Automate HCM Cloud Security and Internal Controls

Key Use Cases for Oracle Advanced HCM Controls

Why use Oracle's built-in Advanced Controls for HCM?

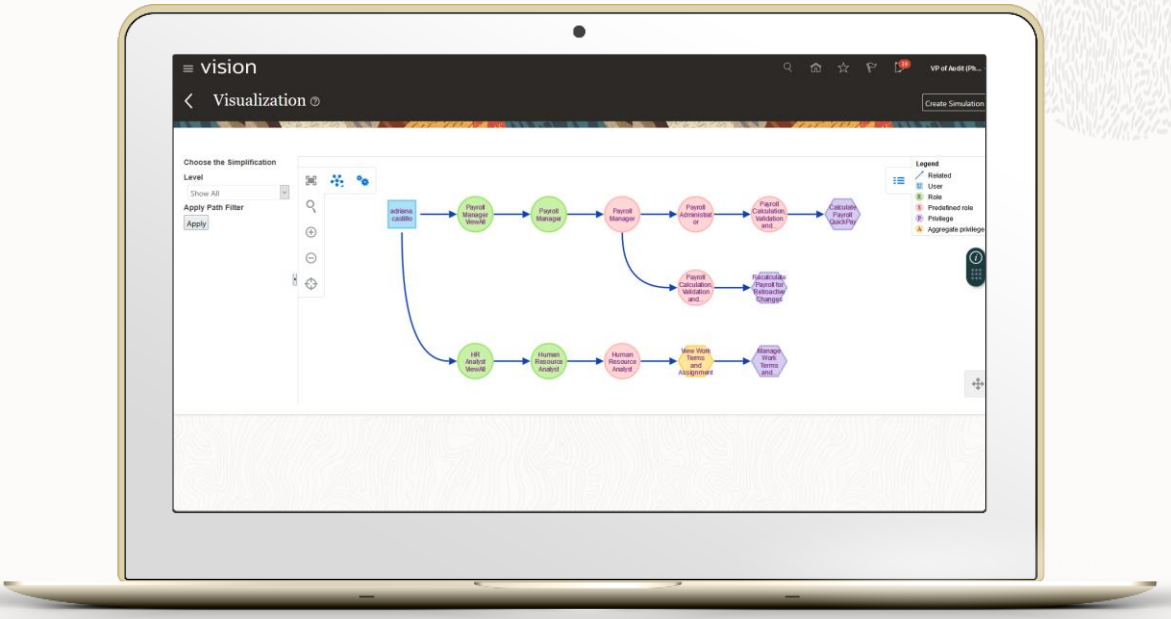
Business leaders use Oracle HCM Cloud's built-in Advanced Controls to automate many routine, labor-intensive risk tasks — especially those involving security, configurations and transactions. It reduces compensation and payroll frauds, security breaches, and stops cash leakage. There are many common tasks to automate, including segregation of duties, ensuring secured access to sensitive data, preventing erroneous transactions, … to name just a few.

Ready to take a closer look?

Key Use Cases

1. Optimize Security Design to Minimize Separation of Duties (SOD) Risk
2. Automate SOD Controls for Compliance Reporting
3. Digitize User Access Certification Workflows
4. Automate Monitoring of User Security
5. Automate Monitoring of Changes to Critical Configurations
6. Automate Monitoring of HCM Transactions

