

The 10 Principles of Security in Modern Cloud Applications

Nigel King, Vice President, Oracle
In-Depth Seminars – D11

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

The Context for Applications

The Enterprise

HR Generalist

CFO

Payables
Supervisor

Marketing Manager

Procurement Manager

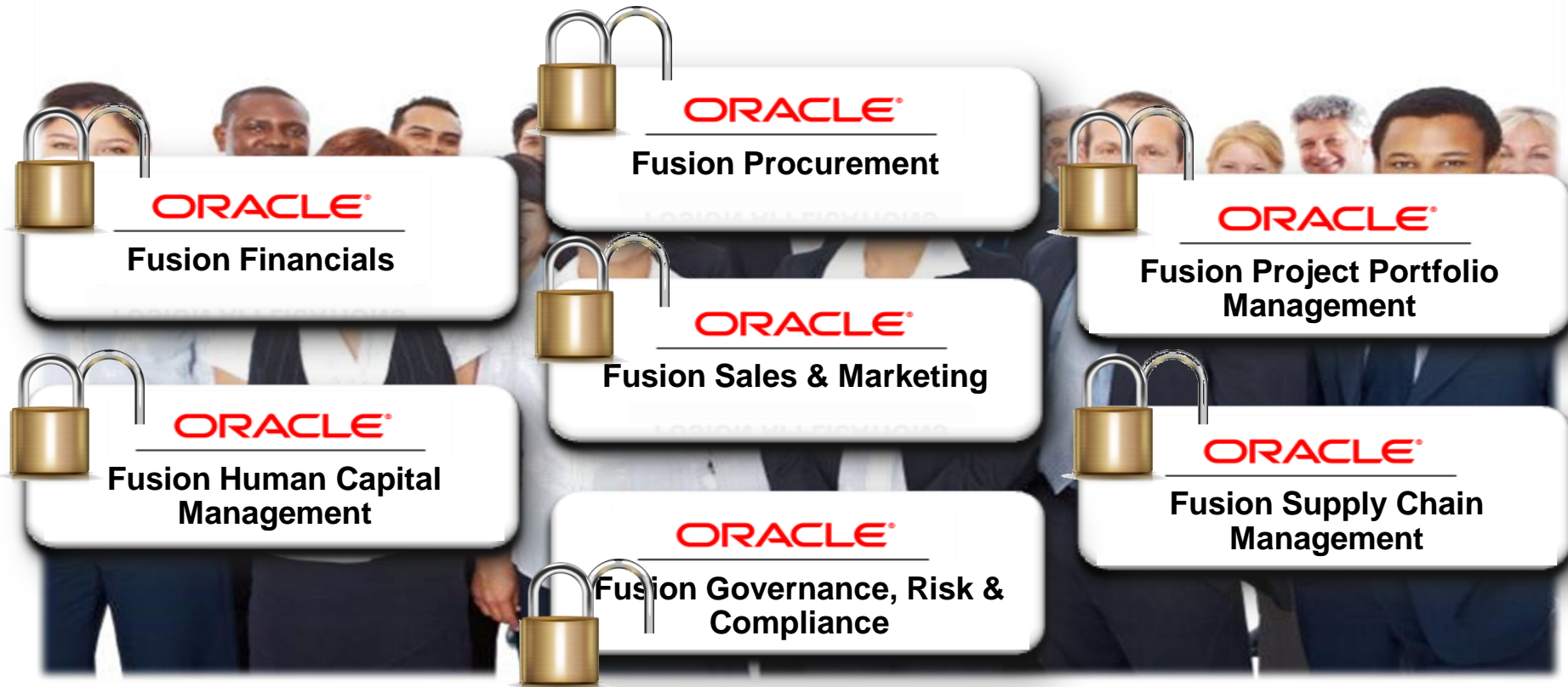
VP of Sales

Applications
Admin

Engineer

ORACLE

Functional Footprint – Role Based Access Control



Functional Footprint – Role Based Access Control



ORACLE®

Fusion Procurement



- Buyer
 - Category Manager
 - Product Manager
- INTERNAL USERS**

- Procurement Contracts Administrator
- Procurement Catalog Administrator
- Procurement Applications Administrator
- Supplier Administrator
- Sourcing Project Collaborator

- Supplier Bidder
 - Supplier Accounts Receivable Specialist
 - Supplier Customer Service Representative
- EXTERNAL USERS**

- Supplier Demand Planner
- Supplier Sales Representative
- Supplier Self Service Administrator
- Supplier Self Service Clerk

190 Seeded Job Roles across over 83 Applications

ORACLE®

- Clean Access Model
- Seamless Transition to IDM



USABILITY



PRODUCTIVITY

- Faster On boarding
- SSO
- Management Approval Workflows
- Easier Regulatory Compliance

BENEFITS OF FUSION SECURITY



RISK



ADMINISTRATIVE COSTS

- Secure Out of The Box
- Across Tools
- Across the Info Lifecycle
- SOD

- Role Provisioning
- Transparent Policies
- Standards Based

The 10 Principles

Fusion Applications Security

1. Role Based Access
2. Account and Role Provisioning Events & Workflows
3. Enforcement Across Tools and Transformations
4. Pervasive Privacy Protections
5. Integration with Governance Risk and Compliance
6. Transparent Security Policies
7. Complete Audit of Security Changes
8. Secure Across the Information Lifecycle
9. Co-existing with your current Security Infrastructure
10. Comprehensive Extensible Reference Implementation

Fusion Applications Security



Procurement Manager

[Apply now »](#)

Date: Apr 28, 2012

Location: London, ENG, GB

Responsibilities

The purpose of the Regional Procurement Manager is

- To **coordinate a team of buyers** and **1** logistic specialists to manage the project spend, NPR spend, implement sourcing strategies and realize pipeline savings.
- To create and implement project procurement strategies and plans.
- To manage material requirements, send requests for quotes;
- To **negotiate with suppliers**,
- To **place purchase orders** **3**
- To **manage logistics**
- To **perform order management according to contract/project req.** **2** and BT processes, rules and directives.
- To ensure slim, fast and efficient processes by continuously improving internal processes and tools towards world class standards, ensure people development using best practices, and manage cross-functional and external relations.
- To **optimize and manage the supply chain and ensure flawless execution with focus on delivery, quality performance, flexibility, responsiveness, and spend and price development.** **4**
- To represent Procurement in Management Meetings MOR / QPR and bring its competence in global supply chains.

Key accountabilities include

- Ensure the competence and performance of procurement project team
- Support tender/bidding process
- Roll-out divisional sourcing strategy and implement project procurement strategy and plan
- Manage purchase contracts for the project & operations in scope
- Manage supply base and improve supplier performance (delivery & quality)
- Manage Material Cost Performance

Qualifications

Degree level or equivalent in a relevant discipline.
Significant experience, preferably within an industrial environment and within a demanding safety critical environment. Ideally you will have experience within railway signalling
Able to develop effective relationships and have proven negotiation skills with the supply chain.
Ability to communicate simply and effectively at all levels and in particular across regions.
Presentable, enthusiastic and trustworthy.
Flexible and able to work accurately to deadlines
Ability to work in multi cultural environment

A Role is a Job Description

Procurement Manager

Procurement professional responsible managing a group of buyers in an organization.

General

External Role Hierarchy

Application Role Mapping

Mapping For: Procurement Manager

Each application in the table below can be expanded to see the corresponding Application Roles within their hierarchy. Select an Application Role below and click the Open button to launch a view details in a new tab.

Actions View Map Remove Roles Open Role Find Policies

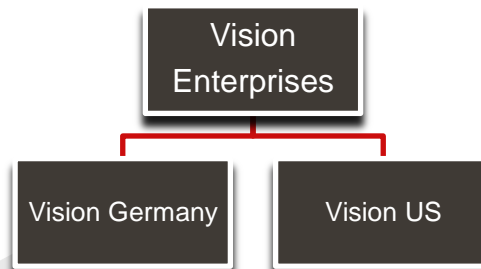
Display Name	Description
obi	
fscm	
Approved Supplier List Entry Management Duty	Perform approved supplier list management tasks including creating, changing, and re
Buyer Management Duty	Reassign purchasing transactions from one agent to another.
Contract Terms and Conditions Override Controls Duty	Is protected clauses, and deletes mandatory clauses and sections in addition to au
Negotiation Analysis Viewing Duty	View negotiation data from a business intelligence perspective as an agent.
Procurement Dashboard Duty	Access the Procurement Dashboard page. The dashboard provides quick access to spe
Purchase Document Analysis as Procurement Manager Duty	purchase order and purchase agreement Business Intelligence Applications da

A Duty is what you do in that Role.

