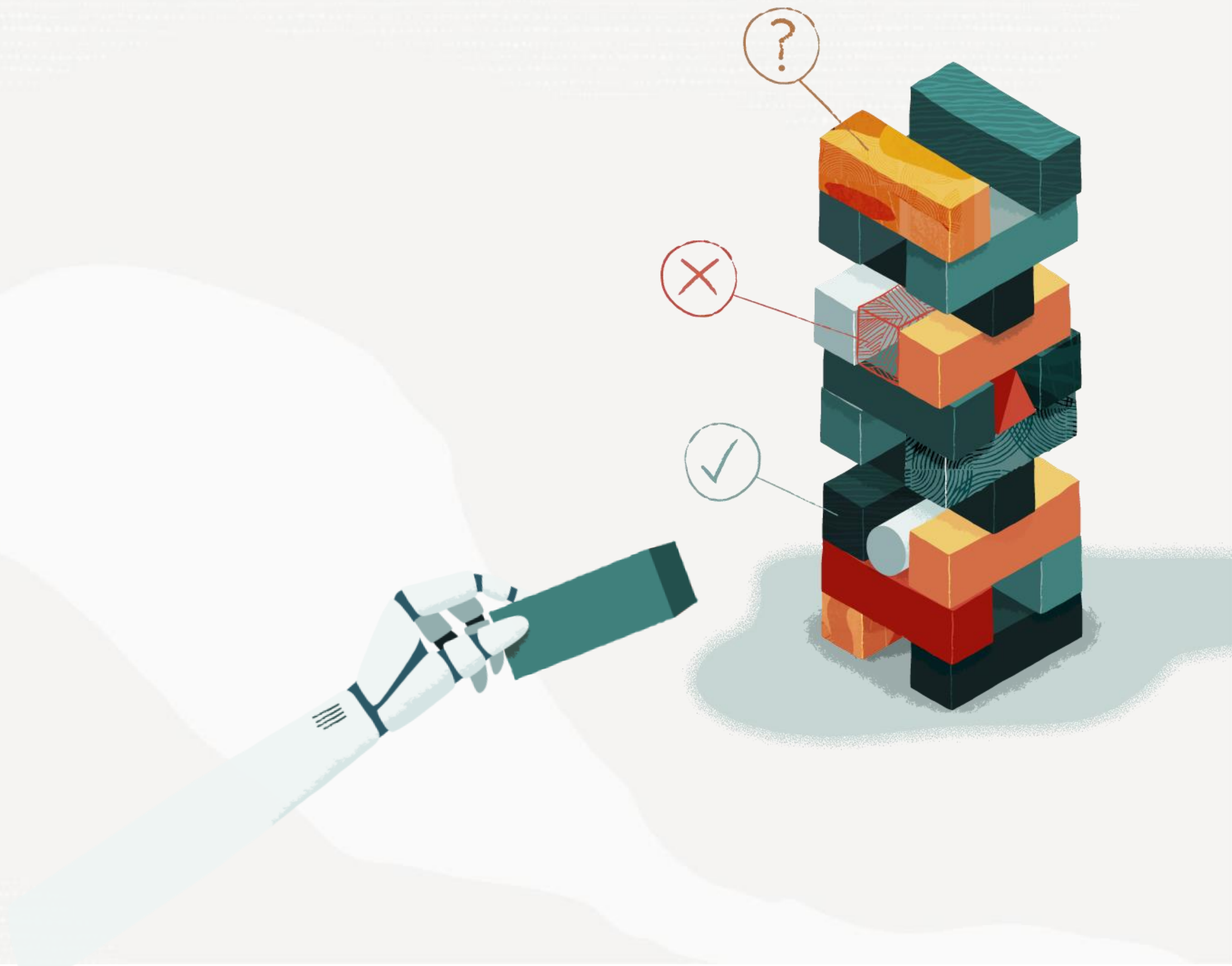
Cloud computing is fundamentally changing all business applications

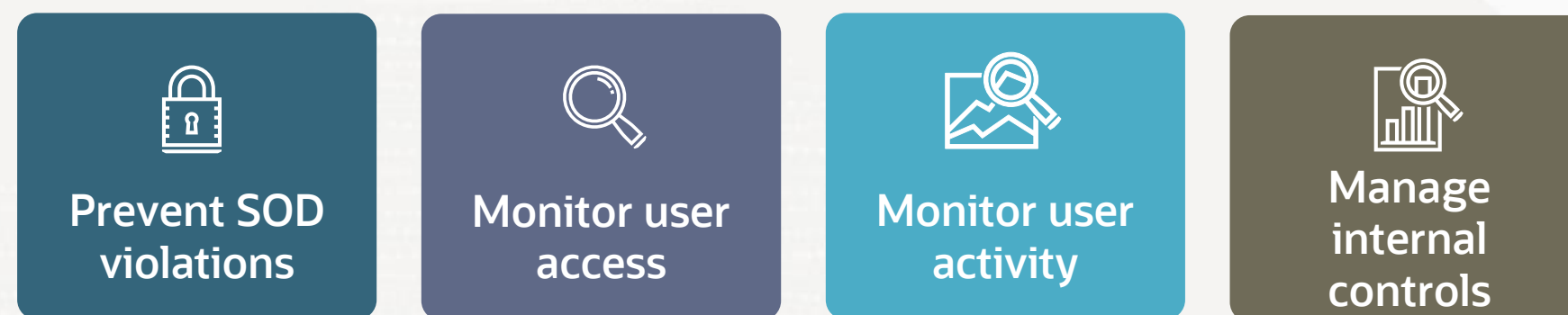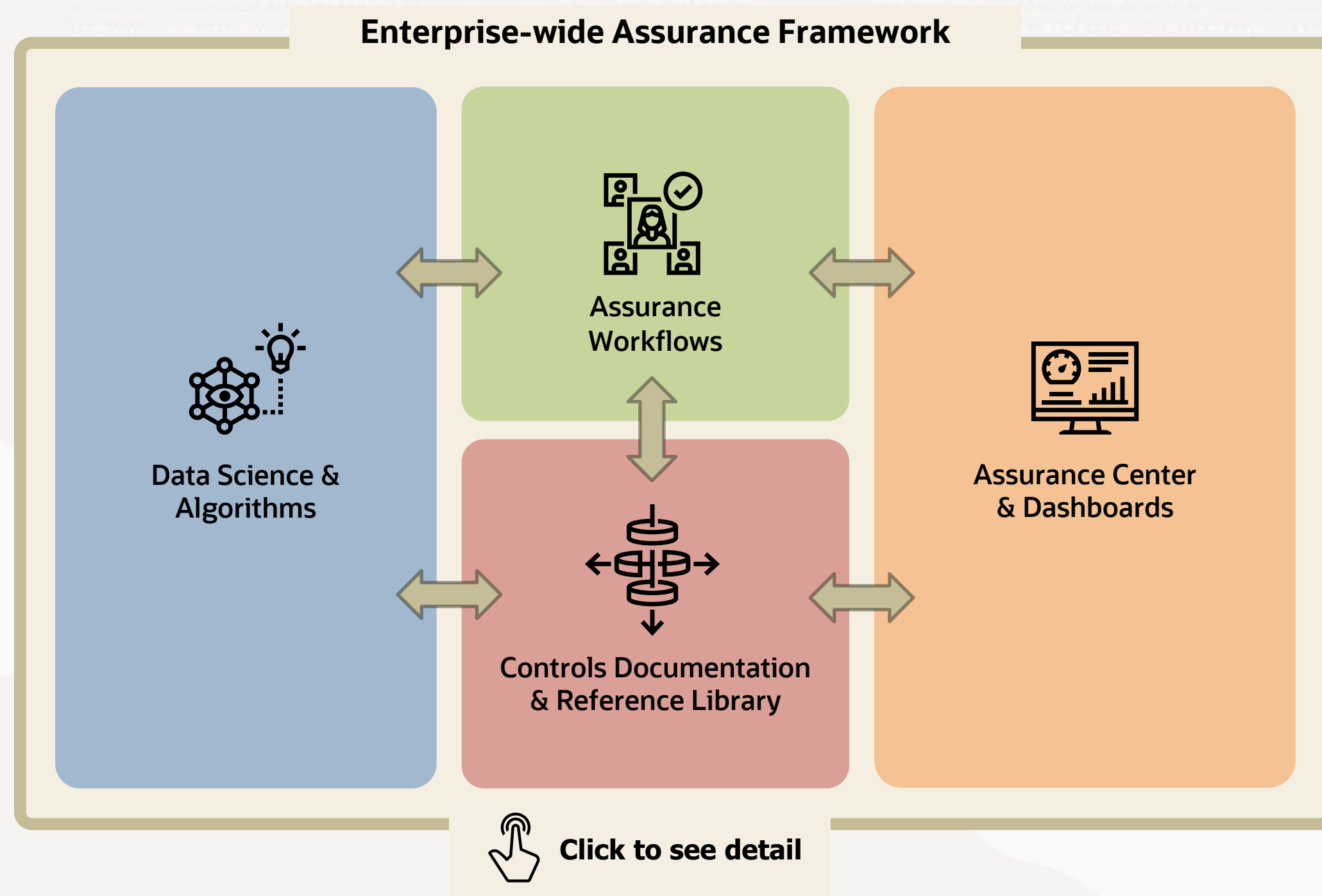## *How do we prepare for this emerging challenge?*

