Oracle Fusion Cloud Risk Management and Compliance

Traditional approaches to compliance and cybersecurity don't meet the evolving financial audit standards for agentic Cloud applications. Oracle Risk Management and Compliance transforms audit from a "check the box" exercise to data-driven continuous assurance and cybersecurity monitoring. Using embedded AI and 300+ algorithms, it monitors millions of transactions, configuration changes, and user access and provides process leaders with deep data analysis to help them certify controls with confidence.

Oracle Risk Management and Compliance (RMC) is an Oracle Cloud ERP module that helps manage cybersecurity risks in Fusion SaaS, enforce Internal Controls over Financial Reporting (ICFR), meet Sarbanes-Oxley (SOX) compliance requirements, and ensure audit readiness.

Comprehensive and embedded—evolves as you grow.

Oracle Risk Management Cloud (RMC) provides a comprehensive, configurable set of capabilities that evolve with your business needs. It enables automated monitoring, analysis, and control of user access and activity across Oracle Cloud ERP.

Leveraging advanced data science and AI, RMC helps accelerate implementation by supporting secure role design, simplifies compliance by identifying and resolving Separation of Duties (SoD) conflicts, and prevents violations during access provisioning. It also strengthens security by monitoring superusers and sensitive configurations and enhances assurance by detecting suspicious transactions - helping protect against fraud and errors.

Included Modules

- ***Advanced Access Controls*** for ensuring segregation of duties.
- ***Advanced Financial Controls*** for monitoring financial transactions.
- ***Financial Reporting Compliance*** for streamlined internal assessments and compliance (10 users).

Related Modules

- ***Advanced HCM Controls*** is the equivalent product for monitoring of user access and activity in HCM.

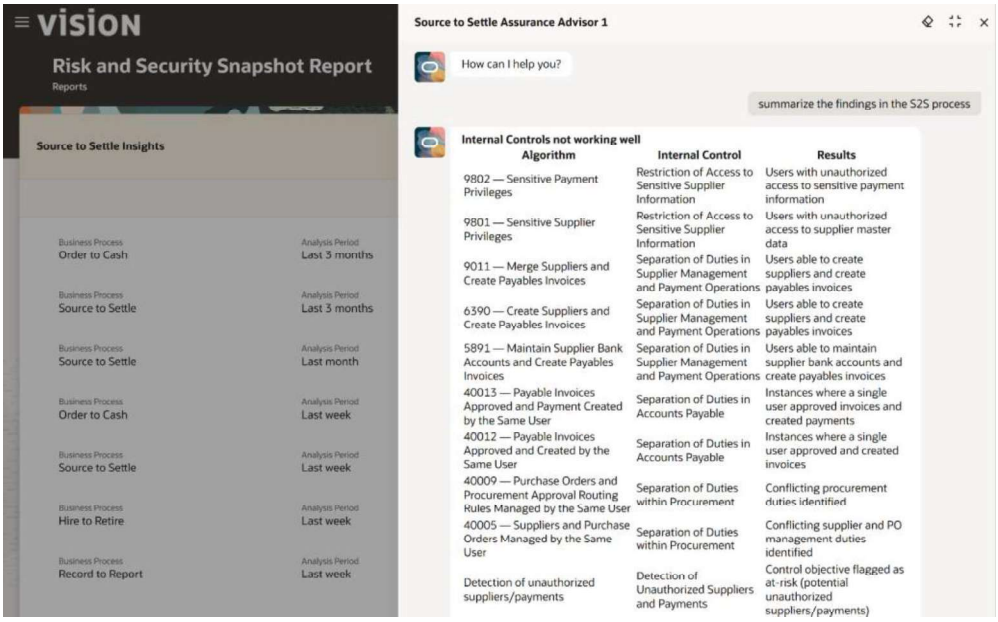

Figure 1: Source to Settle Assurance Advisor

BENEFITS

1. AI-powered cybersecurity with proactive prevention

Embedded AI analyzes user access to prevent inappropriate permissions in role design and before they are granted during user access provisioning. Automate reviews using plain-language risk insights. Only Oracle monitors audit trails for risky drift, securing all accounts natively in the cloud.