ORACLE

Once a New Employee is inducted, You grant them a Role

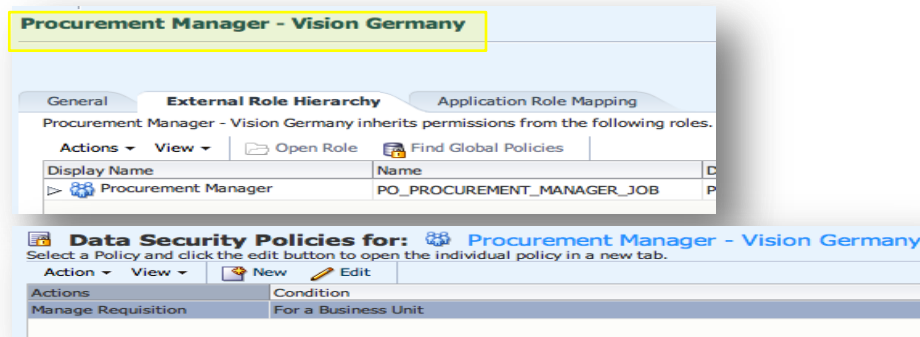
Employee Joins As
Purchasing Manager of
Vision Germany



Roles not tied to Job but
to Employee, such as

- Employee (ERs)
- Purchase Requisitioner

We call these roles:
Abstract Roles



Employee is Granted
the Purchasing Manager Role with Data Secured by
Vision Germany. We call these roles: Data Roles

What can the new Employee Do and View ?

Based on their Role assignment the Employee has duties.

Each of these duties provides access to functionality in Fusion Apps.

This Access to Functionality is what we call **Entitlements**

Procurement Manager

Procurement professional responsible managing a group of buyers in an organization.

General External Role Hierarchy **Application Role Mapping**

Mapping For: Procurement Manager

Each application in the table below can be expanded to see the corresponding Application Roles within their hierarchy. Select an Application Role below and click the Open button to launch a view details in a new tab.

Actions View Map Remove Roles Open Role Find Policies

Display Name	Description
> obi	
▼ fscm	
> Approved Supplier List Entry Management Duty	Perform approved supplier list management tasks including creating, changing, and rev
> Buyer Management Duty	Reassign purchasing transactions from one agent to another.
> Contract Terms and Conditions Override Controls Duty	Edits protected clauses, and deletes mandatory clauses and sections in addition to auth
> Negotiation Analysis Viewing Duty	View negotiation data from a business intelligence perspective as an agent.
> Procurement Dashboard Duty	Access the Procurement Dashboard page. The dashboard provides quick access to spend
> Purchase Document Analysis as Procurement Manager Duty	Access purchase order and purchase agreement Business Intelligence Applications data

Policies for: Buyer Management Duty

Functional Policies Data Security

Actions View New Open Remove

Name	Description	Targets
1 Policy for Buyer Managemen...		Reassign Purchasing Document Manage Procurement Agent

Now the New Employee Starts Using the System

Policies for: Buyer Management Duty

Functional Policies		Data Security
Actions	View	+ New ✎ Open ✖ Remove
Name	Description	Targets
1 Policy for Buyer Managemen...		Reassign Purchasing Document Manage Procurement Agent

When the Employee starts using Fusion Apps She will be able to access the **Menu Tasks** she is entitled to.



Reassign Purchasing Documents

Name: Reassign Purchasing Documents

Description: Reassigns purchasing documents including purchase orders, purchase agreements, and cont...

Schedule: As soon as possible

Parameters:

- * Document Type: Purchase Orders
- * Procurement BU: Vision Operations
- * Old Buyer: [dropdown]
- * New Buyer: [dropdown]

Menu Items

The screenshot displays the Oracle Fusion Applications user interface. On the left, a navigation menu is visible with the following sections:

- Workforce Management**
 - Extract Maintenance
 - New Person
 - Person Management
 - Workforce Structures
- Career**
 - Profiles
- Benefits**
 - Enrollment
 - Plan Configuration
 - Evaluation and Reporting
- Manager Resources**
 - Manager Resources Dashboard
 - New Person
 - Workforce Compensation
- Manage Life Events**
 - Manage Benefit Life Events
- Manage Benefit Plans and Programs**
 - Manage Program/Plan Years
 - Manage Plan Types
 - Manage Benefit Options
 - Manage Benefit Plan Details
 - Manage Benefit Program Details
- Manage Rates and Coverages**
 - Manage Benefit Plan Coverage
 - Manage Benefit Rates
 - Manage Coverage Across Plan Types
- Define Enrollment Display**
 - Manage Plan Grouping
 - Manage Enrollment Authorizations

The main content area shows the 'Person Gallery' section. It includes a search bar with a 'Search' button and a 'Saved Search' dropdown. Below the search bar, there are buttons for 'Advanced', 'Search', 'Reset', and 'Save...'. The 'Search Results' section displays a table with columns for 'Plan Name', 'Status', and 'Plan Type'. The table content indicates 'No search conducted.'.

Tasks

Plan Configuration

Tasks

Manage General Benefits

- Manage Enrollment Action Types
- Manage Reporting Groups
- Manage Regulations
- Manage Benefit Balances

Manage Eligibility

- Manage Benefit Group
- Manage Benefit Service Area
- Manage Derived Factors
- Manage User-Defined Criteria
- Manage Eligibility Profiles

Manage Life Events

- Manage Benefit Life Events

Manage Benefit Plans and Programs

- Manage Program/Plan Years
- Manage Plan Types
- Manage Benefit Options
- Manage Benefit Plan Details
- Manage Benefit Program Details

Manage Rates and Coverages

- Manage Benefit Plan Coverage
- Manage Benefit Rates
- Manage Coverage Across Plan Types

Define Enrollment Display

- Manage Plan Grouping
- Manage Enrollment Authorizations

Overview

Overview ?

Programs and Plans

Rates and Coverages

Eligibility Profiles

Programs

Plans

Search

Advanced

Saved Search

* Required

Plan Name

* Effective As-of Date

1/19/2011

Search

Reset

Save...

Search Results

View

Format



Create



End Date

Quick Create Plan



Freeze



Detach



Plan Name

Status

Plan Type

No search conducted.

Buttons, Regions and Actions

Process Requisitions ? Dgne

Search: Requisition Lines Advanced Manage Watchlist Options Saved Search All my requisition lines requiring action

** Requisitioning BU
 ** Requisition
 ** Buyer
 ** Deliver-to Location
 ** Category Name
 ** Item
 ** At least one is required

Search Reset Save...

Search Results: Requisition Lines

Actions View Format Detach Wrap Add to Document Builder Return Reassign

	Requisition	Line	Item	Line Description	Quantity	UOM	Price	Amount	Currency	Deliver-to Loc
Export	0502199	2		Test Pseduo			10,000	10,000.00	USD	V1- New York
Add to Document Builder	0502197	1		test one	1	Box of 10	90	90.00	USD	V1- New York
	0502195	1	CM76840	Lightning Inkjet Printe	1	Each	165	165.00	USD	V1- New York
Reassign	0502150	2		Test Pseduo			10,000	10,000.00	USD	V1- New York
Split	0502143	2		Test Pseduo			10,000	10,000.00	USD	V1- New York
Update from Catalog	0502134	1	SC00100	Envoy Docking Station	10	Each	59.026	590.26	USD	Austin - TX
	0502050	1	SC00100	Envoy Docking Station	10	Each	59.026	590.26	USD	Austin - TX
View Document History	0502021	1	SC00100	Envoy Docking Station	10	Each	59.026	590.26	USD	Austin - TX
	10502017	1	SC00100	Envoy Docking Station	10	Each	59.026	590.26	USD	Austin - TX
	10502013	1	SC00100	Envoy Docking Station	10	Each	59.026	590.26	USD	Austin - TX
	10501978	1	SC00100	Envoy Docking Station	10	Each	59.026	590.26	USD	V1- New York
	10501970	1	SC00100	Envoy Docking Station	10	Each	59.026	590.26	USD	V1- New York
	10501958	1	SC00100	Envoy Docking Station	10	Each	59.026	590.26	USD	Austin - TX

Procurement BU
Vision Operations

Document Builder

Type
New Order

Requisitioning BU
Vision Operations

Sold-to BU
Vision Operations

Source Agreement
1001120

Style
Purchase Order

Supplier
CV_SuppA02

Supplier Site
CVSuppA02Site02

Currency
USD

Your Document Builder contains 1 lines.

