ORACLE
ADVANCED CONTROLS

ORACLE APPLICATION ACCESS CONTROLS GOVERNOR - FOR E-BUSINESS SUITE

KEY FEATURES

- Continuously monitors application users access from high-level EBS roles and responsibilities to detailed access points
- 450+ Delivered, ready-to-deploy access controls
- 135 + Delivered access entitlements, that logically group similar access points
- 100,000 + Delivered EBS access points: responsibilities, menus, sub-menus, concurrent programs and functions
- Pre-built connector to E-Business Suite
- Role-based remediation of user access incidents supported by application worklists, notifications and workflow
- Simulated remediation plans before deploying to operational environment
- Delivered dashboard analytics and reporting
- Integration with Enterprise Governance, Rick and Controls Manager and Intelligence
- Web Services for closed-loop preventive user provisioning
- Extensible to third-party, in-house and legacy systems
- User-friendly design for business users to author and configure controls

Appropriate implementation of segregation of duties (SOD) is a core tenet of financial reporting and IT governance. Complying with access policies using manual solutions quickly becomes unwieldy and unreliable. Oracle's Application Access Controls Governor (AACG) is a module within the Oracle Advanced Controls suite which is part of the Oracle GRC Suite of products. AACG provides automated, advanced controls that monitor fine-grained access of all e-Business Suite (EBS users, augmenting standard user and role provisioning to EBS applications.

Comprehensive Application Access Management

Oracle's Application Access Control Governor (AACG) is the market leading application for comprehensive management of users access to ERP systems. Beginning with an extensive library of pre-delivered controls, access entitlements and ERP access points,AACG has its own library of controls covering all major business processes. AACG supports a range of frameworks and regulations including Sarbannes-Oxley (SOX), industry and IT governance franeworks lowering compliance costs and increasing manageability even across mulitple, hetereogeneous ERP systems. AACG automates access policy documentationand assessment processes. AACG promotes efficiencies by utilizing an exception-based user access attestation process thereby eliminating redundant effort of atttesting every quarter when position, roles and responsibilites have remained the same.

AACG is a unique solution that analyzes user acess well beyond users and their role level assignments. EBS users, both within and between roles, can often have conflicting and even toxic access privileges as a result of the multiplicity of possible access points and pathways including: permission lists, menus, sub-menus, pages and functions. Finally Auditors assess the validity of users' fine-grained access privileges and determine whether SOD controls are in place and working effectively.

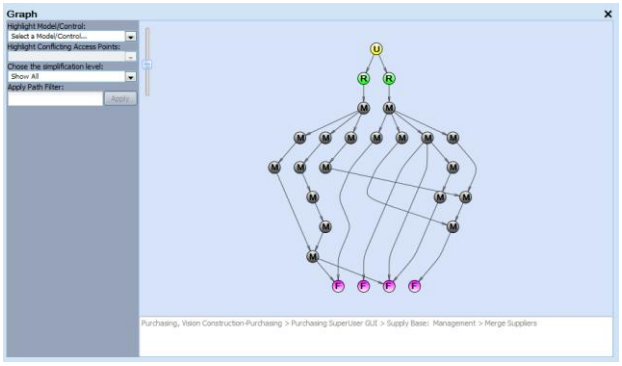

Figure 1: Oracle Application Access Controls Governor Visualization displays fine-grained analysis of complete user's multiple access paths from Users, Roles, Menus, Sub-menus to Functions in an e-Business Suite system.

ORACLE

KEY BENEFITS

- Detect and prevent inappropriate user access in violation of control objectives, access policies and regulations
- Augments EBS access assignments with fine-grained controls
- Remediate access conflicts quickly with automatic notifications, worklists; intelligently eliminates 'false positives'
- Controls user setups to manage operational and project risks for EBS implementations and upgrades
- Preventive user provisioning manages access approvals for new hires and ongoing role management
- Reduces cost of internal and external audits

Closed-Loop, Compliant User Provisioning

Enforcement of access policies in the EBS system extends to: detecting who has privleges to create, edit and or delete critical system setup data and configurations such as spending authorization limits, opening closed accounting periods; who can enter and maintain master data for example for suppliers, customers; employees and item master data; who can enter potentially harmful transactions such as creating invoices and then paying those invoices, who can create purchase orders and then records receipts for those orders, to name just a few. Cleaning up user access and EBS roles and keeping the system healthy from a SOD conflicts is critical.

Today's enterprise requires a closed-loop, compliant user provisioning system to detect and correct existing users' access, all the while maintaining proper SOD going forward as new users are brought into the system, assigned new responsibilities or are reassigned responsbilies. AACG supports preventive user provision by integrating directly with Oracle EBS and Oracle Identity Management using web services application program interfaces as well as third party identity management systems. Oracle AACG has three types of SOD control enforcement: monitor; prevent; approval required. When "prevent" or "approval required" enforcement types are selected, onboarding new or transferring existing users will call AACG to analyze and check for fine-grained SOD violations and return these results to the provisioning system. New users or existing users with new responsibilities are provisioned in a pro-active and preventive manner to efficiently manage to SOD rules.