2. Comprehensive monitoring for Separation of Duties (SoD) Violations

Others may focus only on user access risks. Only Oracle automates monitoring for both potential and actual SoD violations, using embedded AI for enforcement. Visualization tools help quickly address risks, and full transaction monitoring gives process owners' assurance.

3. Automated analysis of real transactions, not just possible access

More than 300 prebuilt algorithms review millions of actual transactions in real time. Spot fraud, policy breaches, or errors across every key business process, from order-to-cash to hire-to-retire, rather than simply analyzing possible access. Within hours, customers can rapidly deploy best practice controls with pre-built algorithms for continuous monitoring of targeted high-risk areas.

4. AI agents deliver process assurance and continuous audit

AI-powered agents deliver actionable insights from prebuilt controls. Oracle automates activity monitoring, audit scoping, and testing, minimizing manual work, improving accuracy, and continuously verifying compliance for increased confidence and speed.

5. Proven reference frameworks for cybersecurity and ICFR at scale

Only Oracle provides you with industry tested reference controls for ICFR and cybersecurity, mapped to automated algorithms for monitoring of your Oracle applications. Leverage 28,000+ business data points to rapidly deploy and sustain compliance, meet SOX needs, and avoid audit surprises.

6. Embedded, secure, and unified platform within Oracle Fusion Cloud

Oracle Fusion Risk Management and Compliance is natively built into Oracle Fusion Cloud, eliminating risky exports and patchwork integrations. Sensitive data remains protected, attack surfaces are minimized, and superior controls transform ERP and supply chain security. Simplify and automate risk and compliance processes to promote risk awareness, collaboration, transparency, and accountability.

Key Features

- Automated monitoring for intra-role violations to prevent inherent risk in ERP roles.
- Access Request Assistant, (AI Agent) that identifies potential violations before users are granted access.
- Deep SoD analysis with visualization and simulation of conflicts.
- Monitoring for SoD in transactions for audit and assurance
- Access Certification Advisor (AI Agent) to enhance User Access Reviews with context and recommendations.
- Continuous monitoring of sensitive ERP configurations
- Continuous monitoring/audit of critical ERP transactions.
- Assurance Advisor (AI Agents) for ERP processes: S2S, R2R, O2C,
- Library of pre-built algorithms and intuitive workbench to author custom algorithms.
- Graphical, persona-based dashboards for actionable insights
- Streamline assessments of Internal Controls over Financial Reporting (ICFR) for assurance, compliance (SOX) and audit readiness.

AI AGENTS

Certification Advisor: Helps ERP process owners complete user access reviews and certifications quickly and with confidence. The agent creates a plain-language briefing for each user/role decision that explains what the role really enables, compares access to the user's job role and peer usage, and includes results from security algorithm analysis—so certifiers can decide keep/remove access faster, with documented rationale and stronger audit evidence.