Recently Added Lines
Envoy Docking Station 59.03 USD

Total 59.03 USD

Edit Create Clear

Fusion Applications Security

1. Role Based Access
2. Account and Role Provisioning Events & Workflows
3. Enforcement Across Tools and Transformations
4. Pervasive Privacy Protections
5. Integration with Governance Risk and Compliance
6. Transparent Security Policies
7. Complete Audit of Security Changes
8. Secure Across the Information Lifecycle
9. Co-existing with your current Security Infrastructure
10. Comprehensive Extensible Reference Implementation

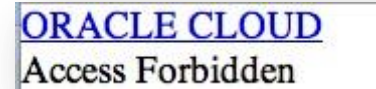
	A	B	C	D	E
1	RESPONSIBILITY_NAME	MENU_NAME	MAIN_MENU	SUB_MENU	CHILD_SUB_MENU
1219	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Journals	Import	Run
1220	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Journals	Generate	Recurring
1221	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Journals	Schedule	Allocation
1222	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Journals	Schedule	Recurring
1223	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Journals	Reconciliation	Reconcile
1224	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Journals	Reconciliation	Reverse
1225	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Jou		
1226	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Jou		
1227	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Bud		
1228	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Bud		
1229	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Bud		
1230	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Budgets	Enter	Journals
1231	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Reports	Define	Row Set
1232	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Reports	Define	Column Set
1233	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Reports	Define	Content Set
1234	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Reports	Define	Order
1235	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Reports	Define	Report
1236	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Reports	Request	Financial
1237	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Reports	Define	Display
1238	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Reports	Define	Report Set
1239	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Reports	Request	Standard
1240	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Other	Report	Set
1241	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Other	Report	View
1242	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Other	Report	Run
1243	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Journals	Import	Run
1244	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Journals	Define	Recurring
1245	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Journals	Import	Correct
1246	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Journals	Generate	Allocation
1247	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Journals	Reconciliation	Reverse
1248	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Journals	Schedule	Allocation
1249	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Journals	Schedule	Recurring
1250	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Journals	Reconciliation	Reconcile
1251	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Journals	Generate	Recurring
1252	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Budgets	Enter	Amounts
1253	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Budgets	Enter	Journals
1254	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Budgets	Enter	Upload
1255	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Budgets	Enter	Transfer
1256	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Reports	Request	Financial
1257	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Reports	Request	Standard

Manual Process
No Auto Provisioning

Count: 3617

ORACLE

Account and Role Provisioning Events & Workflows



Secure Out of the Box

1. Role Based Access
2. Account and Role Provisioning Events & Workflows
3. Enforcement Across Tools and Transformations
4. Pervasive Privacy Protections
5. Integration with Governance Risk and Compliance
6. Transparent Security Policies
7. Complete Audit of Security Changes
8. Secure Across the Information Lifecycle
9. Co-existing with your current Security Infrastructure
10. Comprehensive Extensible Reference Implementation

ORACLE® Fusion Applications

Accessibility Personalization ▾ Administration ▾ Help ▾ Sign Out **Abraham Mason**

22 | Copyright © 2011, Oracle and/or its affiliates. All rights reserved.

Secure OOTB: Enforcement Across Tools

ORACLE Entitlements Server

Authorization Management

System Configuration

Policy Upgrade Management

Accessibility

Help

Sign Out

Signed in as FAAdmin

Search

For Users

In Global Scope

abraham mason

Search Results

Actions View

Name

Abraham Mason

Global External Roles

Project Application Administrator

Data Security Policies for: PJF_PROJECT_ADMINISTRATOR_JOB_BU_Vision Operations

Select a policy and click the edit button to open the individual policy in a new tab.

Action View New Edit

Actions

Manage Contract, Maintain Project Contract Revenue

Condition

Access the project for table PJF_PROJECTS_ALL_VL for project business units on which they are authorize

Actions View

Map

Remove Roles

Open Role

Display Name

fscm

crm

hcm

obi

Application Help Text Administration Duty(OBI)

Customer Contract Setup Duty(OBI)

Functional Setups Duty(OBI)

Projects Administration Duty(OBI)

Reports and Analytics Region Administration Duty(OBI)

Watchlist Administration Duty(OBI)

IDCCS

Upload data for Project Management Import

Description

Adds and maintains custom help for all applications.

In addition to the setup activities allowed by the Contract Setup Duty, this duty p

Uses the functional user overview, and assigned tasks, and task lists.

Configures Oracle Fusion Projects applications.

Selects reports to appear in the Reports and Analytics region of Oracle Fusion App

Maintains the Watchlist categories and items displayed in Oracle Fusion Application

Allows to upload data file to import project management data.

Defined Once. Used Everywhere !

- ADF
- Enterprise Search
- Business Intelligence
- Reporting
- Mobile
- Web Services
- Content Management

Trasactional UIs

Business Intelligence

Universal Content Management

ORACLE

Fusion Applications Security

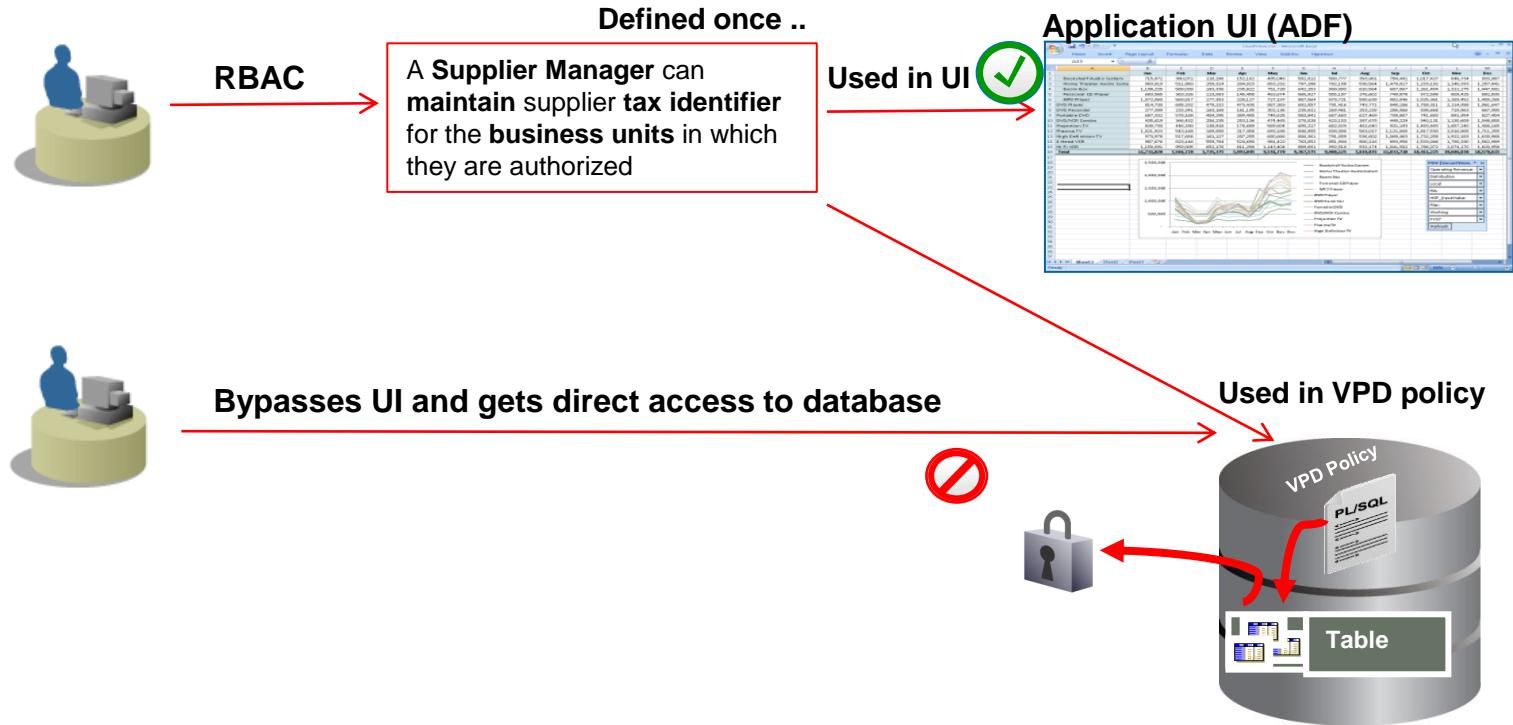
1. Role Based Access
2. Account and Role Provisioning Events & Workflows
3. Enforcement Across Tools and Transformations
4. Pervasive Privacy Protections
5. Integration with Governance Risk and Compliance
6. Transparent Security Policies
7. Complete Audit of Security Changes
8. Secure Across the Information Lifecycle
9. Co-existing with your current Security Infrastructure
10. Comprehensive Extensible Reference Implementation

Secure OOTB: Pervasive Privacy Protections

- Fusion Applications protect personally identifiable information (PII)
- PII = any piece of information which can potentially be used to uniquely identify, contact, or locate a single person.
 - Social Security Number (SSN)
 - Driver's license number
 - State or National Identifier (Identification Card number)
 - Passport Number
 - Account number, credit card number (CCN) or debit card number
 - Home or Physical address (e.g street address)
 - Email address
 - Telephone number



Secure OOTB: Pervasive Privacy Protections



Fusion Applications Security

1. Role Based Access
2. Account and Role Provisioning Events & Workflows
3. Enforcement Across Tools and Transformations
4. Pervasive Privacy Protections
5. Integration with Governance Risk and Compliance
6. Transparent Security Policies
7. Complete Audit of Security Changes
8. Secure Across the Information Lifecycle
9. Co-existing with your current Security Infrastructure
10. Comprehensive Extensible Reference Implementation