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.

Organizations are seizing this opportunity by embarking on ERP, Supply Chain and HCM transformations, which are often material and require a reassessment of internal controls.

Audit standards are responding to this new reality with new requirements for cyber security disclosures and data driven controls that provide objective assurance to all stakeholders.

Oracle Cloud Risk Management

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

Manage internal controls

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

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

- Embeds compliance and assurance into one solution built on data science and algorithms.

- Automates internal controls over financial reporting with AI driven monitoring of user access and activity across Oracle Fusion Cloud Applications.

- Digitizes workflows for control documentation, certification & reporting.

- Eliminates the need to transport or move data for analysis thereby delivering assurance without exposure to integration vulnerabilities.

Prevent SOD violations

Prevent SOD violations

Monitor user access

Monitor user activity

Manage Internal Controls

Design custom roles without SOD violations

Check Access Requests for SOD violations

Design Custom Roles without Separation of Duties (SOD) Violations

Accelerate ERP 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 ERP 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 100+ best-practice rules.
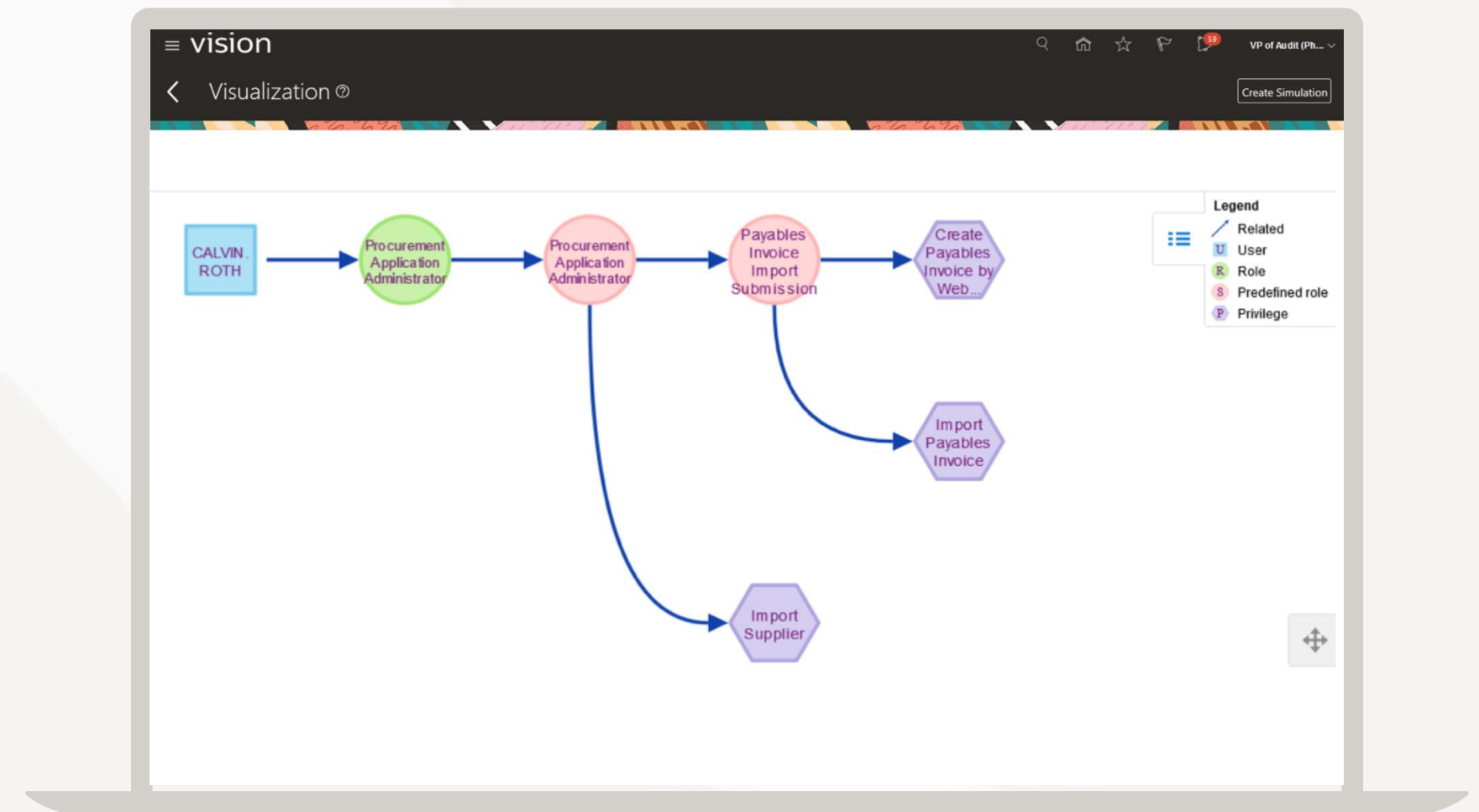
Prevent SOD violations

Prevent SOD violations

Monitor user access

Monitor user activity

Manage Internal Controls

Design custom roles without SOD violations

Check Access Requests for SOD violations

Check Access Requests for SOD violations

Enable self-service user access requests,

- Enable users to request access to ERP roles with simplified workflows. Allow system administrators to direct access requests to business process owners for their review before access is granted.

Prevent SOD conflicts while provisioning

- Review access requests for SOD conflicts, document exceptions and grant access if approved
- Analyze requests and simulate SOD conflicts before approval. You can use our APIs to inform your identity management solution with our SOD analysis results.

Submit

Review

Complete

User submits an access request *in* Cloud ERP

Analyze request with Access Controls

or

Admin assigns to reviewer

Reviewer accepts or declines risk of access request

Admin approves

Assign role & data security

Run Controls & update Incidents

Uses Fusion Risk SOD Webservices
Asynchronous Separation of Duties Simulations

Or use published Risk APIs with your current workflow (Oracle Access Governance, Jira, ServiceNow, IDM etc.)

