Quick, Cloud-based Segregation of Duty Conflict Reporting for SAP®

Access Analyzer expedites the process of identifying and remediating Segregation of Duty (SoD) and sensitive access risks. This greatly simplifies the challenge of eliminating internal control violations and achieving compliance without the need for a large capital project. The foundation of Access Analyzer is an industry-leading, customizable Big 4-proven rulebook that contains over 250 SoD rules across 100+ business tasks, all of which are defined down to the authorization object level.

PRODUCT BENEFITS

- Delivers fast uptime with the lowest total cost of ownership in the market today

- Provides intuitive, web-based dashboard reporting with drill-down capabilities

- Gives visibility into the source of risks by user, role and business process with rich, in-depth utilization intelligence

- Sets mitigating controls for more accurate risk reporting, and simulates new role changes for risk impact

WHY ERP MAESTRO?

70% Used by 7 of the world's top 10 audit firms

75% Average reduction in access risks after 90 days

<1 SaaS-based application requires less than one-hour implementation time

0 Access-related audit deficiencies

Automate SoD access and risk analysis. **Call us for a demo today!**
Contact us at 866.350.9106 or erpmaestro.com/contact

A Suite of Reports Designed for
Audit, IT and Executives

Access Analyzer makes IT and auditors happy with a range of SoD and Sensitive Access risk reports that satisfy executives' and auditors' needs to see the bigger picture, while giving IT and security teams the depth of intelligence needed to solve access issues quickly. The result is alignment and joint ownership of access risks across the business.
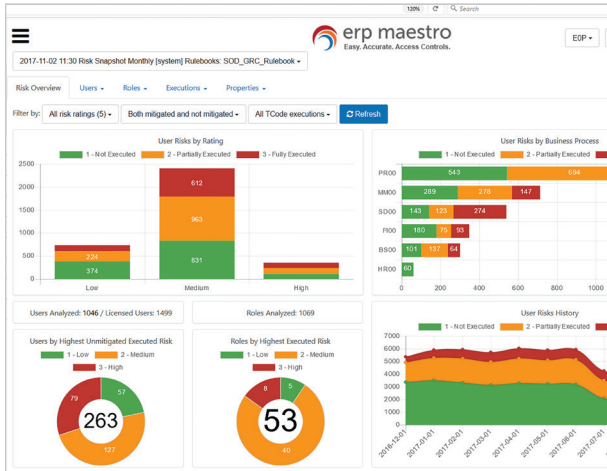
Online Dashboard Reporting

A high-level drill-down dashboard allows companies to visualize the current state of access risks ranked by level (high, medium and low), as well as by user, role and business process. Drill down further to understand the source of risks and possible remediation actions.
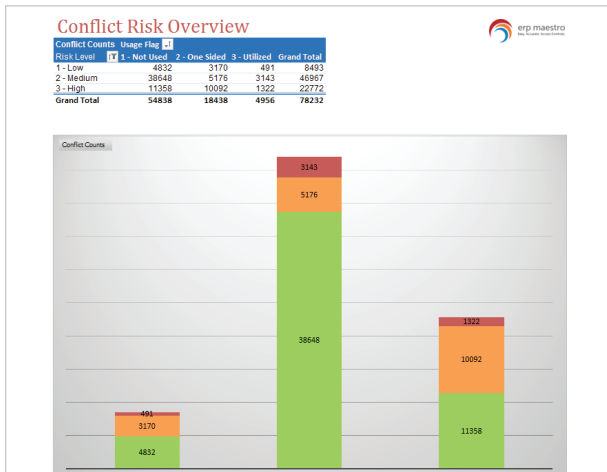
Conflict Risk Overview

Provides a company-wide SoD risk snapshot for two conflicting functions. This is broken down by risk level and overlaid with actual utilization, to provide a total number of conflicts. This unique layer of business intelligence dissects the conflict and categorizes the risk, based on whether both, only one, or none of the functions have been used.

BPO Conflict Report

Focused on the business user, this report translates technical terms to plain English. It lists all users with access conflicts and the specific risks related to these conflicts. It provides both the visibility into areas that need corrective action and the recommended action for each conflicting business function.

User Conflict Matrix

The report provides SoD rules, functions and transactions mapped to users within the matrix. Companies can remediate based on whether the user has access to the function/s and whether they have actually executed it.