Manage Access & Segregation of Duties

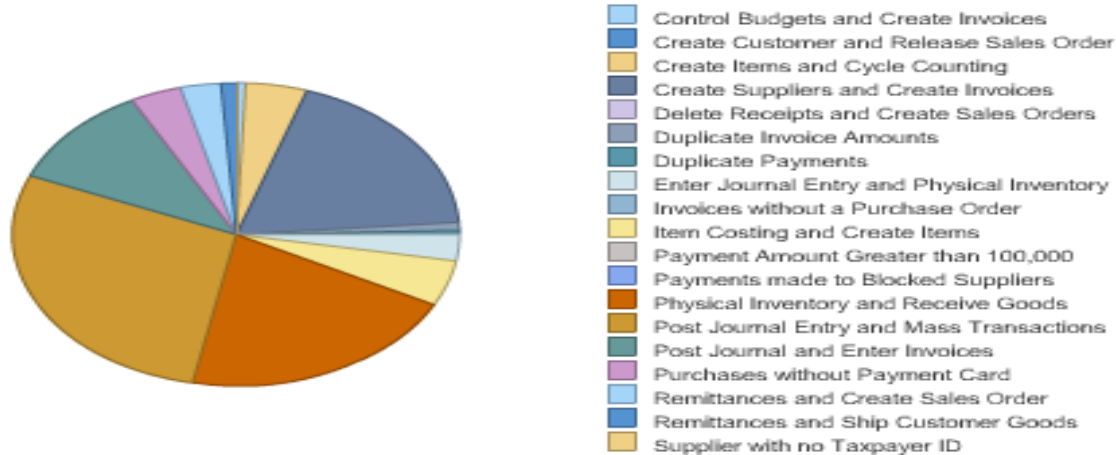
Solution

- Preventive AND Detective Access Controls
- Simulation for Role Design
- Preventive Provisioning
- Pre-built Content and Reports

Preventive Provisioning

Incidents By Control

Incidents By Control



Control_Name	Control_Type	Number_of_Incidents	Last_Run_Date	Control_Owner
Control Budgets and Create Invoices	Access	76	01-APR-2011	KBROWN
Create Customer and Release Sales Order	Access	0	01-APR-2011	ASMITH
Create Items and Cycle Counting	Access	512	01-MAR-2011	ASMITH

Fusion Applications Security

1. Role Based Access
2. Account and Role Provisioning Events & Workflows
3. Enforcement Across Tools and Transformations
4. Pervasive Privacy Protections
5. Integration with Governance Risk and Compliance
6. **Transparent Security Policies**
7. Complete Audit of Security Changes
8. Secure Across the Information Lifecycle
9. Co-existing with your current Security Infrastructure
10. Comprehensive Extensible Reference Implementation

Transparent Security Policies

Accounts Payable Manager

Manages Accounts Payable department and personnel. Overrides exceptions, analyzes Oracle Fusion Payables balances, and submits income tax and withholding reports to meet regulatory requirements.

General External Role Hierarchy Application Role Mapping

Mapping For: Accounts Payable Manager

Each application in the table below can be expanded to see the corresponding Application Roles within their hierarchy. Select an Application Role below and click the Open button to launch a view details in a new tab.

Actions View Map Remove Roles Open Role Find Policies

Display Name	Description
Mass Asset Additions Creation Duty	Submits the mass additions creations program for Oracle Fusion Assets users.
Payables Balance Analysis Duty	Analyzes Oracle Fusion Payables balances.
Payables Business Intelligence Management Duty	Manages access to Payables OBIA Dashboard
Payables Invoice Hold Resolution Duty	Resolves conditions causing invoice holds that did not result from data entry errors.
Payables Invoice Inquiry Duty	Views Oracle Fusion Payables invoices.
Payables Invoice Management Duty	Views invoices and related documents along with installments, holds, and approval history information.
Payables Invoice Processing Duty	Views invoices and related documents and takes action, such as approving and resolving holds.
Payables Payment Processing Duty	Manages Oracle Fusion Payables payments.
Payables Payment Request Inquiry Duty	Views Oracle Fusion Payables payment requests.
Payables Period Close Duty	Oversees all aspects of Oracle Fusion Payables period close that involve running period close reports.

Data Security Policies for: AP_ACCOUNTS_PAYABLE_MANAGER_FUSION_CORP_USA_DATA

Select a Policy and click the edit button to open the individual policy in a new tab.

Action View New Edit

Actions	Resource Name	Condition
Manage Payments By Business Unit	Business Unit	For a Business Unit

ORACLE Entitlements Server

Authorization Management

Search

For External Roles
In Global Scope

Payable Manager

Browse

Search Results

Actions View

Name
Accounts Payable Manager - Vision France
Accounts Payable Manager - Vision Belgium
Accounts Payable Manager - Vision Germany
Accounts Payable Manager - Vision Industrie
Accounts Payable Manager - Vision Italy
Accounts Payable Manager - Vision Operatio
Accounts Payable Manager - Vision Services
Accounts Payable Manager - Vision Spain
Accounts Payable Manager
Accounts Payable Manager FOS_VISOP_ICAP
FOS_VisOP_ICAP
FOS_VisSGD_ICA
Vision India

ORACLE

Fusion Applications Security

1. Role Based Access
2. Account and Role Provisioning Events & Workflows
3. Enforcement Across Tools and Transformations
4. Pervasive Privacy Protections
5. Integration with Governance Risk and Compliance
6. Transparent Security Policies
7. Complete Audit of Security Changes
8. Secure Across the Information Lifecycle
9. Co-existing with your current Security Infrastructure
10. Comprehensive Extensible Reference Implementation

Audit of Security Changes

Who made what changes, and when

Manage Audit Policies

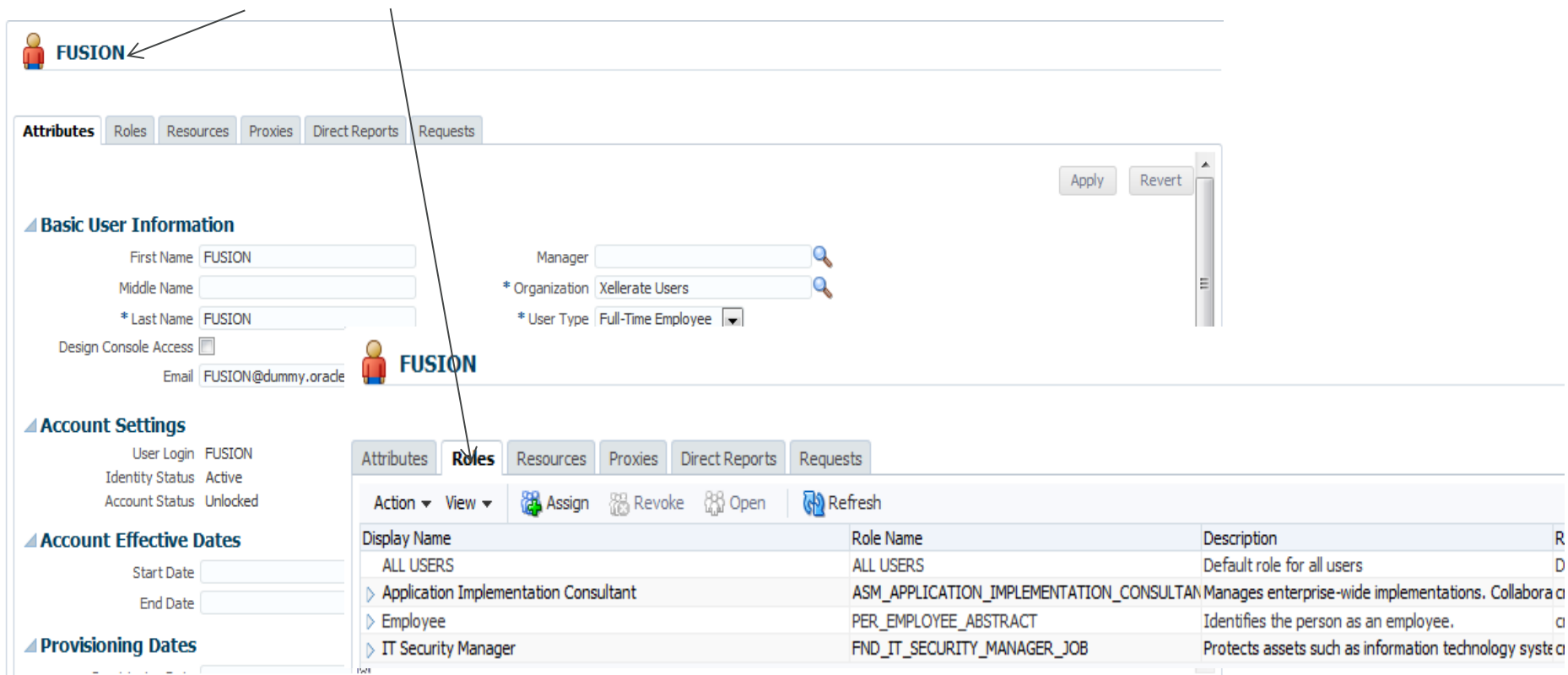
Configure the audit level for individual products, and for Oracle Fusion Applications, which business object attributes to audit.

