ERP Armor Data Sheet

ERP Armor

ERP Armor is designed to evaluate risk through the Assessment phase and to resolve risk through control and role design in the Design and Build phase. Once the risks have been remediated, we provide continuous protection through the Maintain phase with ERP Armor as a Service.

Rules and Roles

ERP Armor is segmented into Rules and Roles, and both are among the most advanced in the industry. **ERP Armor: Rules** is composed of Segregation of Duties conflicts and Sensitive Access rules. **ERP Armor: Roles** are standard custom roles tested at over 100 customers and ready to be deployed in your environment. The Roles are used for Role Design projects along with Role Design Studio.

ERP Armor Architecture

The heart of ERP Armor is the design of your ERP Risk solution that blends a proven ERP Risk Architecture and ERP Risk content developed over 20 years. We take a "security first" approach to compliance by focusing on Sensitive Access conflicts first and then Segregation of Duties rules in **ERP Armor: Rules**. Our architecture also separates configurations and transactions leading to an effective change management strategy. Our ruleset works with industry leading GRC Software and Assessment solutions and includes quarterly updates. This approach can also be found in **ERP Armor: Roles**, where our architecture leads to efficient and effective role design.

ERP Armor: Reports

ERP Armor: Reports is a set of reports and queries that allow both Internal Auditors and External Auditors access to data and analysis needed to assess ERP risk.

Any ERP, Any GRC Software Solution

We support any ERP and any GRC software solution, including proprietary and internally developed solutions. Our foundation has delivered the industry's most complete ruleset for Oracle and we are extending into SAP, Microsoft, Workday, Salesforce and Coupa. We can also integrate with any internal custom solution and other ERP systems.

Contact us

From initial engagement to solution design, our team of experts works closely with you to develop an ERP risk approach with a Risk Assessment, Design, Build, and Maintain process. We recognize every client is at a different stage, so we bring recommendations and resources to complement your risk team. Please contact us at info@erpra.net.

ERP Armor: Rules – Sensitive Access and SoD rules

E-Business Suite: Controls monitoring for more than 500 tables, mapped to specific risks. Extensive library of Sensitive Access conflicts and Segregation of Duties rules covering:

- Rules: SoD/SA over 1,200, Functions – 3,805, Concurrent Programs – 4,546

ERP Cloud: Controls monitoring for more than 1,800 objects, mapped to specific risks. Extensive library of Sensitive Access conflicts and Segregation of Duties rules covering:

- Rules: SoD/SA over 340, Privileges – 2,212

Both E-Business Suite and ERP Cloud (common to both)

Segregation of Duties Conflicts	Sensitive Access Rules
Maintain Suppliers vs Enter PO's	Maintain Suppliers
Maintain Suppliers vs Enter AP Invoices	Enter AP Invoices
Maintain Suppliers vs Enter AP Payments	Enter AP Payments
Enter AP Invoices vs Enter AP Payments	Enter Journals
Enter Journals vs Post Journals	Post Journals
Enter Journals vs Journal Sources	Journal Sources
Maintain Customers vs Maintain Orders	Document Types
Enter PO's vs Document Types	Line Types
Enter PO's vs Line Types	Profile Option
Enter AP Payments vs Payables Options	Profile Option Values

E-Business Suite

Segregation of Duties Conflicts	Sensitive Access Rules
Enter Journals vs Accounting Setup Manager	Accounting Setup Manager
Users vs Menus	Purge Programs
Users vs Request Groups	Menus
Users vs Responsibilities	Responsibilities

ERP Cloud

Segregation of Duties Conflicts	Sensitive Access Rules
Users vs Roles	Users
Users vs Manage System Security Options	System Security Options

Revision 1.1 May 20, 2020

ERP Armor: Roles – Standard Custom Roles

Our **ERP Armor: Roles** library contains 91 roles for EBS and 74 for ERP Cloud. We offer our 'core' IT roles with a subscription to **ERP Armor: Rules**, shown below. For more details, such as the roles for Financials, SCM, HCM, Manufacturing, and others please contact us.

E-Business Suite:

Role Name	Role Description
Sys Admin View Only	View only access to most of the key activities contained in System Administrator, Application Developer, Functional Administrator, Functional Developer, System Administration, and Alert Manager.
User Provisioning	Role designed for help desk users and others who are authorized to do user provisioning. Has the ability to set up a user, reset passwords, and assign Responsibilities to users.
IT Role Configuration	Ability to make changes to Roles via the following functions: Responsibilities, Menus, and Request Groups. Also has the Menu cloning process via Functional Administrator.
IT DBA Configuration	Broad range of configurations that should be subject to the change control process including forms that allow SQL injection. Used primarily when DBAs are asked to move a broad range of development into Production.
Profile Option Configuration	Ability to set profile options through the System Profile Values form.

ERP Cloud:

Role Name	Role Description
Audit Policy Maintenance and Reporting Job Role	Ability to enable and disable audit policies and report on the data. Changes to Audit Policy configuration should go through the Change Management process. No 'Control Owner' should have access to this Role since they could disable the Audit Policies and undermine the control.
Audit Policy Reporting Job Role	Ability to report on the audit policy data. Used by control owners to report on data needed to execute their controls.
User Provisioning Job Role	Provides the ability to create and maintain users, email address, and assign roles to users; also provides ability to reset passwords and disable users. This would be granted to someone who currently has IT Security Manager but should be only authorized to do user provisioning.
Security Configuration Job Role	Provides the ability to build and modify custom roles and all other activities from the IT Security Manager role, other than the User Provisioning abilities. This should only be assigned to IT. All activity through this role should be subject to the Change Management process.
Security Inquiry Job Role	View only access to Users and Assigned roles as well as Role definitions. Also has ability to run reports such as User Role Membership Report and User and Role Access Audit Report.

ERP Armor: Reports – Access to Data and Analysis

ERP Armor: Reports is a set of reports and queries to allow IT Users, Internal Auditors, and External Auditors access to data and analysis needed to assess ERP Risk. We have a large library of pre-built reports and will provide you with new, updated reports based on your needs.

Change Management Population

If you are looking for a population of changes, we can help! Whether you are an IT Auditor, External Auditor, or in IT performing quality assurance over your Change Management process, we can provide reporting for a complete population of changes. We can also work to provide audit support and messaging for your audits.

Continuous Controls Monitoring

Our reporting capabilities can periodically snapshot your data and provide you with the answers you need to test your IT controls and functional controls. Our knowledge of the underlying data model and our 20+ years of experience will provide access to the data you need.

E-Business Suite Examples:

Report	Report Description
Change Management Population	Data from 100+ tables as a population of changes you can use for your Change Management population
SQL Injection	Identify the current state of the data via the Forms that allowed SQL injection
Purchase Orders with Two-Way Match	Where your policy requires that all PO's are 3-way match, we can provide a list of PO's where the 2-way match was configured
User Password Exceptions	Users with password values not consistent with your policy

ERP Cloud Examples:

Role Name	Role Description
Change Management Population	Data from 100+ tables as a population of changes you can use for your Change Management population
Delegations Allowed	Identify the Roles that are allowed to be delegated to other Users
Profile Option Values	Provide a full population of profile options assigned
Password / SSO Configurations	Current state of these critical configurations
Enabled Audit Policies	Current state of these critical configurations and when they have last been updated

Revision 1.1 May 20, 2020