

Automate monitoring and control of user access

Design custom roles without separation of duties (SoD) violations (critical during ERP implementation)

Proactive and risk-aware security design helps avoid costly User Acceptance Testing (UAT) delays and audit findings, eliminating the need for expensive post-go-live role remediation. Poorly designed or generic (seeded) roles are the leading cause of these issues. Automate privilege-level security analysis to assist with configuration of custom roles to avoid ERP implementation delays and expensive security rework. Leverage a library of prebuilt security rules and use an intuitive workbench to visualize conflicts, simulate remediation and design custom roles without inherent risk.

Check access requests for SoD violations.

Enable users to submit self-service access requests, while allowing IT Admins to identify, review and prevent SoD conflicts prior to provisioning access, using AI driven insights. Route access requests to business process owners for approval, document exceptions, and grant access where appropriate. Provide time bound elevated access for critical situations, with complete audit trail of approvals.

Monitor and report sensitive (restricted) access.

Identify users with access to sensitive privileges and data, and take action to report, certify, or remove access as needed. Continuously monitor access to sensitive privileges (e.g. payments, payroll) and sensitive data (e.g. privacy, data protection). Also refer to Cybersecurity capabilities listed above.

Monitor and report separation of duties.

Effective SOD enforcement requires detailed analysis of all privileges and data accessible to each user. Oracle Risk Management uses AI to scan thousands of access paths and access privileges. Continuously monitor access policies across your ERP life cycle – from onboarding to roles changes and new role design. Generate audit ready SoD reports to support audit and ICFR compliance requirements such as SOX. RMC is the only solution that combines analysis of user access at the most granular level and monitoring of all transactions for complete assurance.

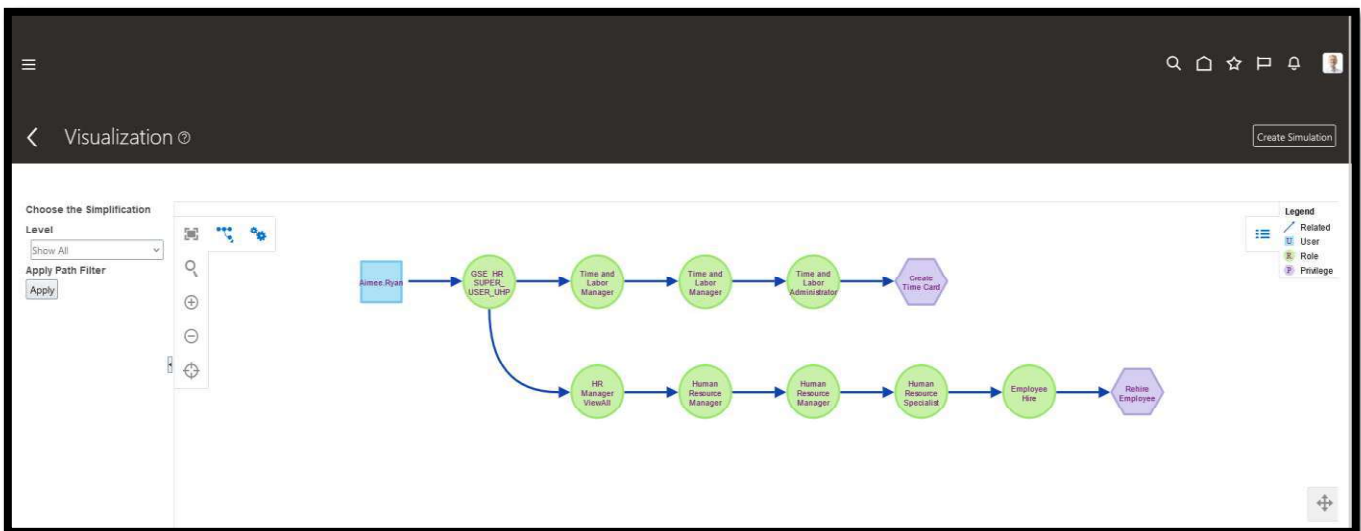


Figure 4: Separation of Duties Visualization

Automate user access reviews and certifications.