Managing Users with Broad Access to Sensitive Data

Certain activities and types of users present special challenges when it comes to managing SOD, like super-user access, granting energency access, and dividing roles and responsibilities among only a few users in smaller organizations. In all these cases, having perfect, single SOD control is sometimes not possible. An AACG control with enforcement type set to "approval required" assures that access is being actively reviewed before being accepted. Additional compensating SOD controls can be identified and put in place to help offset these challenging cases. Oracle's Enterprise Transaction Controls Governor (ETCG) is an integrated application in the Oracle Advanced Controls Suite. ETCG can automatically and continuously monitor transaction activity conducted by users with overly broad access to sensitive data. High-risk activities such as transacting cash receipts and payments against invoices for instance can be monitored for fraudulent activity. Configuration Controls Governor and Preventive Controls Governor - all part of the Oracle Advanced Controls Suite – can also be used as a system of compensating controls overlapping and reinforcing the controls framework.

Relevant SOD Incidents and Smart Remediation

An important part of an SOD solution must include remediation features and functionalty to manage SOD incidents. The initial dectection and prevention of SOD violations can be a big undertaking depending on the numbers of users, roles and EBS instances that are being managed. Automated SOD controls will find many more violations than manual controls and data sampling techniques. Oracle AACG makes sure that the SOD incidents generated are relevant and reported and resolved in the most efficient and way possible. AACG features such as Global Conditions excludes "false positives" or incidents that pose no real SOD risk. For instance, view-only privileges to a supplier is a valid access point but has little or no SOD risk since the user cannot add, delete or change supplier information using this function. AACG Global Conditions can be applied once and all access controls will adopt this filter, excluding view-only access to suppliers and thus not creating incidents for these "apparent" access conflicts Other AACG features that help manage and eliminate irrelevant SOD

RELATED PRODUCTS

Oracle's Advanced Controls is a suite of applications that enforces controls directly in Oracle's E-Business Suite and PeopleSoft Enterprise applications. Oracle's embedded approach increases financial integrity, reduces risk, and optimizes stakeholder value.

- Oracle Applications Access Controls Governor documents, manages, remediates and enforces access policies for effective segregation of duties.
- Oracle Configuration Controls Governor enforces application and data integrity, audits changes to data, monitors setups, and ensures accurate reporting
- Oracle Enterprise Transaction Controls Governor continuously monitors policies, controls, and transactions to detect suspicious business activities.
- Oracle Preventive Controls Governor prevents unauthorized changes to critical application data and setups, and enforces real-time policy changes at a granular application level.

Oracle GRC is comprised of Oracle Advanced Controls, EGRCM and FGRCI applications:

- Oracle Enterprise Governance, Risk and Compliance Manager (EGRCM) forms a documentary record of a company's strategy for addressing risk, controls and regulatory compliance.
- Fusion Governance, Risk and Compliance Intelligence (FGRCI) provides dashboards and reports that pre-sent summary and detailed views of data generated in GRC.

incidents are Path Conditions and User Defined Access Points where controls can be further fine-tuned to ignore certain combinations of access points as well as specific access path configurations, again reducing unneccesary SOD incidents that create noise and waste time closing these incidents.

Getting a valid and usable set of SOD incident data is the first step toward efficient remediation. AACG worklists and notifications ensures that pending incidents are being investigated according to AACG job and duty roles and status updates are applied and tracked through to closure.

Changing a user's access to certain menus, pages and functions in order to resolve SOD violations could have unintended consequences that might prevent users from performing valid job activities. Using AACG Simulations, remediation steps are identified and tested in the AACG environment before the EBS system adminstrator applies change order requests to the operating environment.

Once an incident is addressed by changing a users access in EBS, subsequent periodic, scheduled runs of the controls will automatically close related pending incidents. AACG applies unique self-learning logic to automatically make status updates to the effected incidents and worklist entries without requiring manual updates to pending incidents.

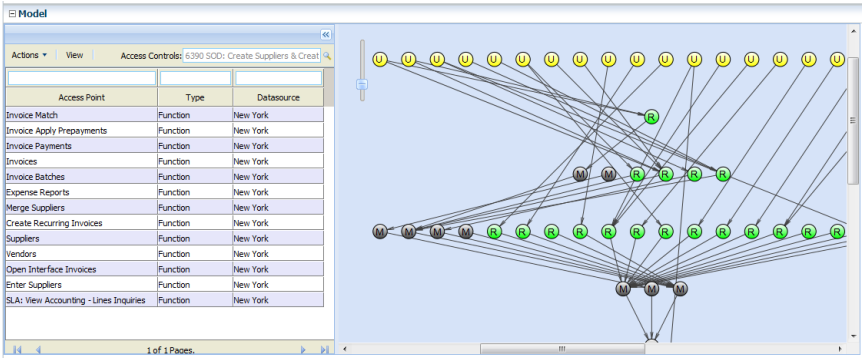

Figure 2: Oracle Application Access Controls Governor Simulations enables remediation planning and steps before updating operational environments.

