ORACLE

Oracle Fusion Cloud Risk Management and Compliance

Oracle Risk Management is a module within Oracle Fusion Cloud ERP to manage risks and meet compliance and privacy mandates (SoD, SOX, GDPR, etc.). Oracle Risk Management subscribers can automate analysis, monitoring and control of ERP security, configurations and transactions.

Oracle Risk Management uses modern data science and AI techniques to help design secure roles, resolve SoD conflicts, monitor sensitive configurations, and detect suspicious transactions to protect against payment fraud and error. Oracle Cloud ERP users can use these AI-driven risk analysis tools to accelerate implementations, anticipate ERP risks, provide actionable insights, simulate and track remediation solutions, and streamline compliance.

- Oracle Risk Management simplifies risk and compliance processes to promote risk awareness, collaboration, transparency and accountability.
- Organizations can automate security and transaction data analysis for SoD, fraud, errors, and policy violations.
- Within hours, customers can rapidly deploy best practice, controls with pre-built algorithms, for continuous monitoring of targeted high-risk areas.

Secure role design

Poorly designed roles are the #1 reason for audit findings after go-live. Oracle Advanced Access Controls helps design secured roles to jump-start security configuration for your ERP implementation. It automates privilege-level security analysis while configuring Job Roles avoiding expensive redesign, rework and delays in ERP implementation, associated with discovering SOD violations during testing, rollout or worse, as an audit finding. With a library of 100+ best practice security, access and privacy controls, it can be up and running in a few easy steps.

Deep SOD analysis

Enforcing SOD compliance requires a detailed analysis of all functions and data that are accessible to each user. Oracle Risk Management is powered by an AI-driven analytical engine that scans thousands of access paths & access privileges for each user. It is the only solution that fully describes a user's access at the most granular level.

Key features

- Automation of risk and compliance processes.
- Secure role design to accelerate ERP implementation.
- Deep SoD analysis with visualization and simulation of conflicts.
- Continuous monitoring of all security, configurations and transactions.
- Library of pre-built controls and intuitive workbench to author custom controls.
- Streamline control assessments, certify compliance, and collaborate with auditors.
- Full visibility with graphical, role-based dashboards.

Included modules

- Financial reporting compliance for streamlined internal assessments and compliance.
- Advanced financial controls for monitoring financial transactions.
- Advanced access controls for ensuring segregation of duties.

Oracle Risk Management provides a library of ready-to-use controls for high-risk business processes, for example, AP, AR, GL, Payroll, Compensation, etc. and an intuitive workbench to visualize conflicts and simulate remediation.

After go-live, organizations can continuously monitor access policies throughout their ERP life cycle: while on-boarding new users, changing role assignments, or designing new roles. Using the graphical workbench, they can easily update access controls to keep up with changing processes and role definitions.

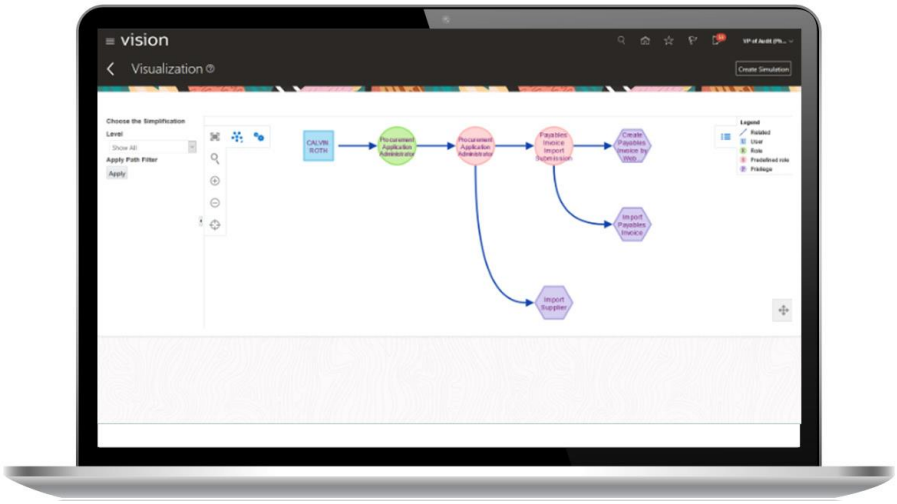

Figure 1: Visualization of access conflict

Sensitive access certification

Organizations can further protect sensitive privileges and data by carrying out periodic certification of sensitive access privileges. Automated workflows eliminate manual compliance tasks that rely on spreadsheets and emails. Administrators can scope sensitive ERP roles and users for approval by process owners, and approve, remove or investigate users with high-risk access.

Access Certification streamlines your organization's periodic reviews to determine whether roles are assigned appropriately to users. Access Certification supports broad, organization-wide reviews such as quarterly audits, as well as, more narrowly focused sensitive-access scenarios.

A certification may involve a static set of user-role assignments, at any given moment or a continuous certification that includes only new user-role assignments, on an on-going basis. While the roles included in a continuous certification remain the same, their assignments to users are updated each day, for certification.

Advanced configuration controls

Organizations can now continuously monitor changes to ERP configurations and master data. They can leverage a library of best-practice controls, across a range of business processes, to capture and audit a trail of changes. They can also,

author new configuration controls using a visual workbench, and a library of pre-built business objects, and over 1300 ERP data elements.

Advanced transaction analysis

Oracle Risk Management provides a capability to continuously monitor ERP transactions. Business process auditors can detect high-risk scenarios like Duplicate Invoices, ghost employees' etc. They can compose new algorithms using visual workbench, and manage exceptions using simple workflow.