Uses Fusion Risk Control Webservices
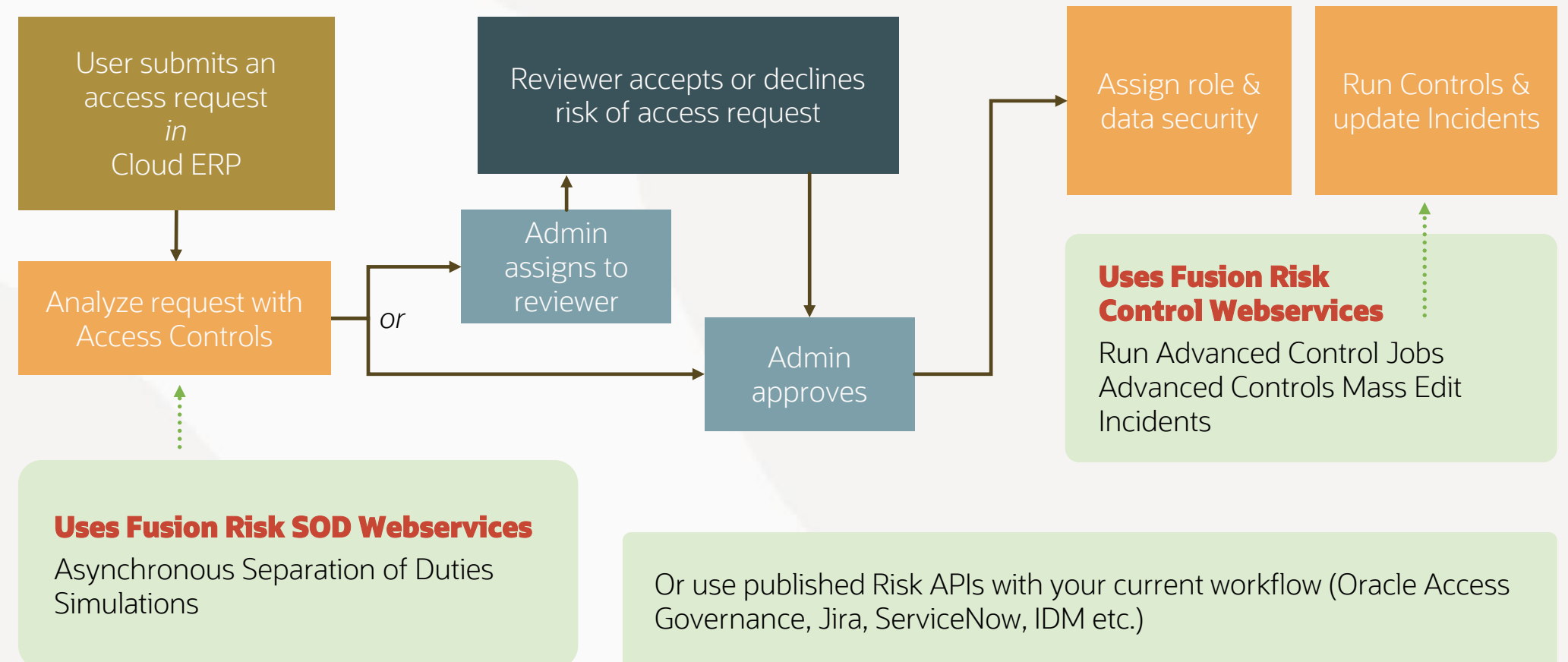Run Advanced Control Jobs Advanced Controls Mass Edit Incidents

Advanced Access Request Workflow - Provisioning with SOD Analysis

Monitor user access

Prevent SOD violations

Monitor user access

Monitor user activity

Manage Internal Controls

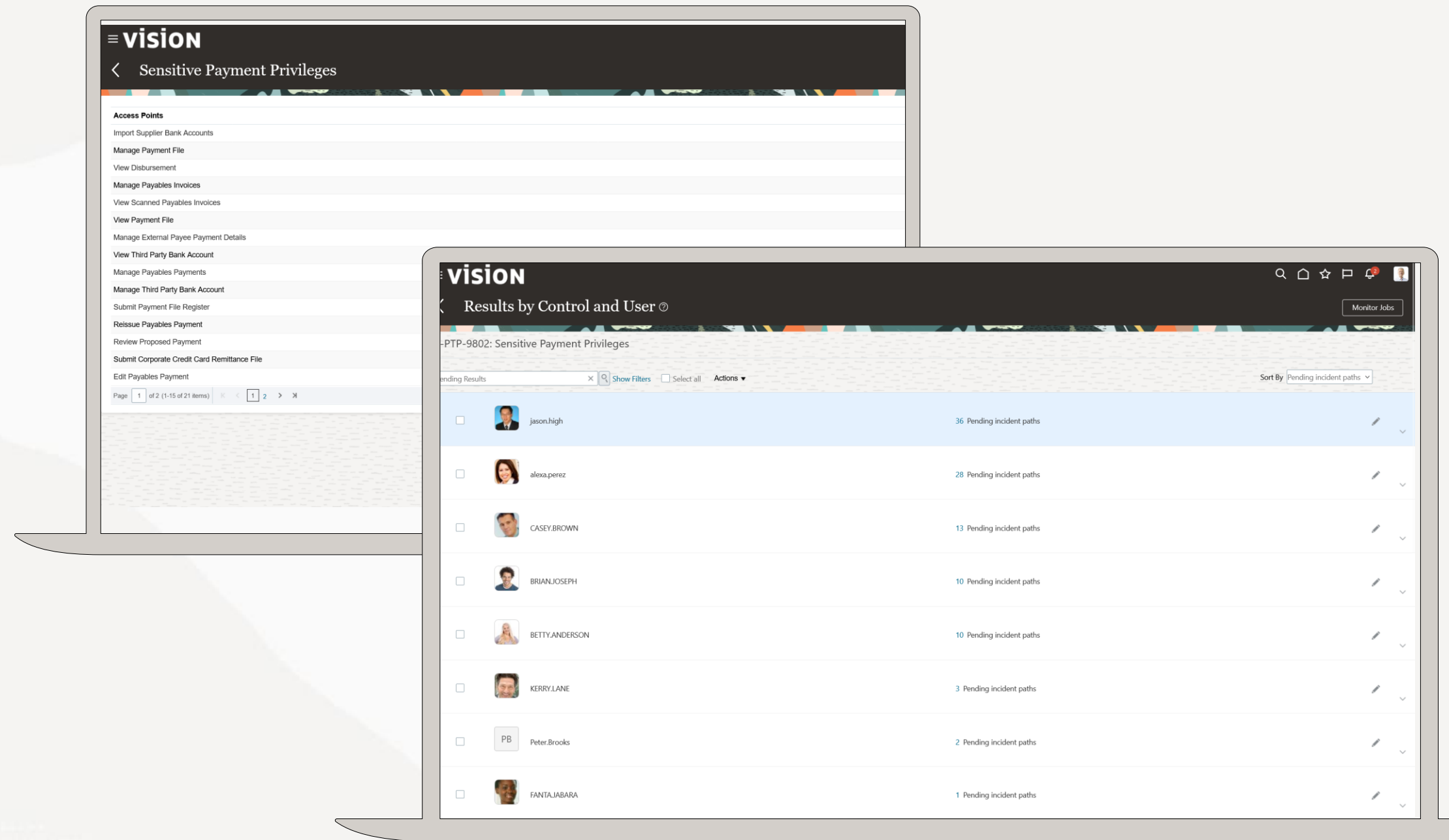Monitor & Report Sensitive (Restricted) Access

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.