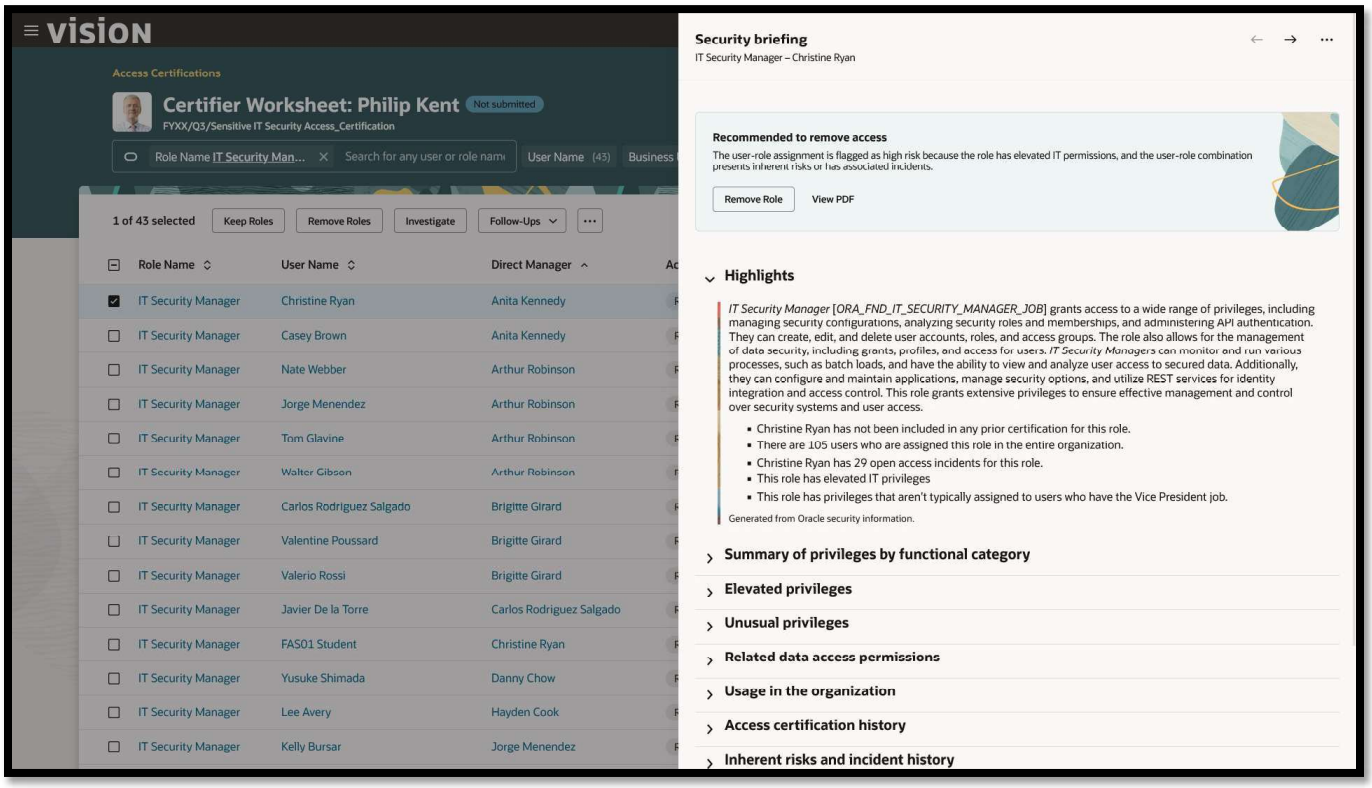

Figure 2: Certification Advisor AI Agent

ERP Access Assistant: Helps business users request Fusion ERP roles without complex IT tickets or forms. The agent helps users select the right predefined persona (for example, AP Manager by business unit), translate needs into the right roles, auto-build the request, run preventive SoD and security analysis, and provide a plain-language risk summary to approvers—cutting request cycle time, supporting confident approvals, and generating audit-ready evidence by default.

Assurance Advisor: Helps business process leaders assess their internal controls using deep analysis from 100+ algorithms. The agent highlights which controls need attention across STS, RTR, OTC, and HTR; summarizes who has excessive or toxic access; identifies transactions with SoD violations or likely duplicate supplier records; and pinpoints the highest-risk activity with supporting evidence—so finance teams can focus on the right issues and risks and certify internal controls with confidence.

Improve Cybersecurity Posture

Prevent unauthorized permissions and access.
Ensure that access policies, including separation of duties, are enforced during role design and user provisioning, with preventive and detective methods. Deploy Risk Management Cloud along with ERP to accelerate security design and avoid costly delays in UAT and unnecessary remediation of security post-go live.

Monitor IT admin/superuser access and transactions.
Highly privileged IT users have broad access for activities that require their attention, expertise, and skills. Ensure that such privileges are used as needed, regularly monitored, and not abused.

Monitor business superuser access and transactions.
Certain business administrator roles often have broad, superuser-like access to facilitate manipulation of configurations, setups, and master data. Because of their deep functional and process knowledge, it makes sense to give these users broad access - provided safeguards are in place to monitor for unusual activity, such as error or misuse.

Monitor nonhuman account access and transactions.
In an increasingly automated world, there are many processes that use aliases, APIs, and automated interfaces. Ensure that all nonhuman interfaces are scrutinized, adequately tested, certified, and monitored for changes and updates.