Automate user access reviews to ensure timely certification by business process owners and meet audit and compliance requirements. Plan and scope access certification campaigns without having to rely on manual data extracts. Leverage AI to empower certifiers with role details, security context, and recommendations – enabling informed decisions and strengthening audit confidence.

Continuously monitor user activity with AI

Monitor changes to critical configurations.

Automate monitoring of changes to critical configurations and master data to detect unauthorized or suspicious activity. Leverage a library of best-practice controls, and author new configuration controls using a visual workbench with pre-built business objects covering 1300+ ERP data elements.

Audit transactions to identify fraud, error, and policy violations.

Move from sample-based reviews to continuous, AI-driven monitoring of financial transactions for complete visibility. Implement compensating controls to identify transactions that indicate potential abuse of privileges.

Enable business process owners and auditors to identify high-risk activity – such as duplicate invoices, ghost employees – using pre-built control libraries or custom algorithms created using an intuitive workbench with streamlined exception management workflow.

Procure-to-pay assurance.

Monitor user access and activity across procure-to-pay to help ensure process integrity. Enforce separation of duties and analyze all purchase orders, invoices, and payments.

Record-to-report assurance

Monitor user access and activity across record-to-report to maintain the integrity of processes. Enforce separation of duties and analyze all subledger transactions, period close adjustments, and manual journal entries.

Order-to-cash assurance

Monitor user access and activity across order-to-cash. Enforce separation of duties and analyze all customer orders, approved credit limits, and payment receipts.

Hire-to-rotate assurance (requires subscription to Advanced HCM Controls).

Monitor user access and activity across the hire-to-rotate process. Enforce separation of duties and analyze all payroll runs, compensation changes, and timecard transactions.

Business Process	Risk Name	Internal Control Name	Internal Control Description	Automated Control Name	Last Run Date	# Pending Incidents	# Accepted or Closed Incidents	Run History
Procure to Pay	ICFR-RM03 Inappropriate Expense of Asset Purchases	PTP-003-SOD Transactional Analysis	Review 100% procure to pay transactions for SOD risks based on the most current SOD rules. The implementation and continual monitoring of specific separation of duties transaction controls to identify where the same person performed conflicting transaction events. Any occurrences must be investigated immediately and identify either prior approval or otherwise resolved appropriately.	CI-PTP-60001: Supplier and Payables Invoices Created by the Same User	4/14/25	25	466	View Run History
		PTP-006-Accounts Payable Invoice Validation	Validate and approve all invoices before payment. Validation steps include (1) PO based on policy (b) Sign-off based on approval matrix and SOD policy (c) Likely duplicate invoice check (across BUS, currency, similar invoice number, similar time frame – not just exact duplicates)	CI-PTP-30002: Duplicate Suppliers and Sites CI-PTP-30003: Backdated Purchase Orders	4/14/25 4/14/25	0 5	0 26	View Run History View Run History
ICFR-RM04 Fictitious or unauthorized payments		PTP-005-Bank Account Change Reviews	Review and ensure updates to bank accounts are authorized and accurate.	CI-PTP-60001: New Bank Account Added to Supplier	4/14/25	1	47	View Run History
				CI-PTP-60007: Changes to Supplier Bank Accounts on a Weekend CI-PTP-60002: Changes to Supplier Bank Accounts	4/14/25 4/14/25	0 0	0 4	View Run History View Run History
		PTP-004-Supplier Validation	New and updated suppliers are only approved by authorized employees. Updates include changes to bank details, invoice amount limits, and matching options.	CI-PTP-60003: Changes to Supplier	4/14/25	0	12	View Run History
				CI-PTP-60005: Frequent Changes to Supplier Payment Methods CI-PTP-60004: Changes to Supplier Site	4/14/25 4/14/25	5 2	88 15	View Run History View Run History

Figure 5: Procure to Pay Assurance Dashboard

Manage internal controls

Oracle Risk Management serves to maintain a centralized repository of financial controls and provides an end-to-end workflow solution to automate assessments, financial reporting certifications, and compliance with mandates such as SOX and GDPR.