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 ERP security data for 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 with data security context (BU, ledger, etc). 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.
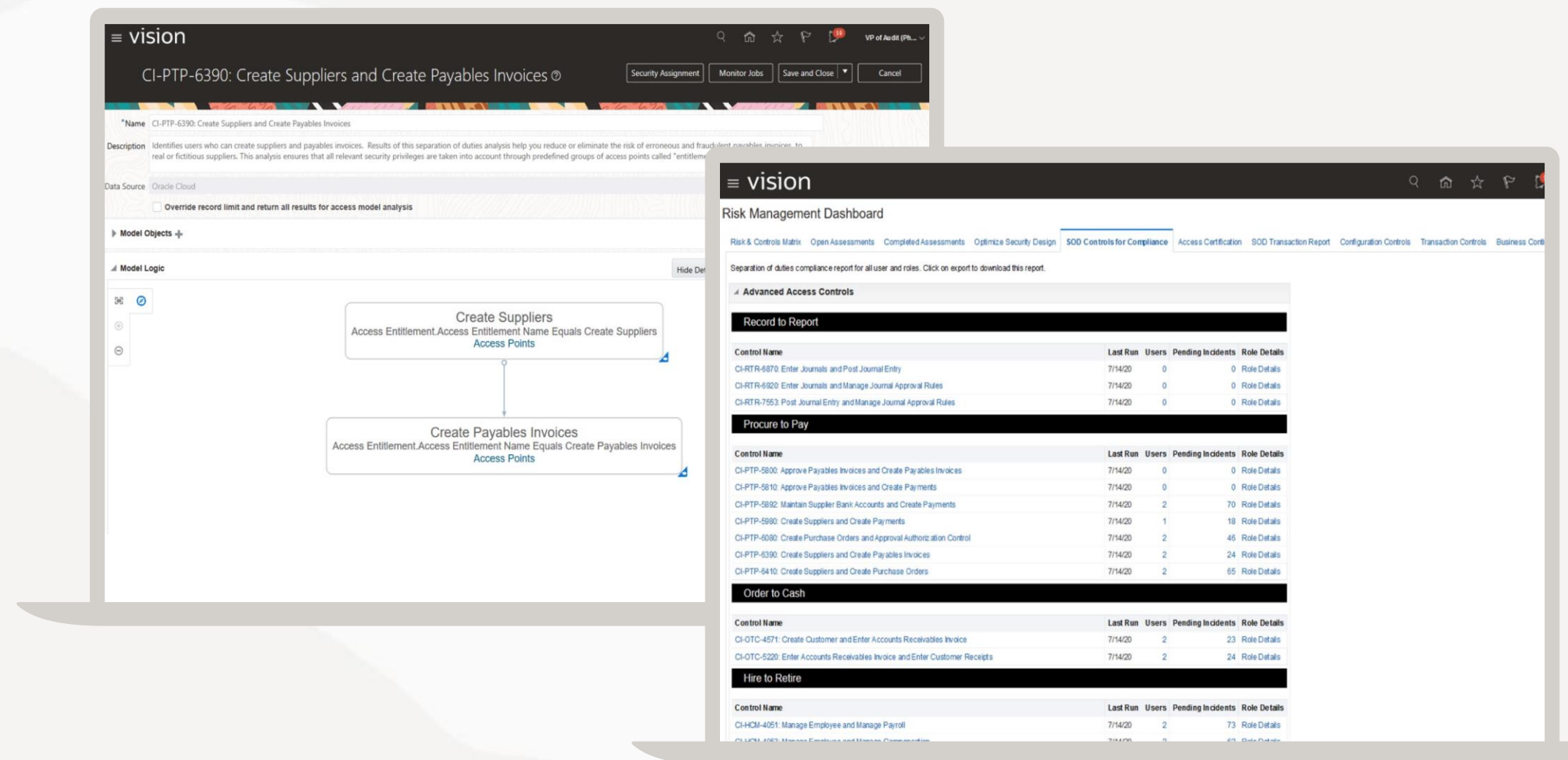
*Audit firms commonly charge ~$50,000-200,000 to compile SoD reports typically done 1 to 4 times per year.

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.

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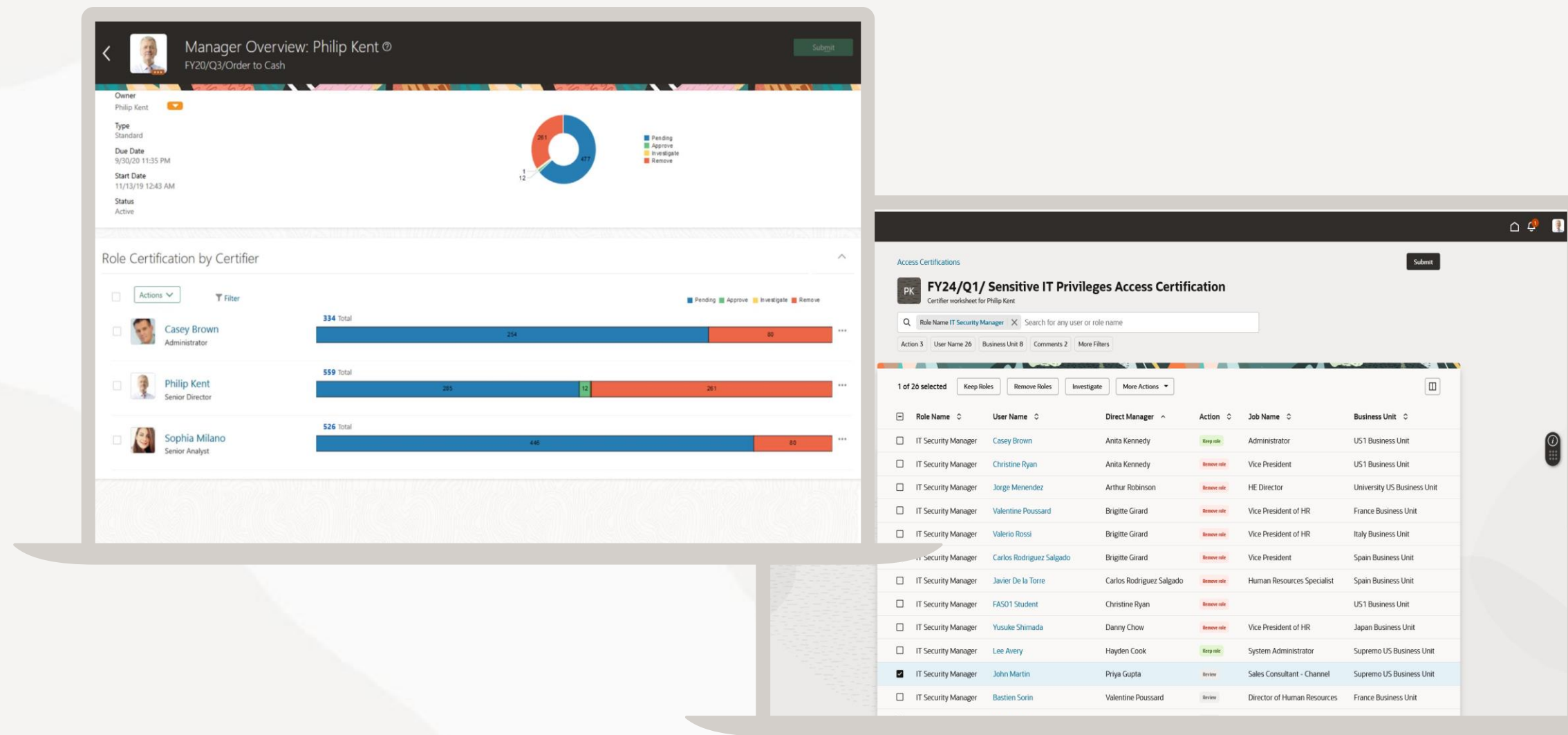
* Compliance process – running reports, building spreadsheets, sending emails & reminders, answering questions and preparing audit reports – usually takes ~2 minutes per employee per year (x 5,000 employees = 250 hours)