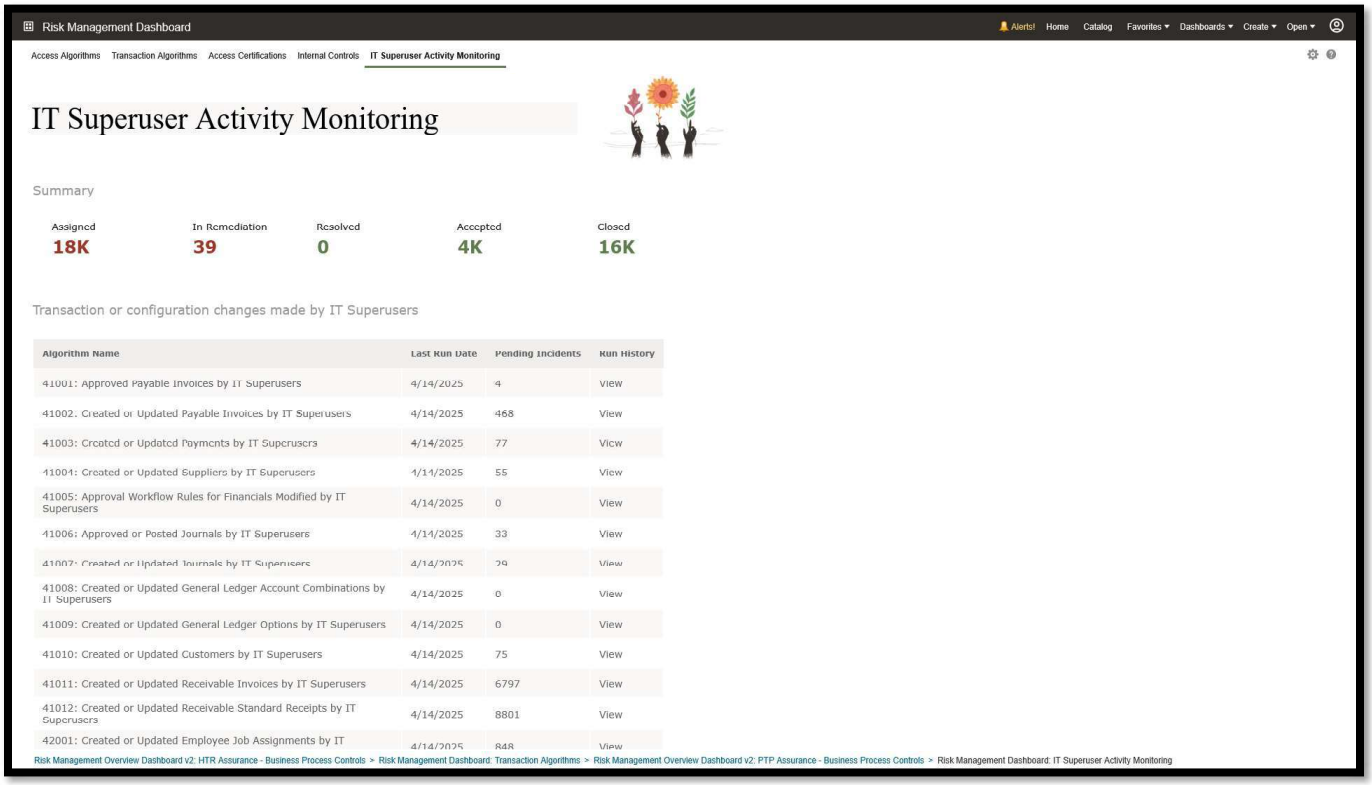

Figure 3: IT Superuser Activity Monitoring Dashboard

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.