Optimize Security Design to Minimize Separation of Duties (SOD) Risk



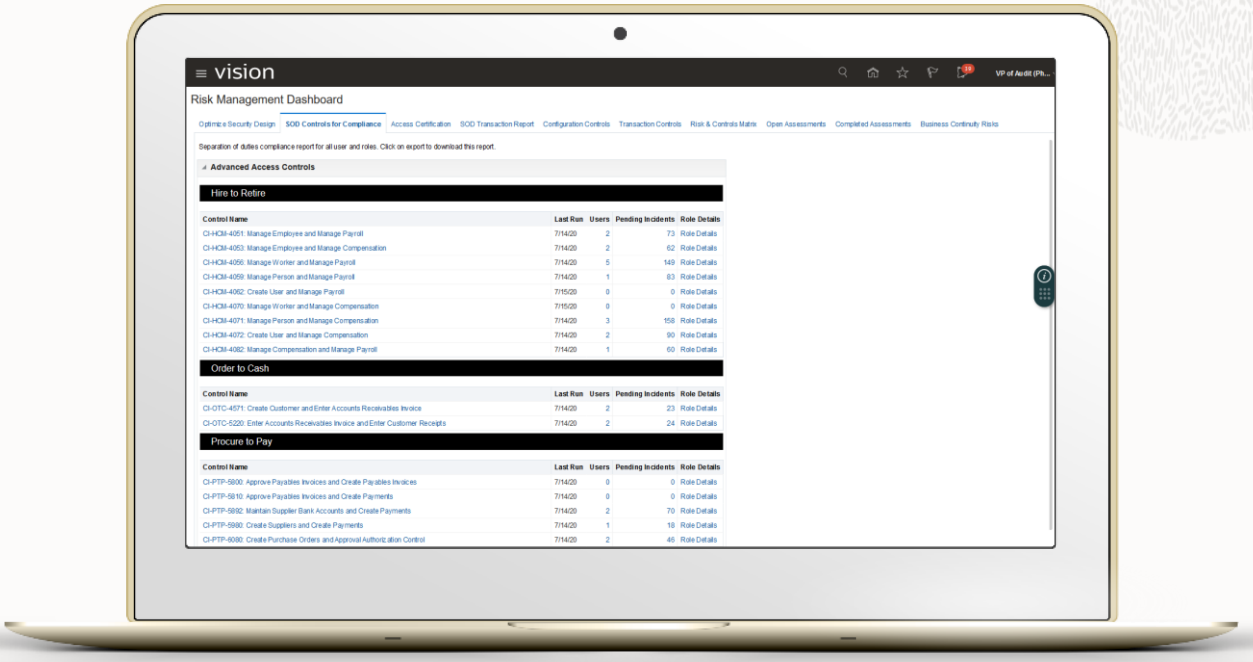
Accelerate HCM security configuration
Automate analysis of user access to identify and eliminate SOD conflicts. Ensure that roles are compliant and audit ready. Start analyzing security configurations in hours, to avoid last-moment user acceptance testing (UAT) issues, that could delay your HCM implementation.

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[1] 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

1 Typically 3-6 weeks of role remediation by ERP experts at $2,000 per day adding up to $30,000 to $60,000

Automate SOD Controls for Compliance Reporting



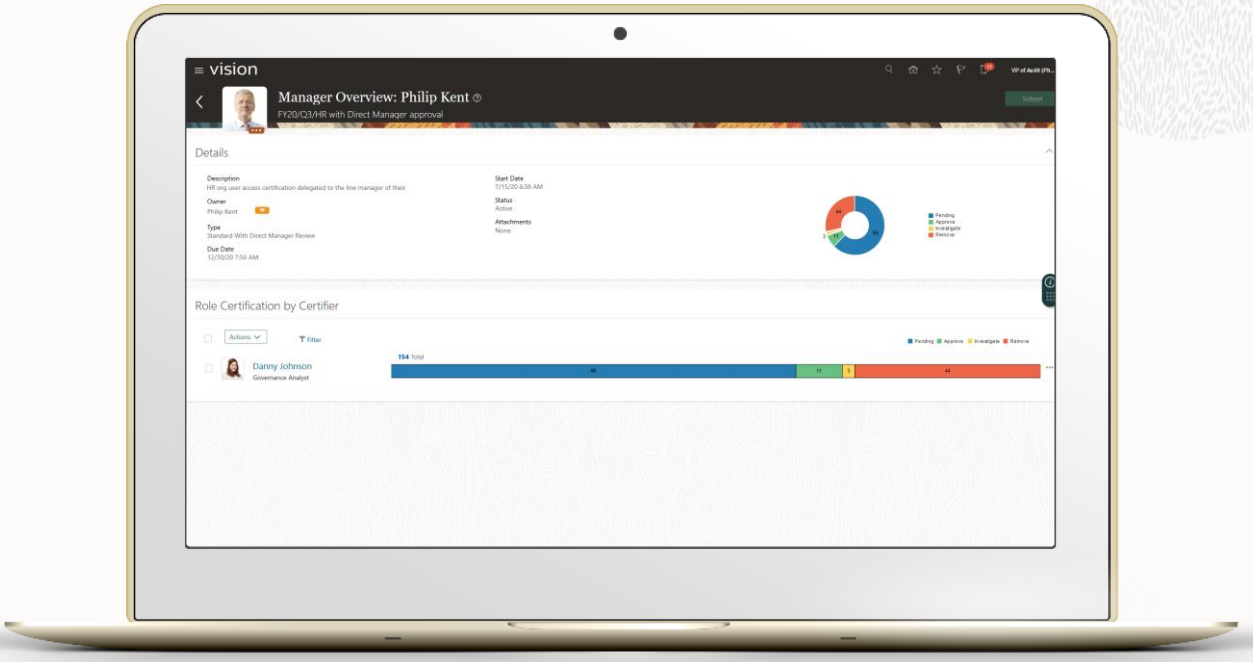
Report SOD results with confidence and ease
Rely on built-in, complete analysis of fine grain functional access with data security context (BU, Region, Function,etc.). Generate compliance-driven SOD reports with confidence each quarter. Reduce audit consulting fees by over $100,000[1] per year.