Monitor user activity
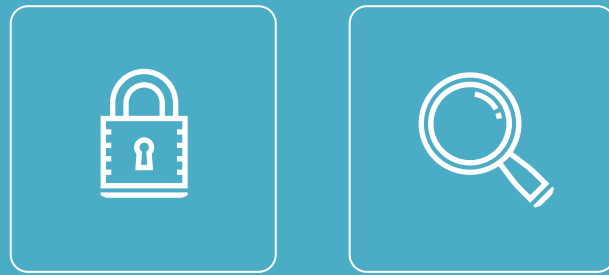
Prevent SOD violations

Monitor user access

Monitor user activity

Manage Internal Controls

Monitor user activity

IT super user activity

Procure-to-pay assurance

Record-to-Report Assurance

Order-to-Cash Assurance

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 including GL, AP, AR, PPM, expenses and procurement.

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 financial transactions to ensure complete oversight.

Leverage library of best-practice configuration rules

- Set up alerts for frequent changes made to supplier bank accounts, payment methods, item master, and/or accounting period. Tailor pre-built or author new rules using a built-in visual workbench.
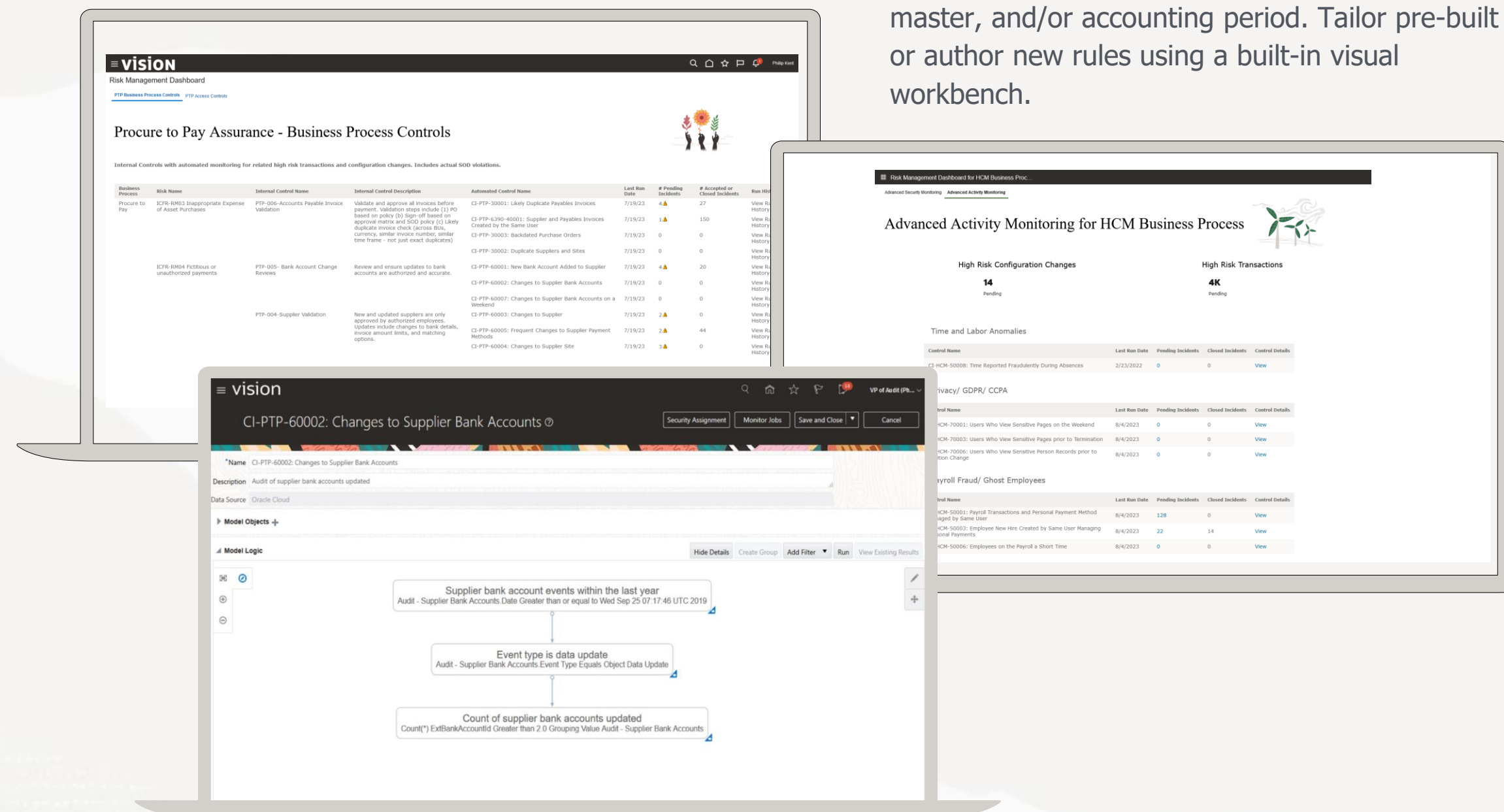
Monitor user activity

