ORACLE DATA SHEET

ORACLE ADVANCED ACCESS CONTROLS CLOUD SERVICE

ORACLE
RISK MANAGEMENT CLOUD

Advanced Access Controls (AAC) Cloud Service enables continuous monitoring of all access policies in Oracle ERP, potential violations, insider threats and fraud. It automates security analysis to ensure segregation of duties, and 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 ERP Cloud.

KEY FEATURES

- Continuously monitor access policies
- Pre-built Best Practice Controls for Segregation of Duties
- Graphical Workbench for users to author and configure controls
- 6,000+ ERP Cloud access entitlements & access points to configure controls
- Remediation of access conflicts supported by visualization & simulation
- Integration with Financial Reporting Compliance Cloud Service
- Embedded dashboard with analytics and reporting

Protect against Fraud & Insider Threats by Enforcing Access Policies

AAC provides comprehensive management of application access. It automates security analysis, identifies violation of access policies, helps rationalize roles and remediate conflicts, and ensures segregation of duties.

AAC 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 ERP Applications -** by designing roles that are free of SoD conflicts.
- **Ensure compliance with audit requirements and mandates (such as SOX) –** by auditing access privileges.
- **Protect information assets from insider threats–** by limiting and monitoring access to sensitive data and super-user privileges.

Ensure Segregation of Duties by Automating Security Analysis

Complete scans of full access-paths: AAC 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

ORACLE

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: AAC 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 ERP Cloud.

AAC also complements Oracle Cloud Access Security Broker with data analysis of who has valid and authorized access within Cloud ERP, and may be resorting to malicious transactions or causing errors

- RELATED SERVICEs
- Oracle Financial Reporting Compliance Cloud Service for streamlined internal assessments and compliance
- Oracle Advanced Financial Controls Cloud Service for monitoring financial transactions.
- Oracle's Cloud Access Security Broker Service for monitoring multi-cloud environments, network traffic, and suspicious Cloud activity.

Upgrade to Industry Best Practices with Pre-built Library of Controls

Upgrade to Industry Best Practices: 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
Reconcile Bank Accounts and Enter Customer Receipts
Create Payments and Create Purchase Orders
Create Payables Invoices and Receive Goods & Services
Verify Physical Inventory and Receive Goods & Services
Enter Customer Receipts and Return Goods & Services

Configure Pre-Built Controls to Monitor Policies: AAC lets organizations configure pre-built controls to enforce access policies, such as segregation of duties, and limited access to sensitive data and super-user 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

Author Controls Graphically: 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 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.

AAC's 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 & flexibility to specify unacceptable access conflicts.

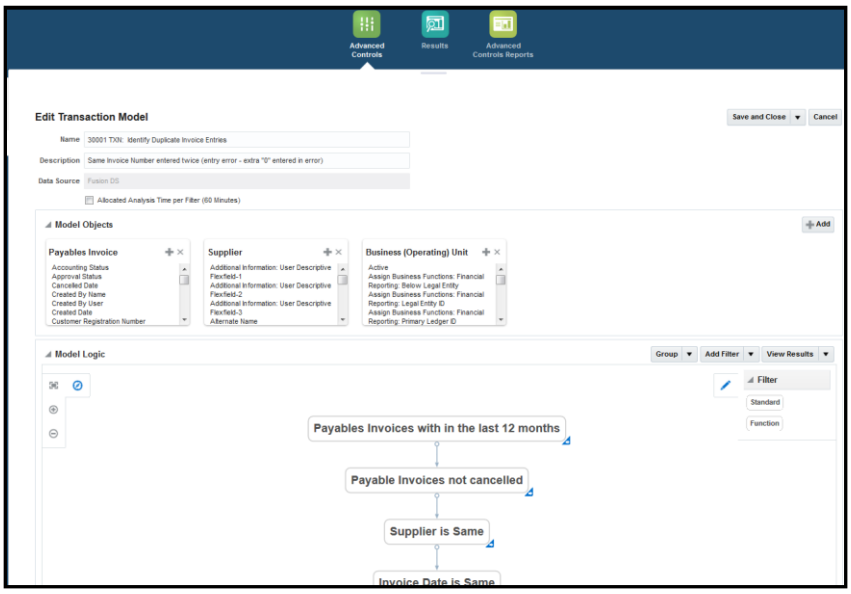

Figure 1. Advanced Access Controls Graphical Control Design Workbench

Sample Access Points	
Financials	Enter Journal Run Balance Sheet Closing Journals Program Manage Bank Account Approve Payables Invoice
Procurement	Maintain Supplier Create Purchase Order from Requisitions
Supply Chain	Receive Receiving Shipment Line Create Miscellaneous Transactions Approve Physical Adjustment

Sample Access Entitlements	
Financials	Create Payments Enter Customer Receipts
Procurement	Create Supplier Create Purchase Order
Supply Chain	Receive Goods & Services Create Inventory Transactions Manage Physical Inventory

The library consists of over 6,000 pre-built Entitlements & Access Points.