Visualize SOD analysis in minutes.
Leverage library of 30+ SOD rules with configurable reports & dashboards. Configure or tailor prebuilt rules with an easy-to-use visual workbench.

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

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

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 & schedules.

Automate routing to direct manager

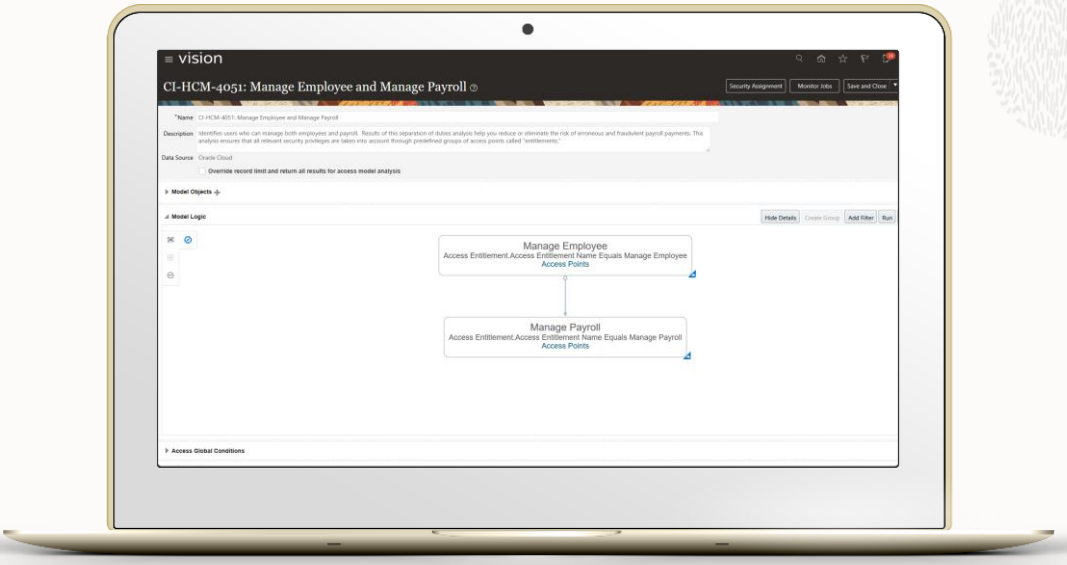
Streamline workflow based on manager hierarchy and/or designated process owners. Reduce compliance fatigue and save ~250[1] hours of manual effort with easy-to-review worksheets.

Continuously certify new users with high-risk access

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

1 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)