Prevent SOD violations

Monitor user access

Monitor user activity

Manage Internal Controls

Monitor user activity

IT Super User Activity
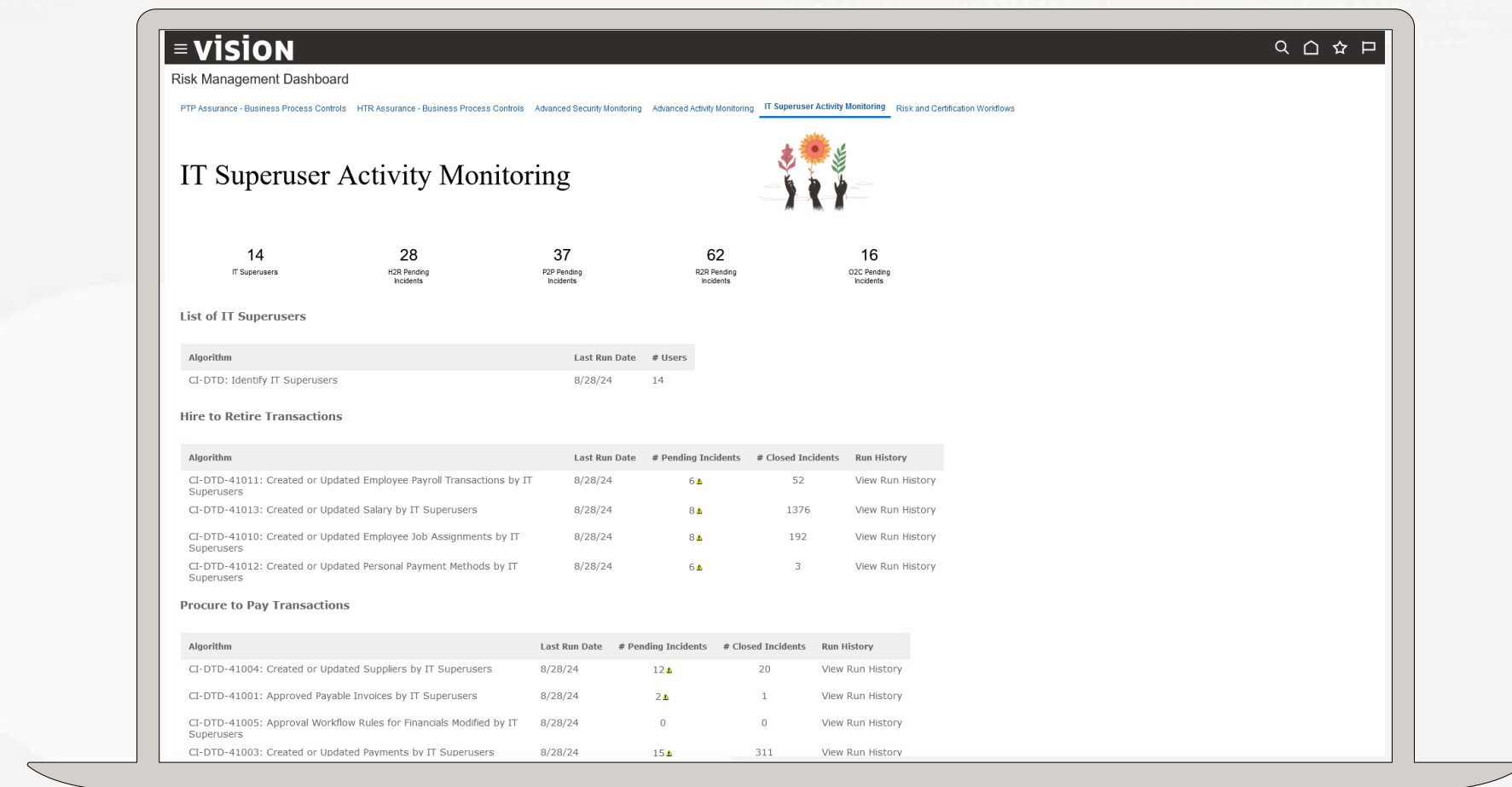
Procure-to-pay assurance
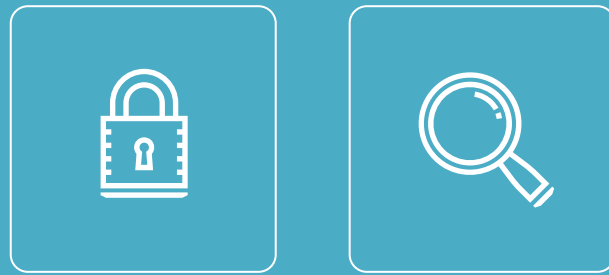
Record-to-Report Assurance

Order-to-Cash Assurance

Hire-to-Retire Assurance

IT 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

Monitor user activity

Prevent SOD violations

Monitor user access

Monitor user activity

Manage Internal Controls

Monitor user activity

IT super user activity

Procure-to-pay assurance

Record-to-Report Assurance
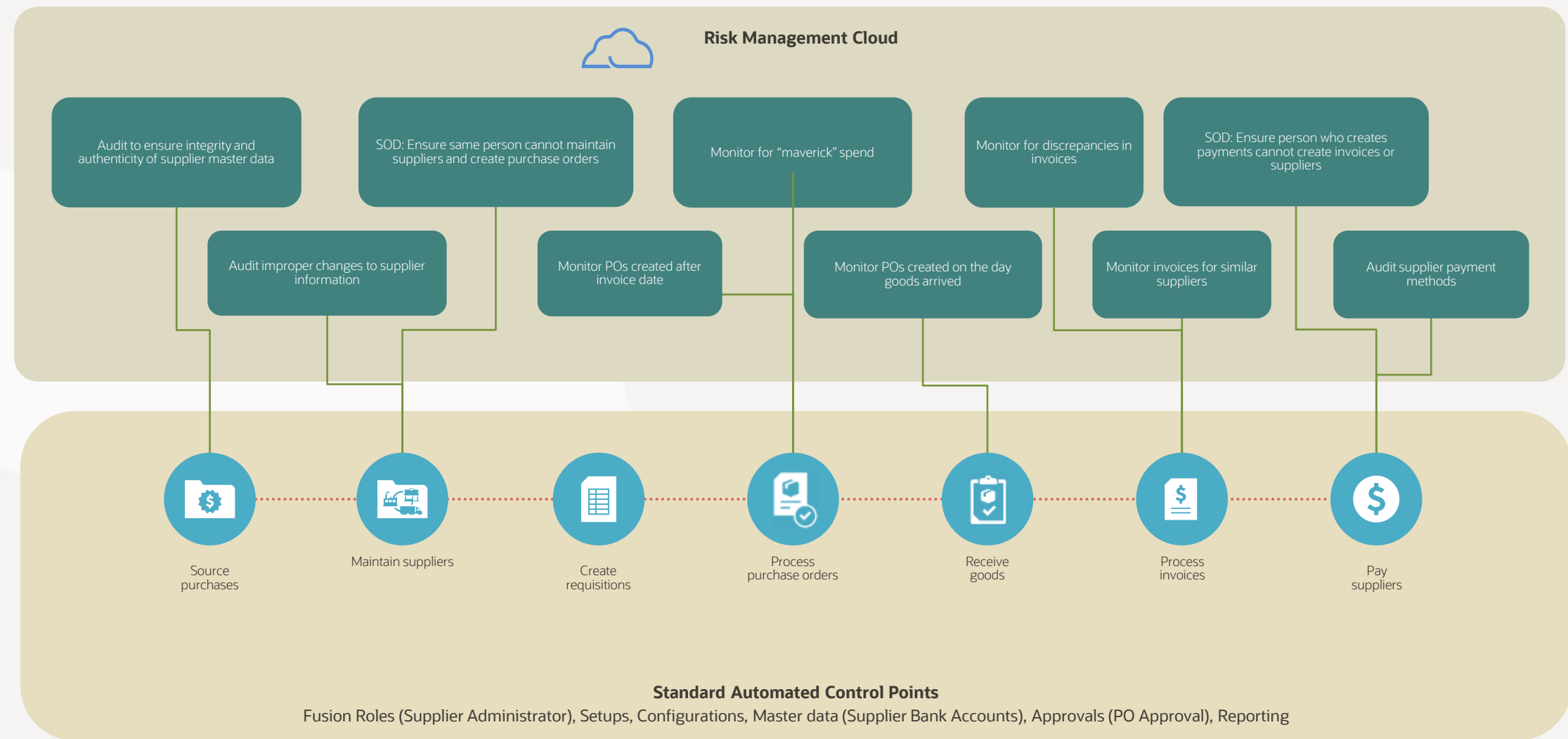
Order-to-Cash Assurance

Hire-to-Retire Assurance

Automate monitoring of changes to critical configurations.

Automate monitoring of your transactions without sampling.