Product	Audit Level
Oracle Fusion Applications (APPS) Fusion Applications Business Objects.	No Auditing
Oracle Business Intelligence Enterprise Edition (OBIEE) Analysis and Dashboard access, Creating/Updating/Deleting Web Catalog objects.	No Auditing
Oracle Business Intelligence Publisher (BIP) User sessions, report requests, report executions.	No Auditing
Oracle Data Integrator (ODI) Metadata changes of ODI.	No Auditing
Oracle Enterprise Scheduling Service (ESS) ESS metadata changes, ESS request operations, Administrative operations to ESS request processor and dispatcher.	No Auditing
Oracle Metadata Services (MDS) Metadata changes like sandbox publish, import.	No Auditing
Pages and Business Objects Extensibility (ADF) Extensibility changes via composers to pages and business objects.	No Auditing
Oracle Platform Security Services Security authorization, user authentication and assertion, credential store and key store services.	No Auditing
Oracle Web Service Manager (OWSM) Audit events fall into two broad categories: a) Auditing of OWSM Policy Enforcement like authentication, authorization, etc on a per request basis. b) Administrative operations like Policies, GPA, Assertion Templates. Also any changes to OWSM Local/Direct Policy attachments.	No Auditing
Oracle SOA Suite (SOA) SOA Metadata customizations.	No Auditing

- Audit of Changes in the definition of a role
- Audit of Changes to the roles assigned to a user
- Audit of the logins of highly privileged accounts
 - *Implementation Consultant*
 - *Security Manager*
 - *Payroll Administrator*
- Audit of the use of a highly privileged function
 - *Voiding of a Check*

IT Audit - Security

Show User and Roles from Oracle Identity Manager (OIM)



FUSION

Attributes Roles Resources Proxies Direct Reports Requests

Basic User Information

First Name: FUSION
Middle Name:
* Last Name: FUSION
Design Console Access: ☐
Email: FUSION@dummy.oracle

Manager:
* Organization: Xellerate Users
* User Type: Full-Time Employee

Account Settings

User Login: FUSION
Identity Status: Active
Account Status: Unlocked

Account Effective Dates

Start Date:
End Date:

Provisioning Dates

Attributes Roles Resources Proxies Direct Reports Requests

Action View Assign Revoke Open Refresh

Display Name	Role Name	Description	
ALL USERS	ALL USERS	Default role for all users	D
▶ Application Implementation Consultant	ASM_APPLICATION_IMPLEMENTATION_CONSULTAN	Manages enterprise-wide implementations. Collabora c	
▶ Employee	PER_EMPLOYEE_ABSTRACT	Identifies the person as an employee.	a
▶ IT Security Manager	FND_IT_SECURITY_MANAGER_JOB	Protects assets such as information technology syste c	

IT Audit - Security

Show User and Role Change Reporting

The screenshot displays the Oracle BI Publisher Enterprise interface. On the left, a 'Catalog' pane shows a tree of folders, with 'Role and Organization Reports' expanded. The main area shows a list of reports, including 'User Membership History', which is highlighted. A line points from this report to the right-hand pane, which displays the 'User Membership History' report details.

Oracle BI Publisher Enterprise

Search: All | Home | Catalog | New | Open | Signed In As: fusion

User Membership History

Last Name: | First Name: | User ID: CATEGORY_MGR01
Organization: | Employee Status: Active | Employee Type: Full-Time | Apply

Oracle Default

User Membership History

Filter Criteria

User ID	CATEGORY_MGR01
Employee Status	Active
Employee Type	Full-Time

User Details

User ID: CATEGORY_MGR01	Organization: Xellerate Users
User First Name: Ted	Employee Status: Active
User Last Name: Remer	Employee Type: Full-Time

Membership Details

#	User Role	Membership Status	Effective From	Updated By
1	cn=FusionGroups,cn=groups,dc=us,dc=oracle,dc=com,PER_EMPLOYEE_ABSTRACT	Active	February 21, 2013 01:24:22+00:00	Internal User
2	cn=FusionGroups,cn=groups,dc=us,dc=oracle,dc=com,PON_CATEGORY_MANAGER_JOB	Active	February 21, 2013 01:36:00+00:00	Internal User

Fusion Applications Security

1. Role Based Access
2. Account and Role Provisioning Events & Workflows
3. Enforcement Across Tools and Transformations
4. Pervasive Privacy Protections
5. Integration with Governance Risk and Compliance
6. Transparent Security Policies
7. Complete Audit of Security Changes
8. Secure Across the Information Lifecycle
9. Co-existing with your current Security Infrastructure
10. Comprehensive Extensible Reference Implementation

Secure OOTB: Secure Across Info Lifecycle

- Sensitive data in file system and backups (data-at-rest) protected using **Transparent Data Encryption**
- Sensitive data in cloned, non-production databases protected using **Oracle Data Masking**
- Sensitive data protected from database administrators and other privileged users using **Oracle Database Vault**

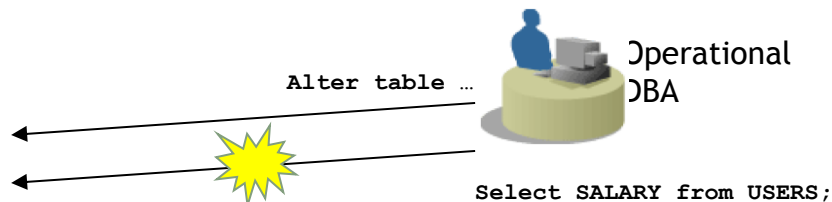


1095007






































Protect Data from View and Alteration as well as Insider Threat using *Database Vault*

Database Vault	Operational DBA	Data DBA / Manager
Select SALARY from users;	X	✓
Alter system. Alter table..	✓	X

* Example roles and privs



Sensitive Data in cloned instance
protected by *Data Masking*

LNAME	SSN	SALARY
KING	     	   
SCOTT	       	    
SMITH	       	     



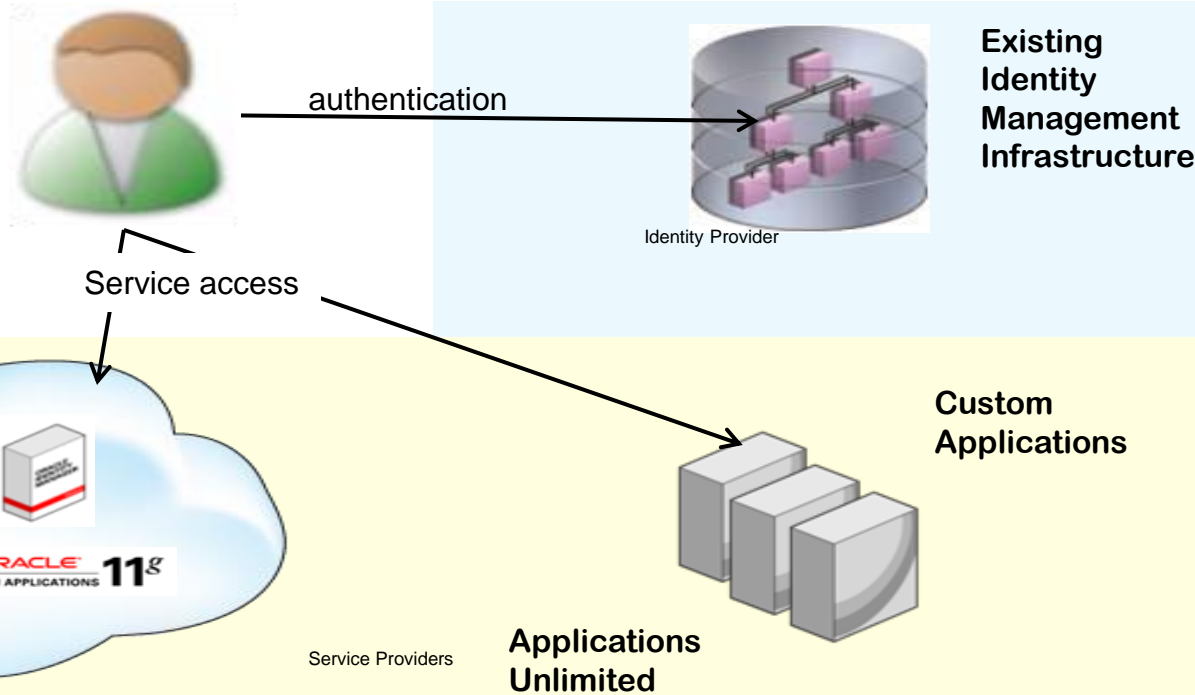
LNAME	SSN	SALARY
KING	111-11-1111	\$99,000
SCOTT	222-22-2222	\$888,000
SMITH	333-33-3333	\$77,000

Fusion Applications Security

1. Role Based Access
2. Account and Role Provisioning Events & Workflows
3. Enforcement Across Tools and Transformations
4. Pervasive Privacy Protections
5. Integration with Governance Risk and Compliance
6. Transparent Security Policies
7. Complete Audit of Security Changes
8. Secure Across the Information Lifecycle
9. Co-existing with your current Security Infrastructure
10. Comprehensive Extensible Reference Implementation

Secure OOTB: Co-existing with your current Security Infrastructure

Allows a user to log in once & access all applications...