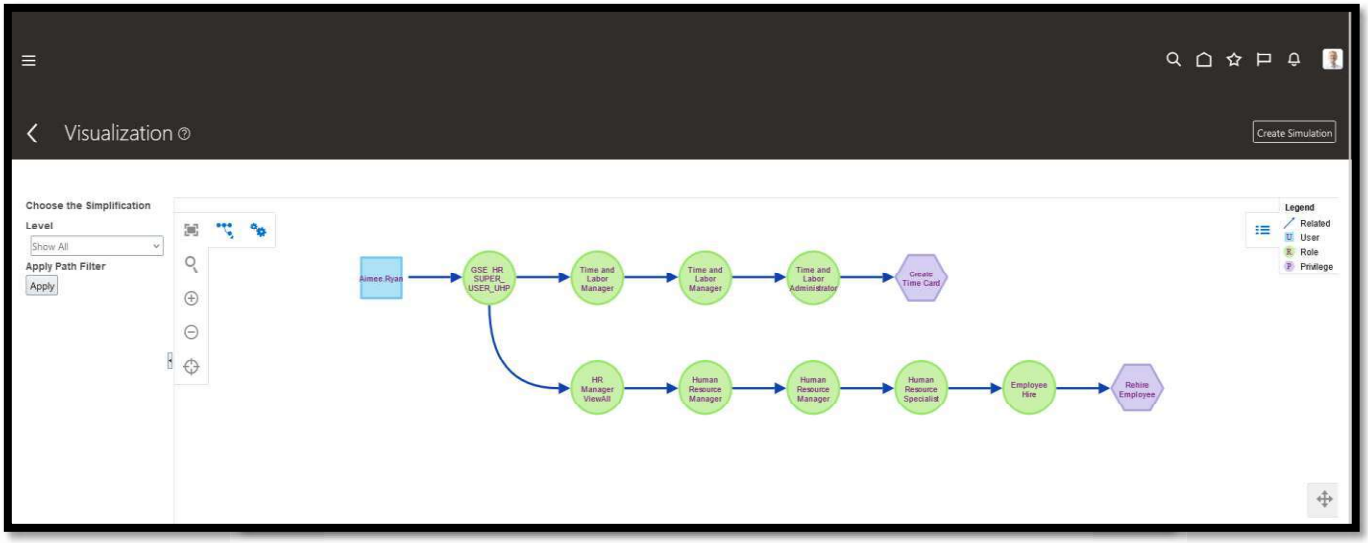

Figure 4: Separation of Duties Visualization

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-retire assurance (*requires subscription to Advanced HCM Controls***).**
Monitor user access and activity across the hire-to-retire process. Enforce separation of duties and analyze all payroll runs, compensation changes, and timecard transactions.

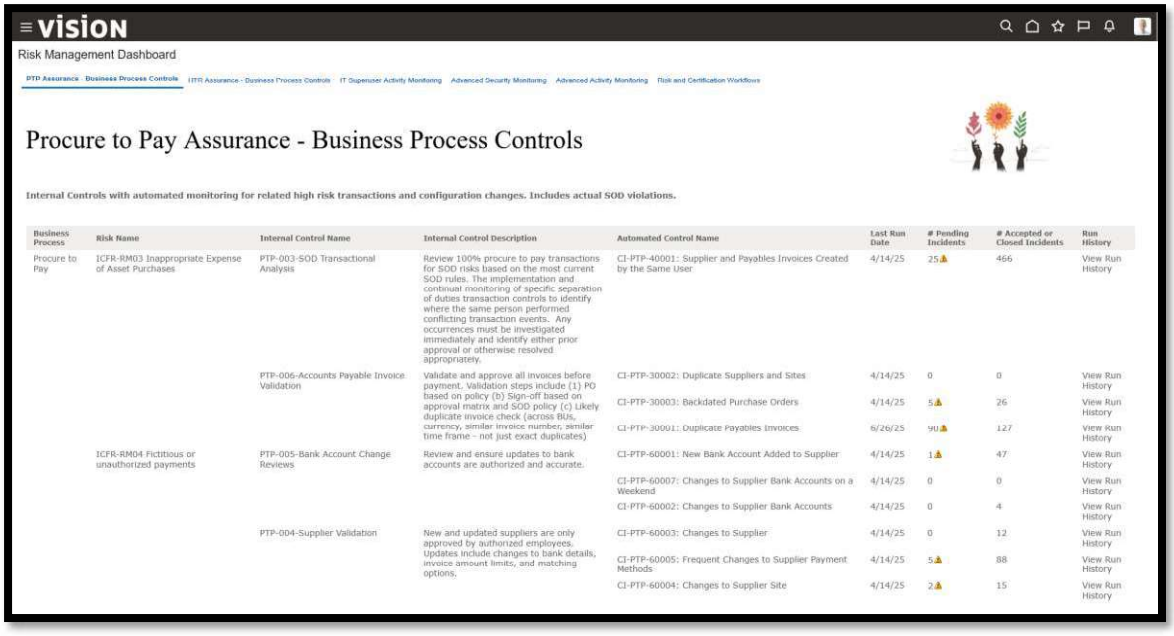

Figure 5: Procure to Pay Assurance Dashboard

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.