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.

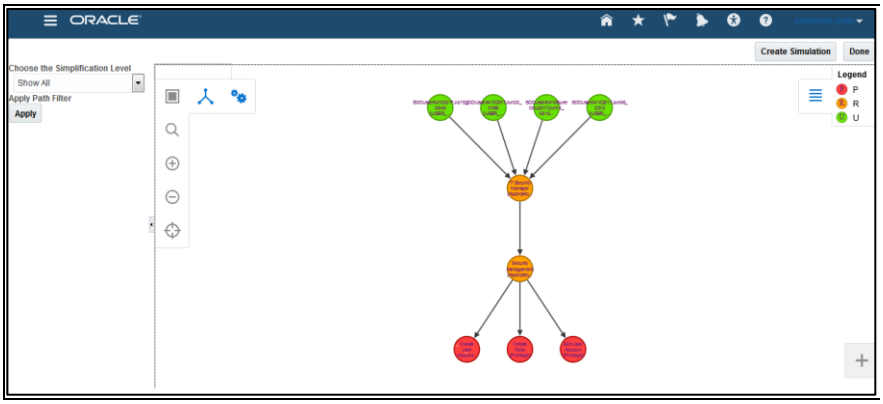

Figure 2. Advanced Access Controls offers visualization of access conflicts

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 chose 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.

Implement Integrated Risk Management using an Embedded Solution

Substantiate Financial Reporting Compliance: AAC Control Analysis yields powerful Audit results, which can be related to documented business risks. It enables Access Certification, the process of documenting the results of SoD analysis, so that it is readily available and verifiable as audit evidence. This ensures additional scrutiny of access privileges by line managers, and enforces accountability.

Controls Analysis & Results serve as powerful and objective evidence to substantiate compliance with access policies, as part of Internal Controls Framework.

Achieve a pragmatic balance between control and productivity: Organizational access control needs vary between business units, locations, business processes based on the number of employees. For instance, when faced with limited employee resources, organizations often need to grant wider access privileges to certain users, thereby introducing SoD risk and vulnerability. Oracle Risk Management offers transaction monitoring to mitigate risk in such situations.

Occasionally, situations arise where a certain user has to be intentionally granted excess privileges to carry out certain tasks, which may violate established SoD policies. This may be caused by another employee's absence, or to fix a one-time issue, under time-constraints.

Under such circumstances, organizations can limit their exposure by granting additional access to specific users for a limited time, rather than changing role definitions. They can also monitor the activity of such users within that time window, to mitigate risk and collect audit evidence.

Provide Executives with Continuous Insight & Metrics: Create confidence in the security and the effectiveness of access controls by providing information that is easy to understand. Executive dashboards can be configured to display actionable insights related to access risks for timely follow up and quick resolution.

Comprehensive and Embedded – Evolves as You Grow

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

Ensure Segregation of Duties	• *Automate Security Analysis* *Analyze access privileges using complete scans of all access paths* *Identify root cause of access violations by visualizing access conflicts*
Upgrade to Industry Best Practices	• *Upgrade your existing controls to industry best practices* • *Get immediate value by using pre-built controls* • *Reduce complexity by grouping fine-grained privileges into functional entitlements*
Author New Controls	• *Empower users to author new access rules and policies graphically* • *Accelerate authoring of new controls graphically by leveraging a library of 6000+ pre-built access points in Oracle Cloud.*
Remediate Access Violations	• *Optimize role definitions by addressing intra-role conflicts* • *Respond to risks based on severity* • *Remediate conflicts, or choose to monitor with compensating controls* • *Evaluate remediation plans by simulating impact of proposed changes on results*
Manage Application Access Risks using an embedded solution	• *Strengthen/Substantiate Financial Reporting Compliance efforts with access audit results.* • *Assess risk mitigation value, and prioritize access controls* • *Link access analysis results to Financial Reporting Controls* • *Mitigate access risks by monitoring transactions using compensating controls in Advanced Financial Controls*

ORACLE

CONTACT US

For more information about Advanced Access Controls, visit cloud.oracle.com/risk-management-cloud or call +1.800.ORACLE1 to speak to an Oracle representative.

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

Integrated Cloud Applications & Platform Services