Fusion Applications Security

1. Role Based Access
2. Account and Role Provisioning Events & Workflows
3. Enforcement Across Tools and Transformations
4. Pervasive Privacy Protections
5. Integration with Governance Risk and Compliance
6. Transparent Security Policies
7. Complete Audit of Security Changes
8. Secure Across the Information Lifecycle
9. Co-existing with your current Security Infrastructure
10. Comprehensive Extensible Reference Implementation

Secure OOTB: Reference Implementation

ORACLE

FUSION APPLICATIONS



OOTB

✓ roles you will recognize as jobs

✓ hierarchy of duties

✓ data security policies

✓ SOD Policies

✓ Provisioning Events

To extend

Security Console

✓ new jobs

✓ new duties

ORACLE

Configuration Flexibility



“What if I want to expand what reports the channel directors can see?”

Configuration Flexibility

Add a Duty Role

Job Role

Channel Director

Duty Role



Sales Transaction
Analysis Duty



Social



Hiring



Notifications



Learning



Navigator



Getting Started



Analytics



Security Console

Security Console

Create Role

Compare Roles

Search Channel Sales Director



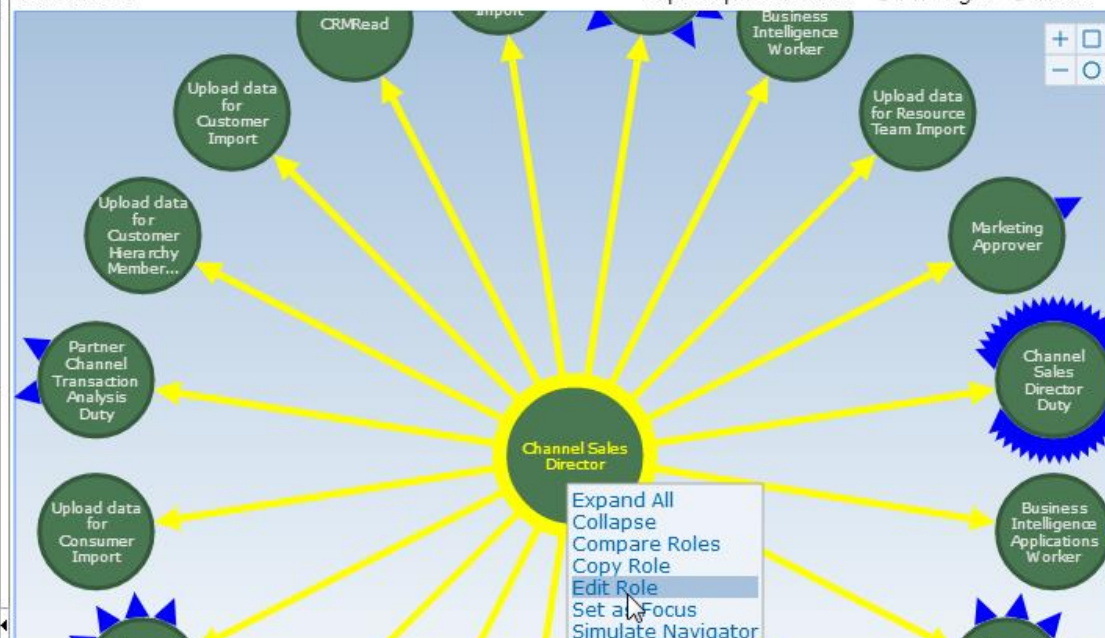
Refine

Search Results (1)

Channel Sales Director

Code
ZPM_CHANNEL_
SALES_DIRECTOR_
JOBDescription
Supervises
channel roles to support
partner
relationships and
transactions.

Visualization

Expand paths toward: ☒ Privileges ☐ Users

Security
Console

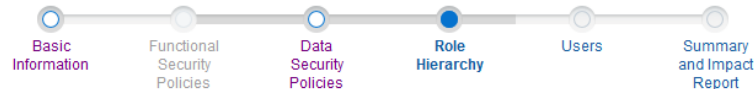
Edit Role : Role Hierarchy

Back

Next

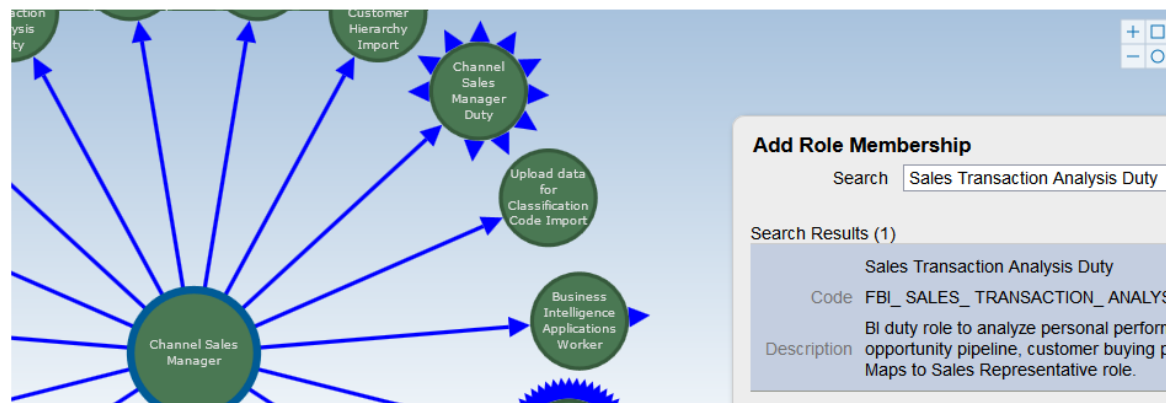
Cancel

Channel Sales Manager



Below is a visualization of this role.

Add Role



Add Role Membership

Search

Refine

Search Results (1)

Sales Transaction Analysis Duty

Code FBI_SALES_TRANSACTION_ANALYSIS_DUTY

Description BI duty role to analyze personal performance against quota and also opportunity pipeline, customer buying patterns, to better cross sell and up sell. Maps to Sales Representative role.

Add Role Membership

Cancel

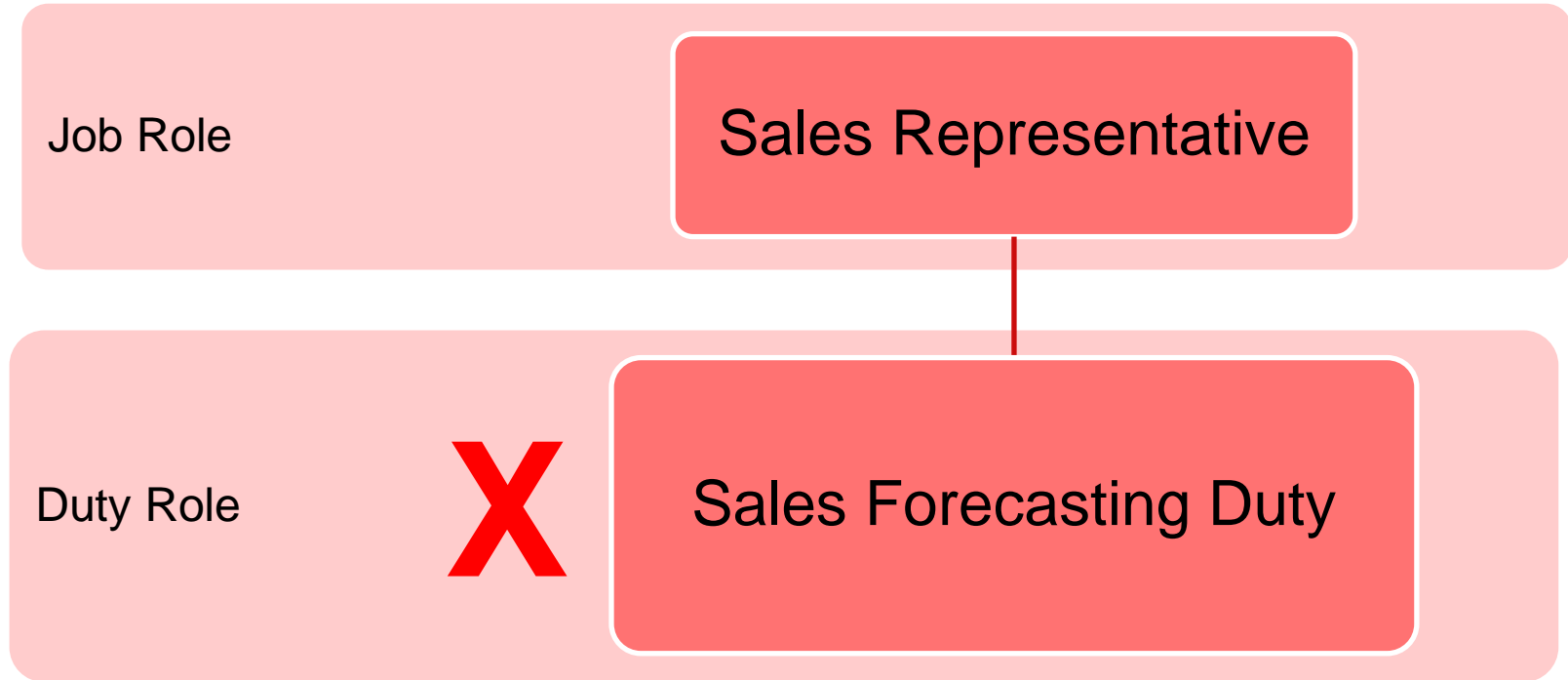
Configuration Flexibility



“Most business groups have their sales reps do forecasting, but I know of one where the sales managers do that, not the sales reps. **What should I do?**”