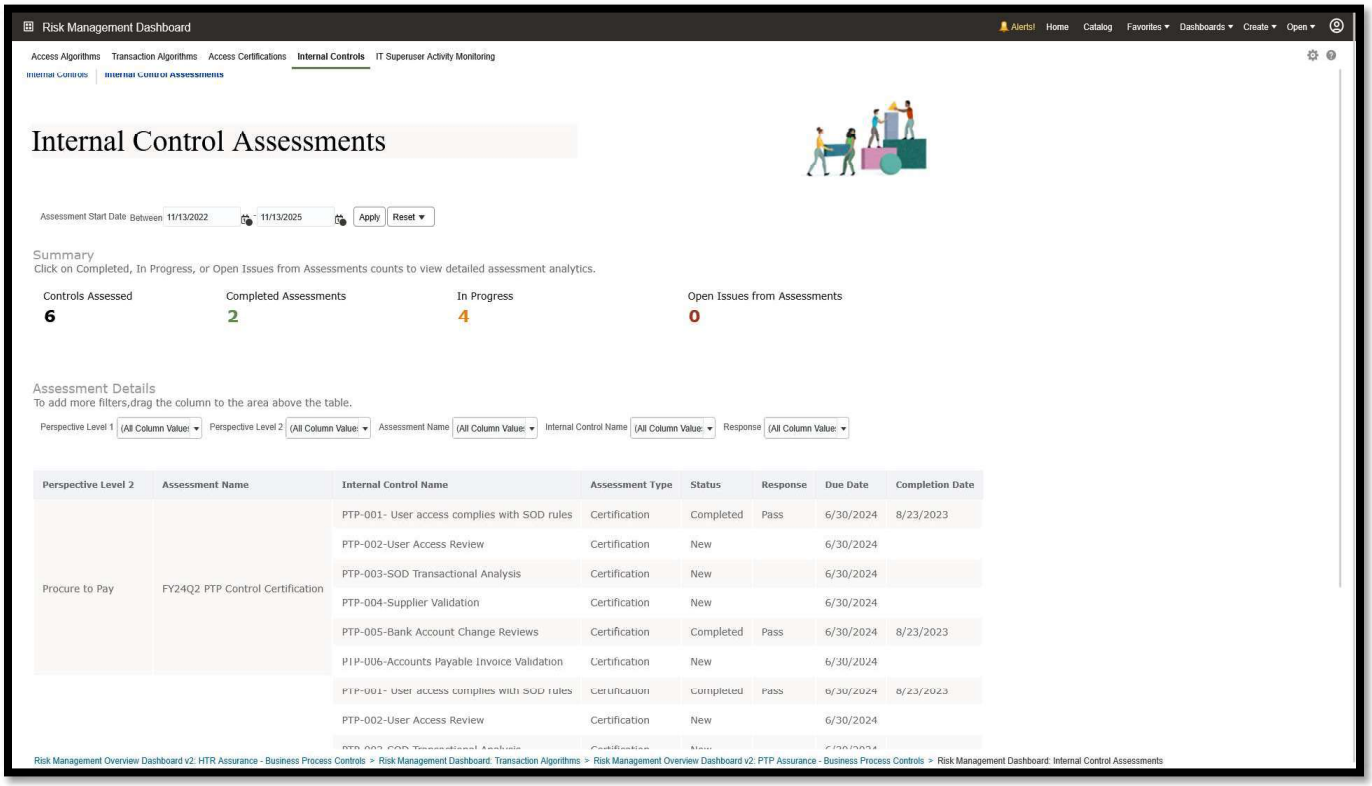

Figure 6: Internal Control Assessment Dashboard

Connect with us

Call **+1.800.ORACLE1** or visit **oracle.com.** Outside North America, find your local office at: **oracle.com/contact.**

blogs.oracle.com facebook.com/oracle twitter.com/oracle