Role Conflict Matrix

Provides transaction usage at role level and keeps roles from bloating. It highlights all of the single and composite roles that inherently cause conflict risks within the SAP security environment.
The report also identifies which users with access to the roles analyzed are actually executing the related tcodes.

Security Roles Report

The Security Roles Report lets you predict the impact a change would have on any given role, by knowing the transaction codes used by each user. This is done in the context of the entire role, all transaction codes and all users. It's useful for job-based role design environments that have bloated job responsibilities.

Sensitive Access Analysis

With the Sensitive Access Report, business users and executives can actively monitor the base of SAP users with access to sensitive functionality for audit and operational purposes.

Mitigating Controls

This feature allows the risk owners to setup mitigating controls for risks by user, role or transaction. This allows for a more accurate view of the organization's risks for reporting & compliance.

Control form (screenshot)

Field	Value
Control Id	M01
Name	M1
Type	Automatic Detective
Frequency	Quarterly
Control Objective	ensure all PO's are reviewed before payments
Control Description	PO's are manually reviewed every month
Requires Testing	☑

Rules Mitigated

EM_SOD_Baseline	SOD_BS06	Basis Utilities (BS04) vs. System Configuration (BS06)
EM_SOD_Baseline	SOD_FI03	Cash Application (AR02) vs. Bank Reconciliation (FI03)
EM_SOD_Baseline	SOD_MM01	Maintain Asset Document (FA01) vs. Goods Receipts to PO (MM05)
EM_SOD_Baseline	SOD_MM04	AP Payments (AP01) vs. Goods Receipts to PO (MM08)
EM_SOD_Baseline	SOD_MM11	Purchasing Agreements (PR05) vs. Clear Differences - WM (MM08)
EM_SOD_Baseline	SOD_PU05	Maintain Bank Master Data (FI04) vs. Manual Check Processing (AP04)
EM_SOD_Baseline	SOD_SD09	Sales Pricing Condition (SD06) vs. Process Customer Credit Memos (AR06)
EM_SOD_Baseline	SOD_SD10	Delivery Processing (SD02) vs. Maintain Customer Master Data (SD01)

Map Rules

Owner	support
Created	support 06/30/2015 10:14:28 -04:00
Last updated	zach.shapiro@erpmaestro.com 07/21/2015 13:12:27 -04:00

Save

What-If Simulation

Generate an analysis that details which users and roles are at risk for potential conflicts.

WhatIf Report

JobID	WhatIf Analysis Name	User ID	Role Name	Role Change
4024	new id check	AIDA.DEJESUS	R:BC....:APPLICATION_DISPLAY	Remove
4024	new id check	AIDA.DEJESUS	R:BC....:CONFIG_DISPLAY	Remove
4024	new id check	AIDA.DEJESUS	R:BC....:CORE_TEAM	Remove
4024	new id check	AIDA.DEJESUS	R:BC....:DEVELOPER_DISPLAY	Remove
4024	new id check	AIDA.DEJESUS	R:FIN....:AP_INVOICE_CLERK	Add
4024	new id check	AIDA.DEJESUS	R:FIN....:CASH_APP_MANAGEMENT	Add
4024	new id check	AIDA.DEJESUS	R:FIN....:CUST_CREDIT_MAINT	Add
4024	new id check	AIDA.DEJESUS	R:FIN....:EU_INSTRASTAT_REPORT	Add
4024	new id check	AIDA.DEJESUS	R:FIN....:PROCESS_PAYMENT_PROP	Add
4024	new id check	AIDA.DEJESUS	R:FIN....:RELEASE_PAYMENT_PROP	Add
4024	new id check	AIDA.DEJESUS	R:FIN....:AR_CREDIT_RELEASE	Add
4024	new id check	AIDA.DEJESUS	R:FIN....:BILLING_CREDIT_MGMT	Add

Fast, Powerful, Secure

Our cloud-based software as a service allows for unprecedented agility, enabling most clients to be up and running Access Analyzer reports in less than an hour. Because our application is web-based, there are never any upgrades, you're always using the latest version. Access Analyzer is SOC II-certified and never extracts PII or sensitive data in the course of running its analyses. Powered by Microsoft Azure, our cloud architecture employs the strongest industry-standard security measures available, including SSL encryption.

Leading organizations around the world choose ERP Maestro for secure access controls and compliance

FARO · AMYRIS · GE · tyco · PeroxyChem · zulily

Call or Visit Us Online

1.866.350.9106 | erpmaestro.com

SAP® Certified
Integration with SAP Applications

SAP Silver Partner