Automate Monitoring of User Security

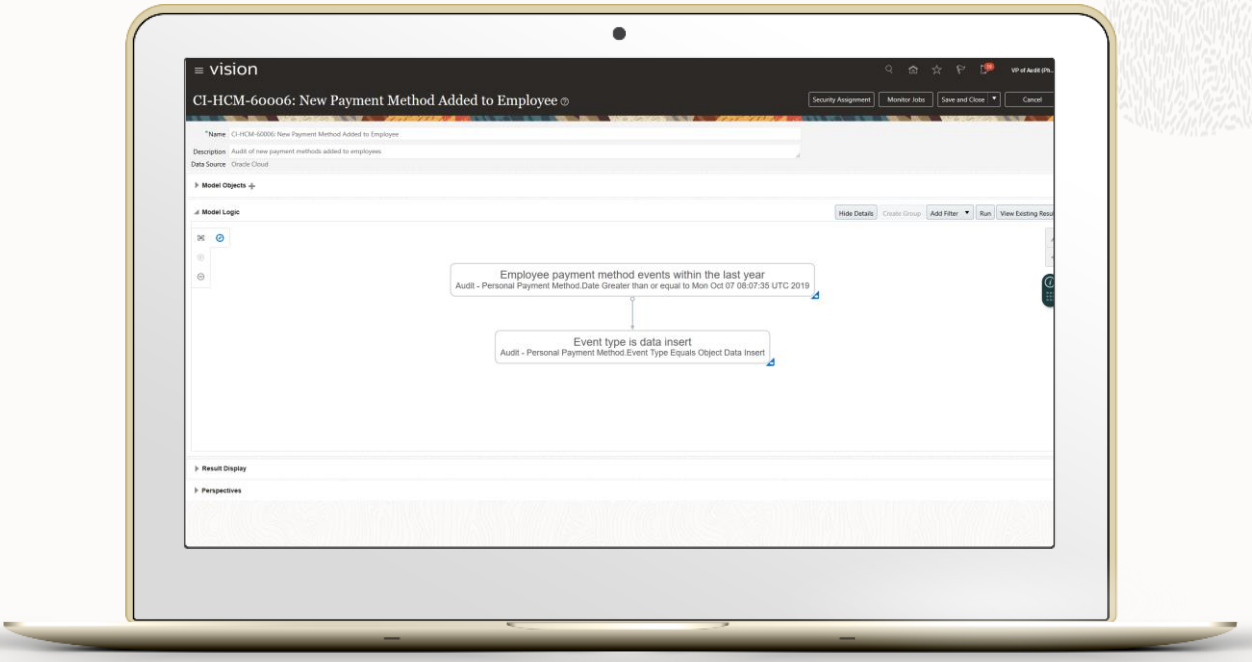


Proactively enforce security and privacy policies beyond compliance
Continuously analyze roles & user access as business functions or responsibilities evolve. Quickly identify SOD violations to refine roles and security configurations, in response to ever-changing organizations.

Modify pre-built rules, or create your own using easy visual workbench
Leverage pre-built library of 30+ best-practice security rules, to accelerate deployment. Author new rules quickly, using a robust library of objects and functions.

Manage access exceptions with ease
Monitor exceptions on a dashboard, and resolve issues using a simple incident workflow. Accelerate resolution of conflicts with the aid of visualizations and simulations

Automate Monitoring of Changes to Critical Configurations

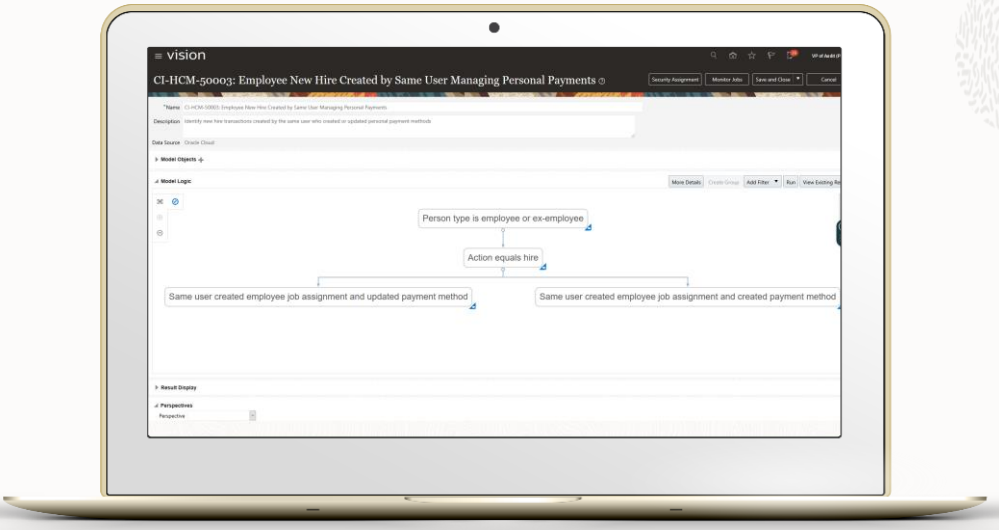


Automate risk-based analysis of setup and master data changes
Detect breaches and evaluate risks with automated analysis of critical configuration changes across key processes including compensation, payroll, benefits, recruiting, talent management

Leverage library of best-practice configuration rules
For example: : Get alerts for frequent or unauthorized changes made to employee master data, payroll settings, compensation changes, employee bank accounts, payroll periods, etc. Tailor pre-built or author new rules using a built-in visual workbench.

Manage exceptions with ease
Ensure all exceptions are routed to process owners for timely reviews (replacing emails and spreadsheets)

Automate Monitoring of HCM Transactions



Audit 100% of all HCM related transactions

Leverage built-in AI to analyze all transactions & data (such as employee data, compensation, payroll, etc.). Eliminate error and added cost, by replacing hand-crafted legacy audit scripts with a modern workbench for authoring rules.

Stop significant cash loss

Average loss per case is $1,509,000[1]

Manage exceptions with ease

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

Eliminate exposure and loss of sensitive data

Protect your propriety data by eliminating the need to bulk extract of employee, compensation and payroll data for script-based analysis or 3rd party tools

1 *Association of Certified Fraud Examiners, 2020 Global Study on Occupational Fraud and Abuse*.

Learn more

oracle.com/applications/erp/risk-management-cloud.html

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

Integrated Cloud Applications & Platform Services