Pre-built Connectors and Policy Controls

ACCG has a library of more than 400 high-value advanced SOD controls that mitigate user access risks to ERP daily operations and implementation projects. Controls are powered by delivered business objects that map ERP users to their roles, menus, sub-menus, and functions. Business objects such as AACG Entitlements group similar EBS Access Points and empower business users to configure their own controls without any special technical knowledge or query scripting. All AACG controls have a user-friendly "drag and drop" design workbench where business users either deploy the pre-configured controls as delivered, modify certain parameters for their specific needs or configure wholly new controls for their unique, specific requirements. AACG intuitive design utilizes conditional filters and Boolean logic as compared to other solutions that are technical, proprietary and maintenance intensive. Instead of complex and fragile control syntax that must be learned and maintained, AACG uses search technology to find SOD incidents that satisfy the control's conditions. The AACG connector to EBS performs full and incremental data synchronization, graphing the EBS authorization model that supplies controls with the most up-to-date data.

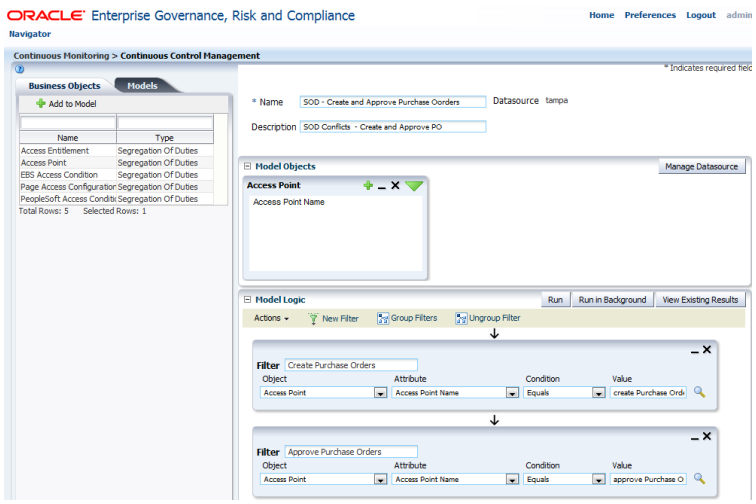

Figure 3: Oracle Application Access Controls Governor Modeling Workbench empowers business users to easily configure SOD controls using delivered Business Objects and an intuitive drag and drop design to setup conditional model logic.

Configurability and Extensibility

Choose and license available pre-built connectors and controls, considering your EBS configuration. AACG can also map access points across complex, heterogeneous configurations of business applications and extends to any application system including third-party and in-house legacy systems, thereby replacing scripts and costly manual controls. AACG supports any authorization model including Role Based Access Controls (RBAC) and Multi-Organization Access Controls (MOAC), In addition, AACG can be extended by any user provisioning system. AACG workflow notifications can be extended with Service Oriented Architecture (SOA) integration.

Integrated Suite of GRC Applications

AACG can be implemented either as a separate application or as a component of an integrated Advanced Controls Suite. AACG is integrated with Enterprise Governance, Risk and Compliance Manager sharing a single, common security implementation based on user privileges and data roles. AACG incidents display in EGRCM as results and are associated with specific controls, risks and processes. Worklists and notifications prompt and alert investigators to resolve pending incidents. Controls and incident dashboards deliver analysis, trends and reports across the enterprise and multiple ERP instances within a single and secure role-based view. Dashboards, summary and detail reports are embedded in AACG using GRC Intelligence (GCRI) or can be run in a separate environment.

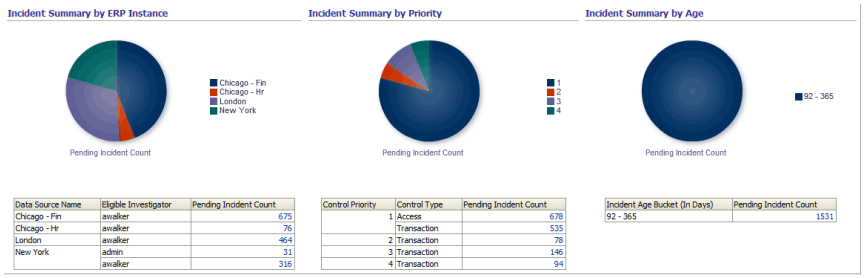

Figure 4: Governance, Risk and Compliance Intelligence monitoring of both SOD and transaction incidents across both EBS and PeopleSoft applications.

Contact Us

For more information about [insert product name], visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together