Design and document internal controls

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.

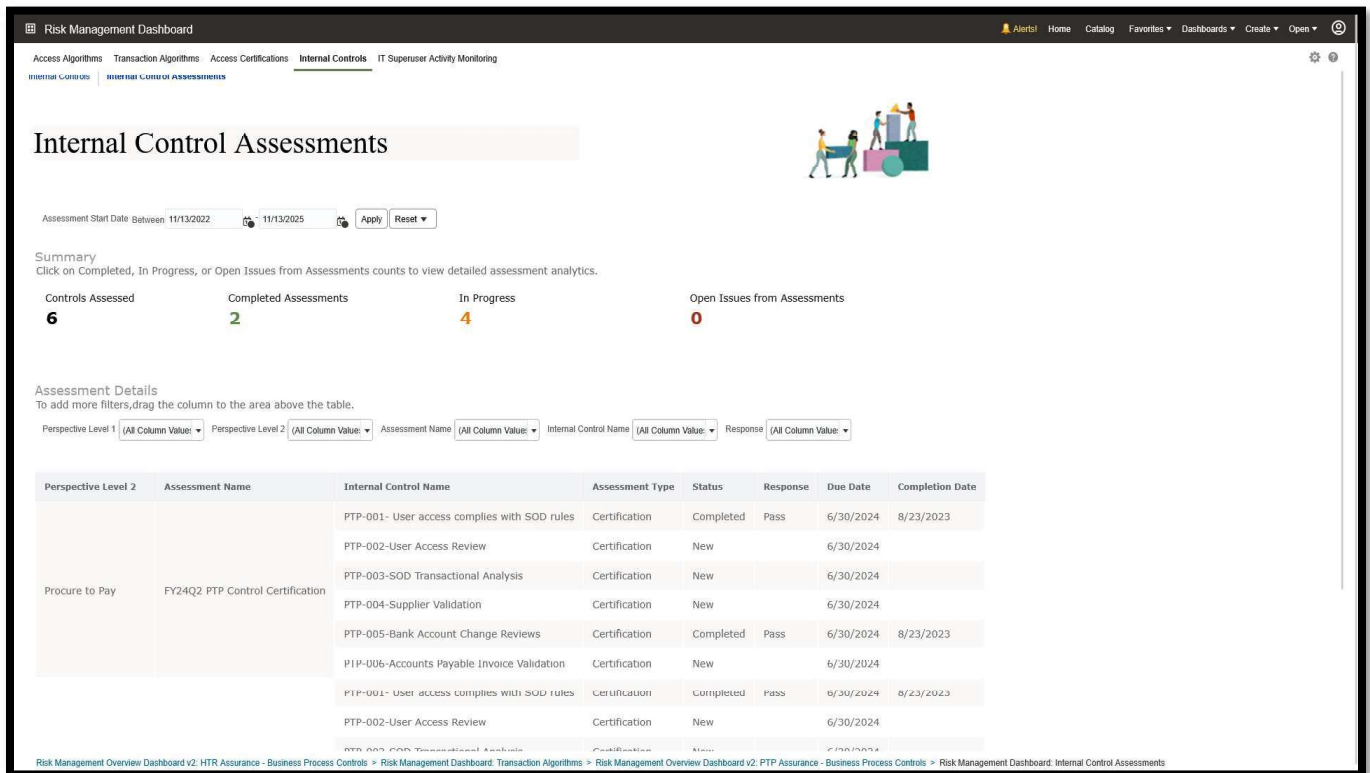


Figure 6: Internal Control Assessment Dashboard

Connect with us

Call +1.800.ORACLE1 or visit [oracle.com](https://www.oracle.com). Outside North America, find your local office at: [oracle.com/contact](https://www.oracle.com/contact).

blogs.oracle.com

facebook.com/oracle

twitter.com/oracle

Copyright © 2026, Oracle and/or its affiliates. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.