Procure-to-pay assurance

Automate monitoring of changes to critical configurations and transactions

- Audit payment related transactions

- Eliminate exposure and loss of sensitive data

- Detect and prevent fraudulent payments

- Stop significant cash loss

- Manage exceptions with ease

Risk Management Cloud

Audit to ensure integrity and authenticity of supplier master data

SOD: Ensure same person cannot maintain suppliers and create purchase orders

Monitor for "maverick" spend

Monitor for discrepancies in invoices

SOD: Ensure person who creates payments cannot create invoices or suppliers

Audit improper changes to supplier information

Monitor POs created after invoice date

Monitor POs created on the day goods arrived

Monitor invoices for similar suppliers

Audit supplier payment methods

Source purchases

Maintain suppliers

Create requisitions

Process purchase orders

Receive goods

Process invoices

Pay suppliers

Standard Automated Control Points
Fusion Roles (Supplier Administrator), Setups, Configurations, Master data (Supplier Bank Accounts), Approvals (PO Approval), Reporting

Overlay of **Procure-to-Pay** business process with illustrative examples of access, configuration and transaction controls

Monitor user activity

Record-to-report assurance

Automate monitoring of changes to critical configurations & transactions

- Audit all financial transactions
- Monitor unusual activities and prevent errors
- Manage exceptions with ease
- Ensure accurate reporting to protect financial integrity

Prevent SOD violations

Monitor user access

Monitor user activity

Manage Internal Controls

Monitor user activity

IT super user activity

Procure-to-pay assurance

Record-to-Report Assurance

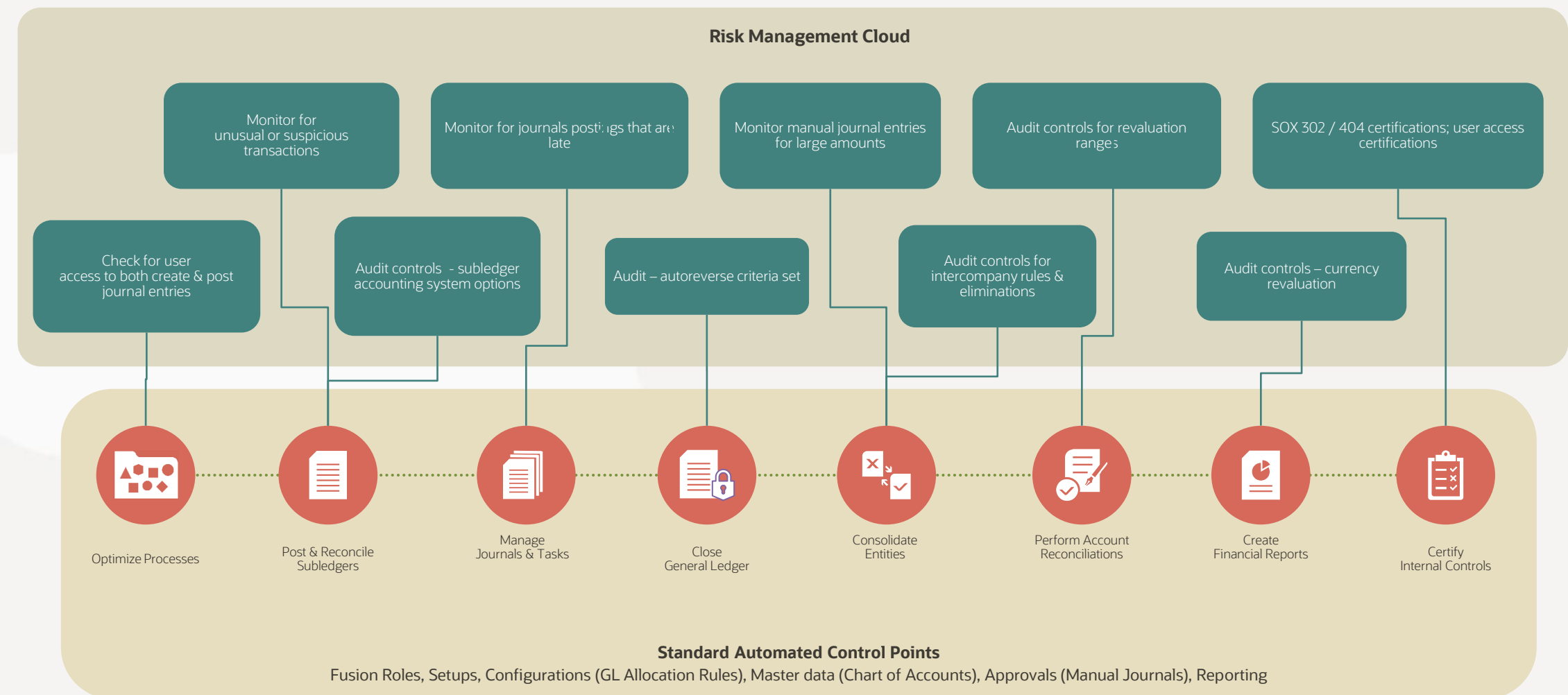Order-to-Cash Assurance

Hire-to-Retire Assurance

Automate monitoring of changes to critical configurations.

Automate monitoring of your transactions without sampling.

Risk Management Cloud

Monitor for unusual or suspicious transactions

Monitor for journals postings that are late

Monitor manual journal entries for large amounts

Audit controls for revaluation ranges

SOX 302 / 404 certifications; user access certifications

Check for user access to both create & post journal entries

Audit controls - subledger accounting system options

Audit – autoreverse criteria set

Audit controls for intercompany rules & eliminations

Audit controls – currency revaluation

Optimize Processes

Post & Reconcile Subledgers

Manage Journals & Tasks

Close General Ledger

Consolidate Entities

Perform Account Reconciliations

Create Financial Reports

Certify Internal Controls

Standard Automated Control Points
Fusion Roles, Setups, Configurations (GL Allocation Rules), Master data (Chart of Accounts), Approvals (Manual Journals), Reporting

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

Monitor user activity

Prevent SOD violations

Monitor user access

Monitor user activity

Manage Internal Controls

Monitor user activity

IT super user activity

Procure-to-pay assurance

Record-to-Report Assurance
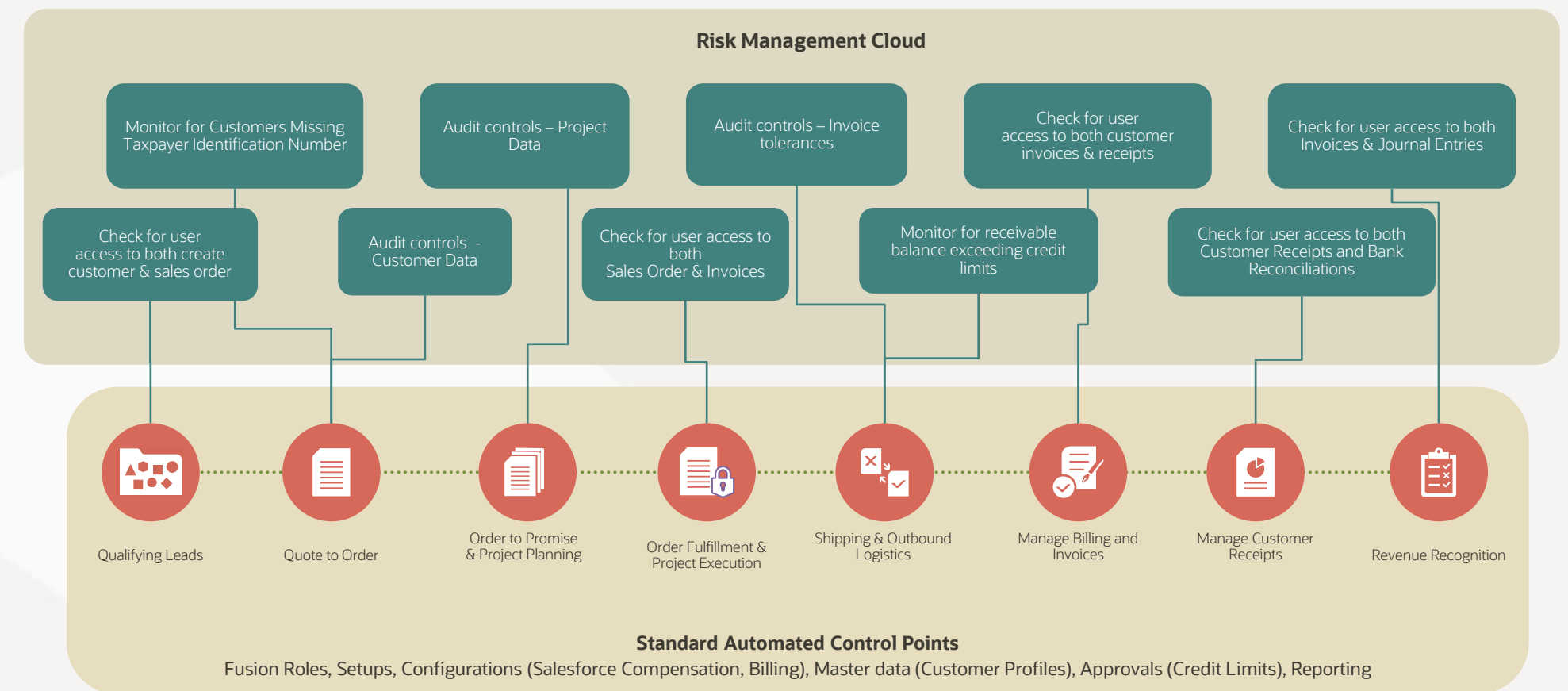
Order-to-Cash Assurance

Hire-to-Retire Assurance

Automate monitoring of changes to critical configurations.

