ORACLE
Human Capital Management Cloud

Oracle Advanced HCM Controls

Advanced Access Controls Cloud Service enables continuous monitoring of all access policies in Oracle HCM, potential violations, insider threats and fraud. It automates security analysis to ensure segregation of duties, and supports compliance with access policies. Organizations can easily upgrade their existing processes by deploying a pre-built library of best practice access controls, or graphically author new controls to suit their changing needs. They can manage all their application access risks, using access controls and compensating monitoring controls with a secure solution embedded within the Oracle HCM Cloud.

Access Controls for HCM

Key Features

- Continuously monitor access policies
- Pre-built Best Practice Controls for Segregation of Duties
- Graphical Workbench for users to author and configure controls
- Embedded dashboard with analytics and reporting

PROTECT AGAINST FRAUD AND ENFORCE ACCESS POLICIES

Advanced HCM Controls provides comprehensive management of application access. It automates security analysis, identifies violation of access policies, helps rationalize roles and remediate conflicts, and supports the segregation of duties.

Advanced HCM Controls helps organizations:

- Prevent fraud – by restricting privileges so that no user is able to perform end-to-end financial transactions independently
- Accelerate secure deployment of Cloud HCM Applications - by designing roles that are free of SoD conflicts.
- Strengthen compliance with audit requirements and mandates (such as GDRP, SOX) – by auditing access privileges.
- Protect information assets from insider threats– by limiting and monitoring access to sensitive data and super-user privileges.

ORACLE

SUPPORT SEGREGATION OF DUTIES BY AUTOMATING SECURITY ANALYSIS

Complete scans of full access-paths: Advanced HCM Controls analyzes application access by using automated complete scans of all access paths, to identify if a user has access to one or more privileges that violate SoD policies. It allows access administrators to focus on legitimate conflicts by speedily eliminating false positives. Administrators are able to identify root cause of each conflict, by visualizing the access paths involved. They are able to visualize access paths for each role and user, facilitating remediation of the conflict.

Fine-grained analysis of privileges: Auditors typically require a fine-grained SoD analysis based on granular functional and data privileges. The only scalable and sustainable way to deliver these complex requirements is via a pre-integrated solution that automates and simplifies the entire SOD lifecycle.

When faced with this challenge, organizations may find it expedient to adopt a coarse-grained analysis of composite or enterprise roles, offered by some provisioning services. However, as they evolve, they quickly lose track of what privileges are included in these broad sets of roles, which makes coarse-grained SoD inaccurate and unreliable. Such seemingly elegant solutions, in fact result in audit objections that are expensive in the long run.

Pre-integrated & Embedded: Advanced HCM Controls is the only pre-integrated solution that provides fine-grained SOD analysis of functional and data security across all privileges, role hierarchies, and user assignments, for Oracle HCM Cloud.

ESTABLISH INDUSTRY BEST PRACTICES WITH PRE-BUILT LIBRARY OF CONTROLS

The library of controls is based on best business practices and over a decade of customer experience that add value by recognizing ground realities and important considerations from successful implementations.

Sample Access Controls:

- Ghost Employee Fraud: Payroll and Employee Transaction by Same User
- SOD: Find users who can run payroll and create employees
- Find Employee bank account information changed multiple times in the last 30 days
- Multiple deposits to same account per payroll run
- Employee logs too many hours per payroll period
- SOD: Find users who can run payroll and update time cards

Configure Pre-Built Controls to Monitor Policies: Advanced HCM Controls lets organizations configure pre-built controls to enforce access policies, such as segregation of duties, and limited access to sensitive data and superuser privileges.

Accelerate Implementation: The application delivers pre-built controls that are ready to use, accelerating deployment and increasing return on investment. These controls can be up and running quickly to automate monitoring of access controls and ensuring segregation of duties.

RESPOND TO EVOLVING NEEDS BY AUTHORING NEW CONTROLS

Organizations can meet their specific requirements by modifying existing controls or authoring new controls, using a visual editor. Users can author controls by specifying combinations of access point

Mitigate Risk and Strengthen Compliance

Key Benefits

- Strengthen fraud and security controls
- Prevent fraudulent payments
- Lower cost of compliance with controls
- Provide separation of duties

privileges that would violate an access policy. A set of privileges may also be grouped into broader entitlements to reduce complexity, and provide ease of use and maintenance.

Advanced HCM Controls' authoring workbench provides easy–to-use building blocks to construct powerful searches using conditional filters and Boolean logic such as AND and OR. This provides users unparalleled ease and flexibility to specify unacceptable access conflicts.

MANAGE ACCESS CONFLICTS USING SOPHISTICATED ANALYSIS

Visualize Results Instantly to Identify Root Causes of Conflicts: AAC displays entire access paths from roles to privileges to allow users to quickly identify the source of the conflict, and help develop a remediation plan.

Optimize Role definitions: By identifying & addressing access conflicts within any given role, organizations can rapidly rationalize roles that have inherent access conflicts. This leads to a quick resolution of conflicts, and accelerates implementation design and deployment.

Prioritize responses to access violations: Organizations can choose to respond to access risks pragmatically, based on the severity and ground realities. They may choose to either remediate access conflicts, or accept conflicts and monitor transactions by deploying compensating controls.

Simulate Impact of Remediation Actions: Users can simulate & evaluate the impact of remediation actions, and assemble a multi-step plan before deploying.

Minimize Manual Interventions: AAC identifies each conflict and tracks its status without the need for any manual intervention. As users deploy remediation steps, on each subsequent analysis, AAC automatically determines if a previously identified conflict has been resolved, and closes it.

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