Configuration Flexibility

Remove a Duty Role





Edit Role : Role Hierarchy

Back

Next

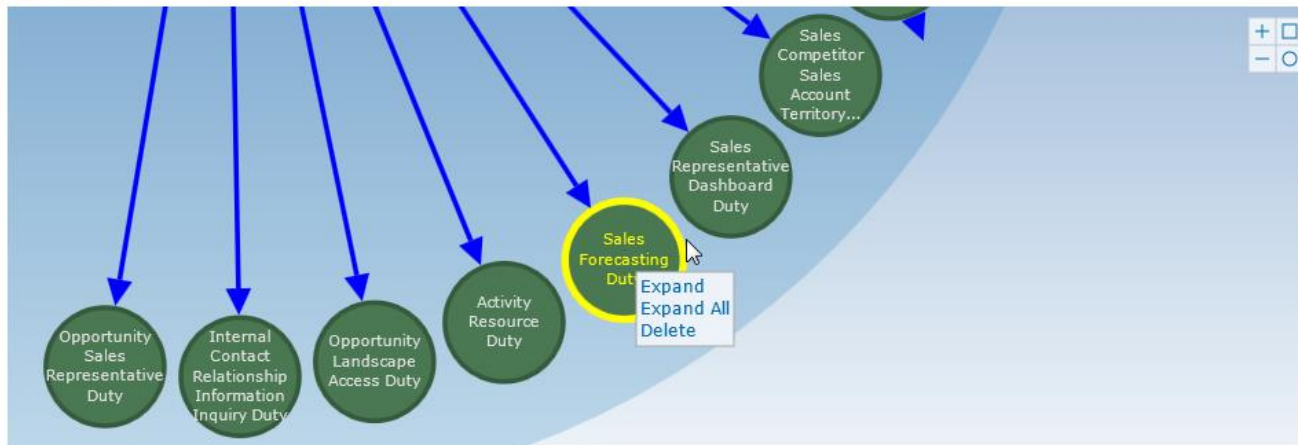
Cancel

Sales Representative



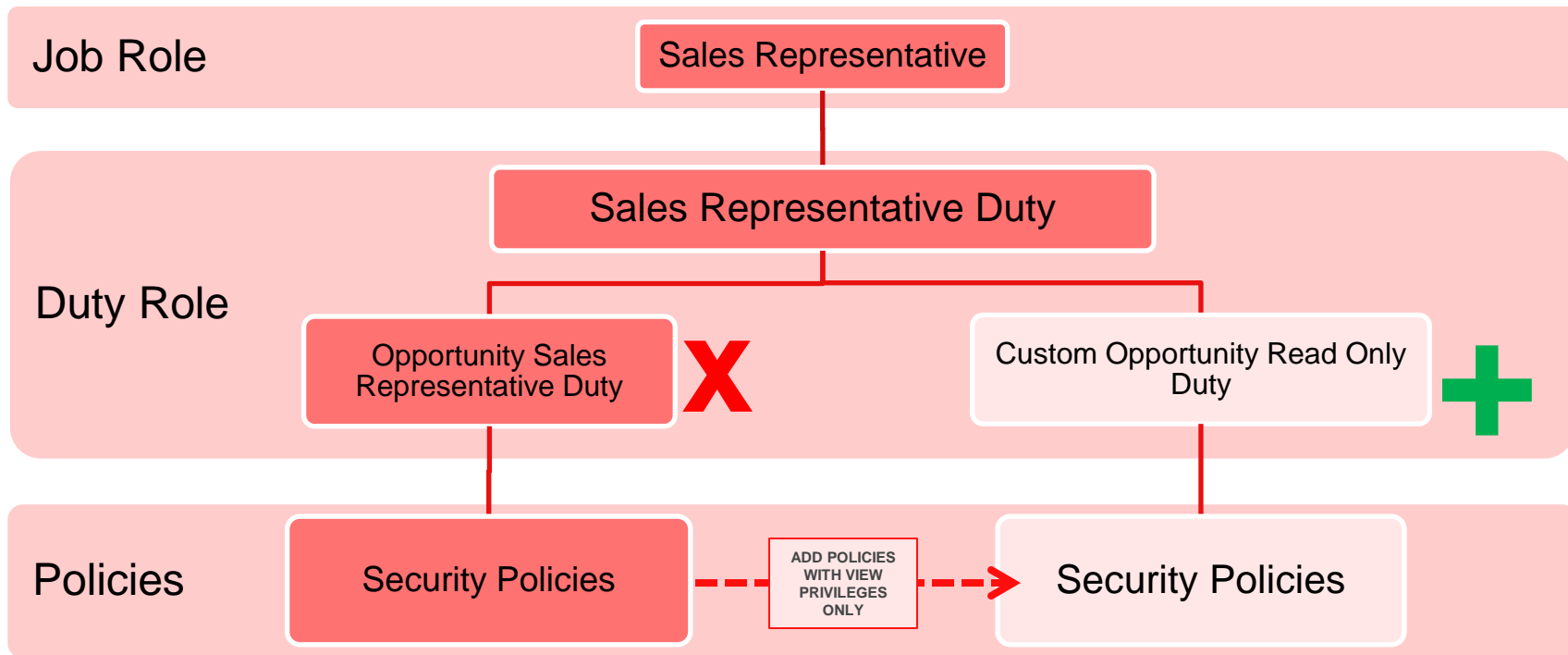
Below is a visualization of this role.

Add Role



Configuration Flexibility

Remove Duty Role and Add Custom Duty Role



Security
Console

Security Console

Create Role

Compare Roles

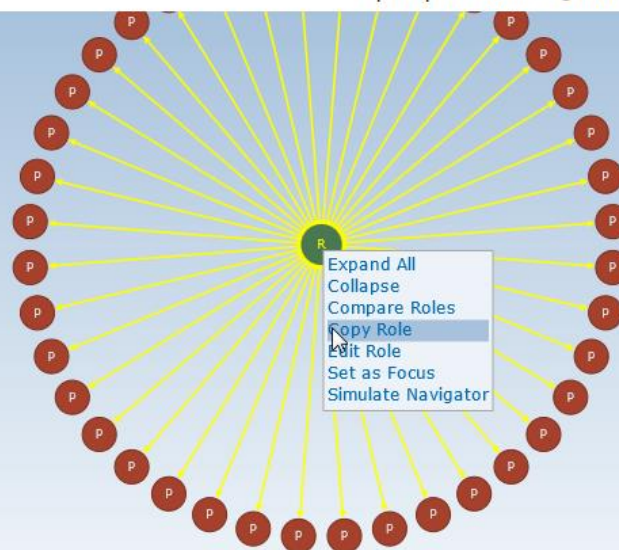
Search Opportunity Sales Representative Duty

Refine

Search Results (1)

Opportunity Sales
Representative DutyCode
MOO_
OPPORTUNITY_
SALES_
REPRESENTATIVE_
DUTYDescription
Manages or views
all aspects of the
application. This
role is for
salespersons.

Visualization

Expand paths toward: ☒ Privileges ☐ Users



Social



Hiring



Notifications



Learning



Navigator



Getting Started



Analytics



Security Console



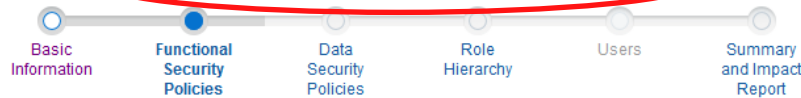
Copy Role : Functional Security Policies

Back

Next

Cancel

Copy of Opportunity Sales Representative Duty



Determines the actions a user can perform on a functional resource through this role.

Add Functional Security Policy Remove Functional Security Policy

Privilege Name	Inherited from Role	Description
Manage Opportunity Group Space		Allows creating of group spaces for an opp...
View Opportunity Sales Coach		Allows access to Sales Coach features. Sal...

Rows Selected 2

Manage Opportunity Reports: Details

Resource Name	Description
privilege:MOO_VIEW_OPPORTUNITY_SALES_COACH_PRIV	privilege:MOO_VIEW_OPPORTUNITY_SALES_COACH_PRIV
/WEB-INF/oracle/apps/sales/opptyMgmt/salesMethod/ui/flow/Show...	/WEB-INF/oracle/apps/sales/opptyMgmt/salesMethod/ui/flow/Show...