Automate monitoring of your transactions without sampling.
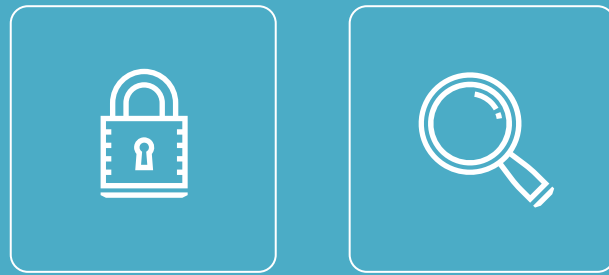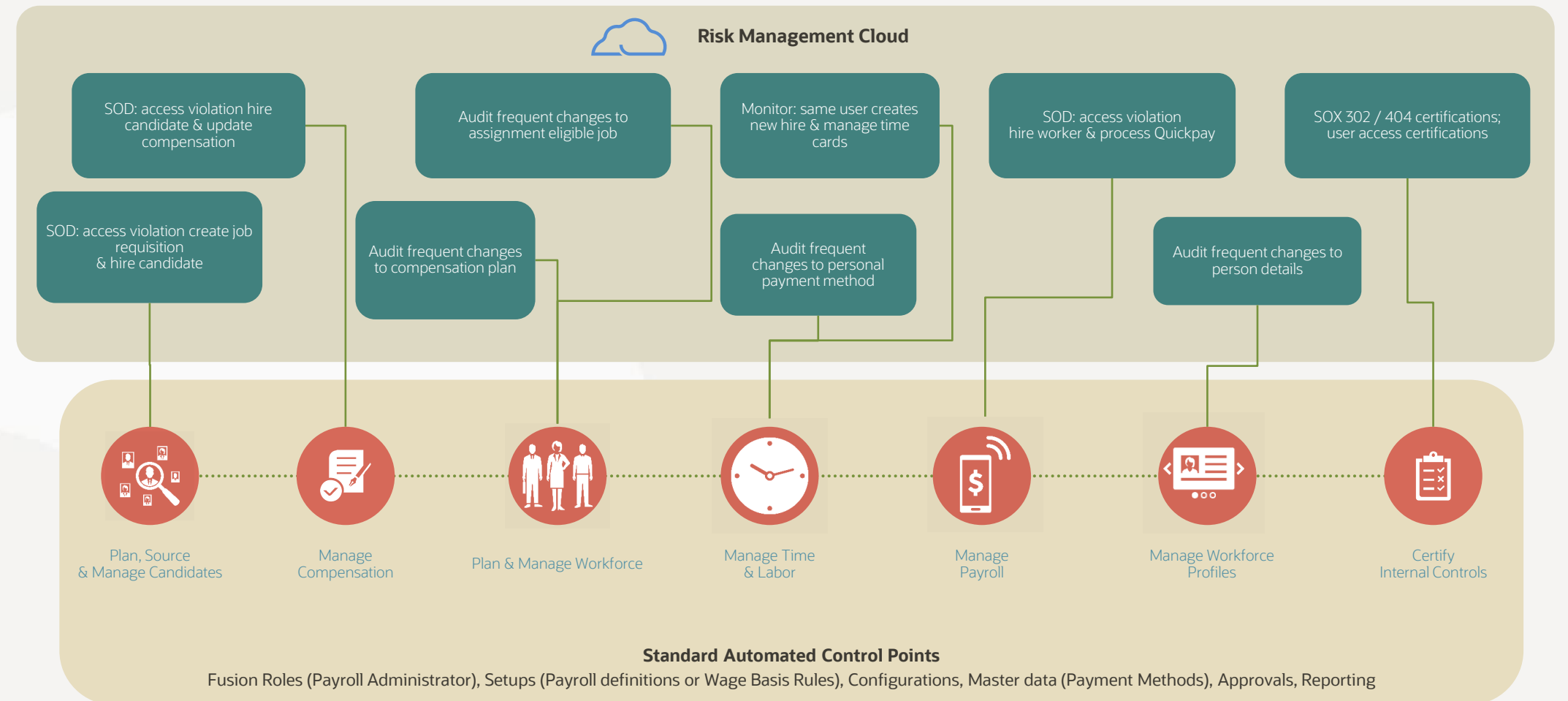
Order-to-cash assurance

Automate monitoring of changes to critical configurations & transactions

- Audit receivables transactions
- Monitor cash and receipts
- Manage exceptions with ease
- Monitor and eliminate revenue losses

Risk Management Cloud

| Monitor for Customers Missing Taxpayer Identification Number | Audit controls – Project Data | Audit controls – Invoice tolerances | Check for user access to both customer invoices & receipts | Check for user access to both Invoices & Journal Entries |

| Check for user access to both create customer & sales order | Audit controls - Customer Data | Check for user access to both Sales Order & Invoices | Monitor for receivable balance exceeding credit limits | Check for user access to both Customer Receipts and Bank Reconciliations |

Qualifying Leads | Quote to Order | Order to Promise & Project Planning | Order Fulfillment & Project Execution | Shipping & Outbound Logistics | Manage Billing and Invoices | Manage Customer Receipts | Revenue Recognition

Standard Automated Control Points
Fusion Roles, Setups, Configurations (Salesforce Compensation, Billing), Master data (Customer Profiles), Approvals (Credit Limits), Reporting

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

Monitor user activity

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

Prevent SOD violations

Monitor user access

Monitor user activity

Manage Internal Controls

Monitor user activity

IT super user activity

Procure-to-pay assurance

Record-to-Report Assurance

Order-to-Cash Assurance

Hire-to-Retire Assurance

Automate monitoring of changes to critical configurations.

Automate monitoring of your transactions without sampling.

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.

Manage Internal Controls

Manage Internal Controls

Document (RCM), Test & Certify Controls (ICFR/SOX)

- Collaborate efficiently and effectively to design, document and assess internal controls, using a risk based approach and a unified repository for your internal controls.

- Certify Internal Controls over Financial Reporting (ICFR/SOX)

- Ensure strong internal controls and audit readiness. Automate periodic testing and certification of controls with intuitive workflows.

Prevent SOD violations

Monitor user access

Monitor user activity

Manage Internal Controls

Simplify audits and assessments

Report and track compliance issues

Build trust and transparency with embedded dashboards

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

Line 1

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.

Process Leaders/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.

Line 2

Fusion IT Team 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.

Risk & Controls /Financial governance/ Compliance (ICFR/SOX)

Faster certification and testing cycles.

Enhance relationships with process owners with 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.

Easier collaboration with process owners while remaining independent.

Helps manage scope and streamlines negotiations of external audit engagements with reliance on automated internal controls.

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

Back to main menu