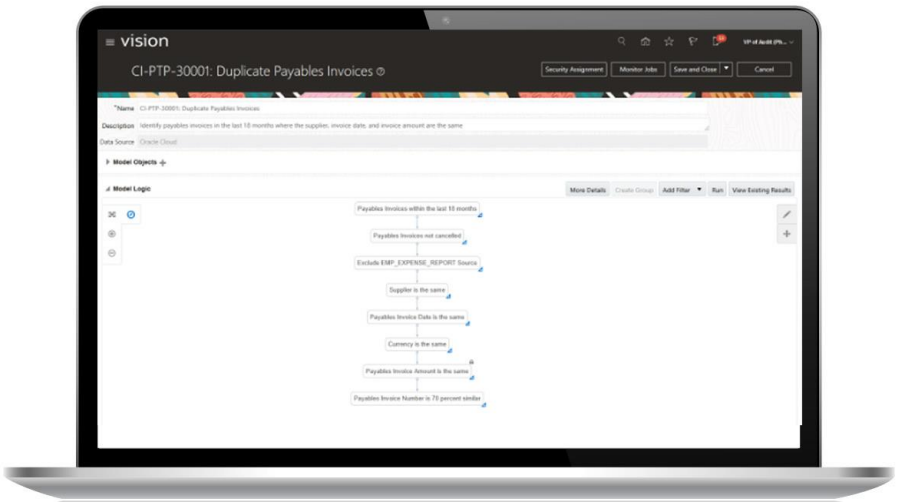

Figure 2: Visual workbench to build model logic

It allows organizations to implement compensating controls, to identify transactions where excess privileges may have been abused. Organizations can ensure that broad super-user privileges granted for emergencies are not abused and revoked in a timely manner.

Risk and compliance workflows

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

It provides an automated solution to complete Data Protection Impact Assessments, certify and monitor employee access to personal data, respond to SAR requests on personal data access and use. Employees can also, report data breach and other security incidents.

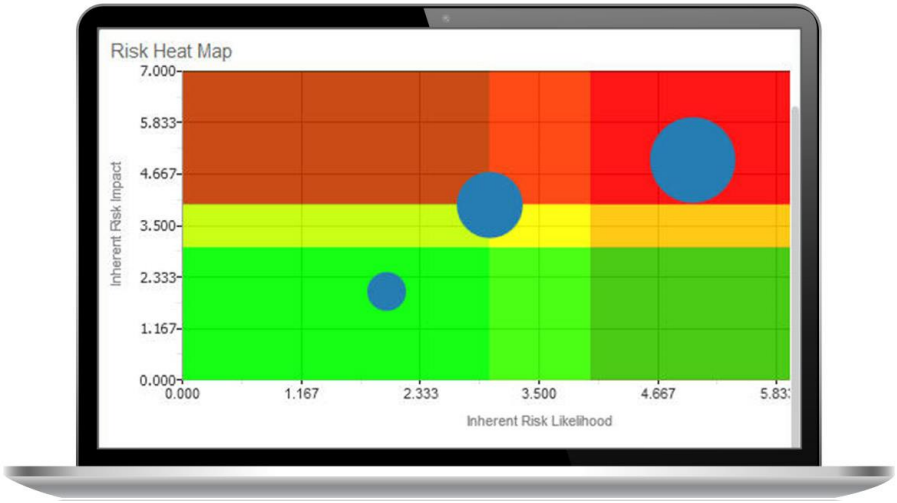

Figure 3: Risk heat map

Users can perform workflow-based risk analysis, evaluations and implement treatment plans to mitigate risks. They can perform periodic or ad hoc control assessments, capture test results, and provide ready evidence for audits.

Comprehensive and embedded—evolves as you grow

Oracle Risk Management offers a comprehensive set of capabilities that can be configured to match your changing needs over time. These capabilities include:

Secure role design

- Optimize role definitions by addressing intra-role conflicts.
- Remediate conflicts, or choose to monitor with compensating controls.
- Evaluate remediation plans by simulating impact of proposed changes on results.

Deep SoD analysis

- Automate Security Analysis.
- Analyze access privileges using complete scans of all access paths.
- Reduce complexity by grouping fine-grained privileges into functional entitlements.
- Identify root cause of access violations by visualizing access conflicts.

Sensitive access certification

- Generate access certifications by querying a repository of entitlements and assigning it to a certifier/approver.
- Scope a certification based on a specific role, business process or set of users.
- Take corrective action upon identifying violations of policies.

- Gain full visibility and control of the periodic certification process.

Advanced configuration controls

- Monitor changes to sensitive ERP Configurations and Master Data.
- Capture and audit trail of changes using a library of best-practice controls.
- Author controls using a visual workbench and a repository of business objects and attributes.

Advanced transaction analysis

- Get immediate value by using pre-built controls.
- Upgrade your existing controls to industry best practices.
- Empower users to author new access rules and policies graphically.
- Accelerate authoring of new controls graphically by leveraging a library of pre-built business objects.

Risk and compliance workflows

- Document Risk & Controls uniformly across the Enterprise.
- Automate risk analysis and evaluations, using best practices.
- Reduce compliance costs by eliminating labor intensive tasks.
- Improve security and collaboration by replacing unsecured spreadsheets, emails and documents.
- Strengthen internal controls by delegating to process owners.
- Demonstrate controls are enforced, known risks are controlled, and emerging risks are identified and mitigated.

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