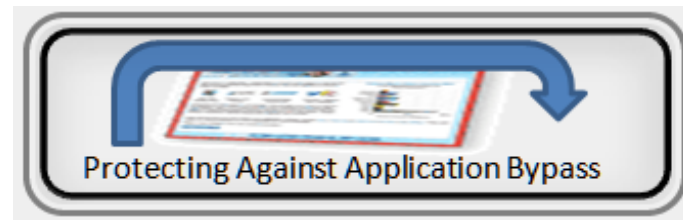
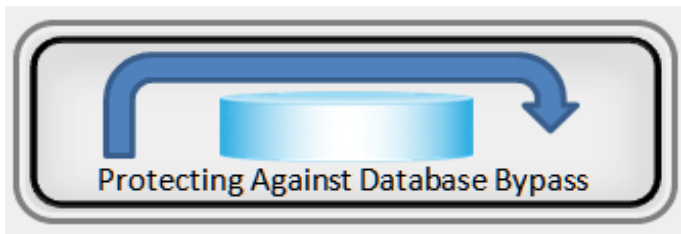
Securing the Database

MEGA BREACHES ON THE RISE



Considerations for Maximum Security

Preventive and Detective Controls



ORACLE DATABASE SECURITY

Maximum Security for Critical Infrastructure

PREVENTIVE

Encryption & Redaction

Masking & Subsetting

Privileged User Controls

ORACLE®



DETECTIVE

Activity Monitoring

Database Firewall

Auditing & Reporting

ORACLE®



ADMINISTRATIVE

Key Management

Privilege & Data Discovery

Configuration Management

ORACLE®



ORACLE®

Oracle Database Security Innovations

Privilege Analysis

Data Redaction

Real Application Security

Conditional and Unified Auditing

SQL Grammar based Database Firewall

Privileged User Controls

SQL Command Controls

At-source Data Masking

Sensitive Data Discovery

Transparent Data Encryption

Label-based Access Control

Virtual Private Database

ORACLE DATABASE SECURITY

Maximum Security for Critical Infrastructure

PREVENTIVE

Encryption & Redaction

Masking & Subsetting

Privileged User Controls

ORACLE®



DETECTIVE

Activity Monitoring

Database Firewall

Auditing & Reporting

ORACLE®



ADMINISTRATIVE

Key Management

Privilege & Data Discovery

Configuration Management

ORACLE®



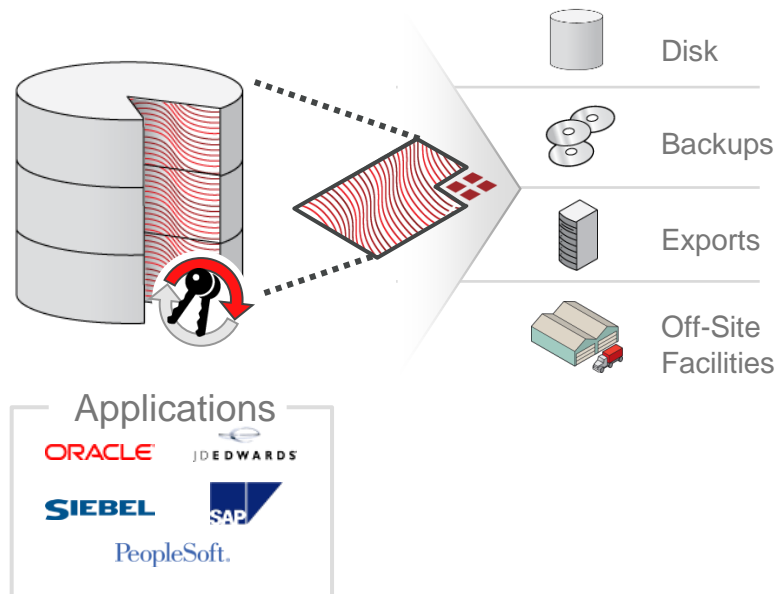
ORACLE®

Encryption is the Foundation

Preventive Control for Oracle Databases

Advanced Security

- Transparent data encryption
- Prevents access to data at rest
- Requires no application changes
- Built-in two-tier key management
- “Near Zero” overhead with hardware
- Integrations with Oracle technologies
 - e.g. Exadata, Advanced Compression, ASM, GoldenGate, DataPump, etc.

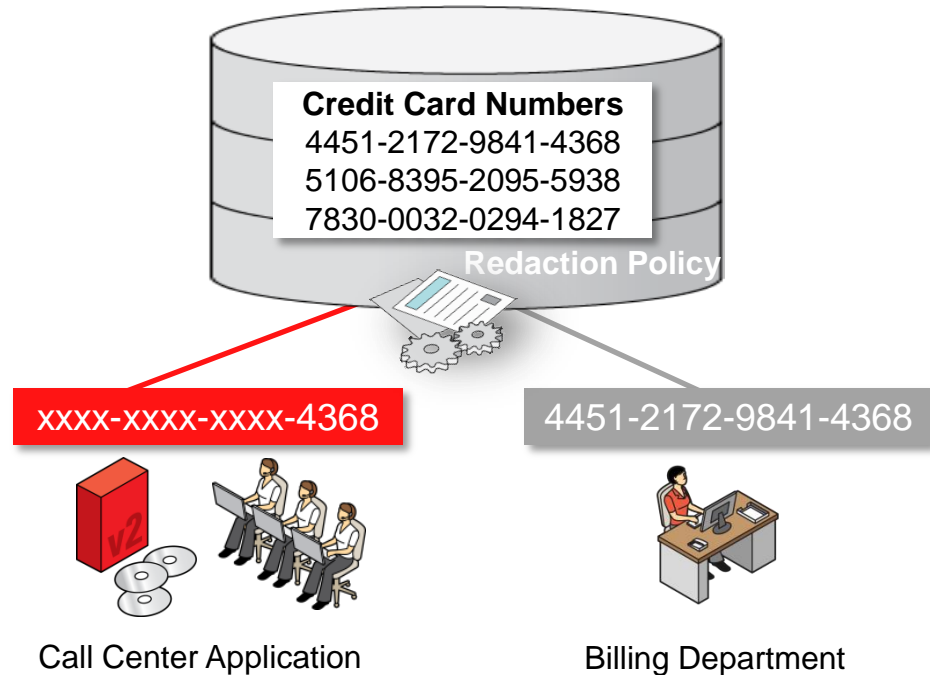


Redaction of Sensitive Data Displayed

Preventive Control for Oracle Database 12c and 11g (11.2.0.4)

Advanced Security

- Real-time redaction based upon user, IP, app context, session factors, ...
- Applies to columns on tables/views
- Full/partial, random/fixed redaction
- No impact on operational activities



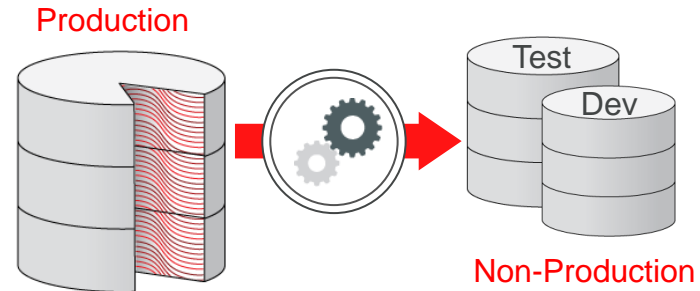
Masking Data for Non-Production Use

Preventive Control for Oracle Databases

Data Masking

- Replace sensitive application data
- Referential integrity detected/preserved
- Extensible template library and formats
- Application templates available
- Support for masking data in non-Oracle databases

LAST_NAME	SSN	SALARY
AGUILAR	203-33-3234	40,000
BENSON	323-22-2943	60,000



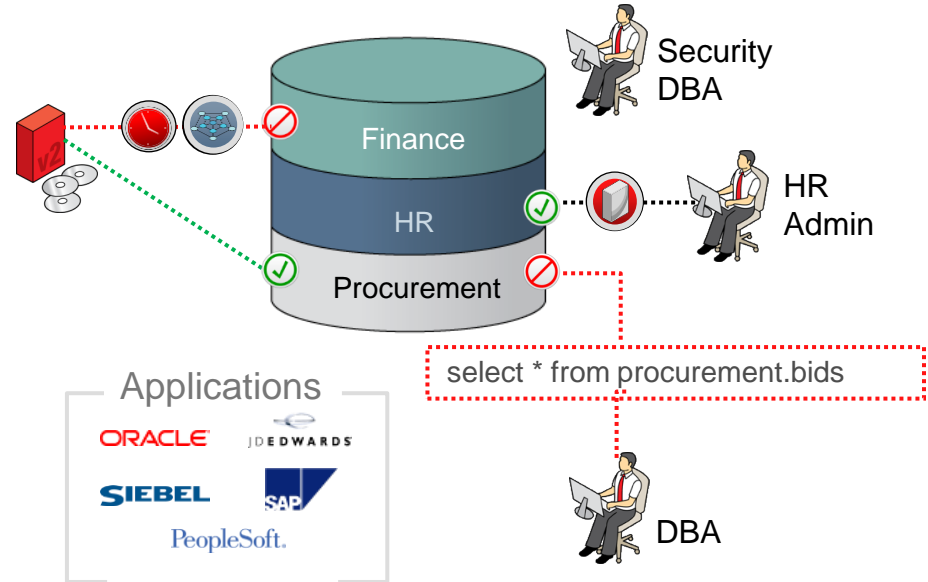
LAST_NAME	SSN	SALARY
ANSKEKSL	323—23-1111	60,000
BKJHHEIEDK	252-34-1345	40,000

Preventive Controls Inside the Oracle Database

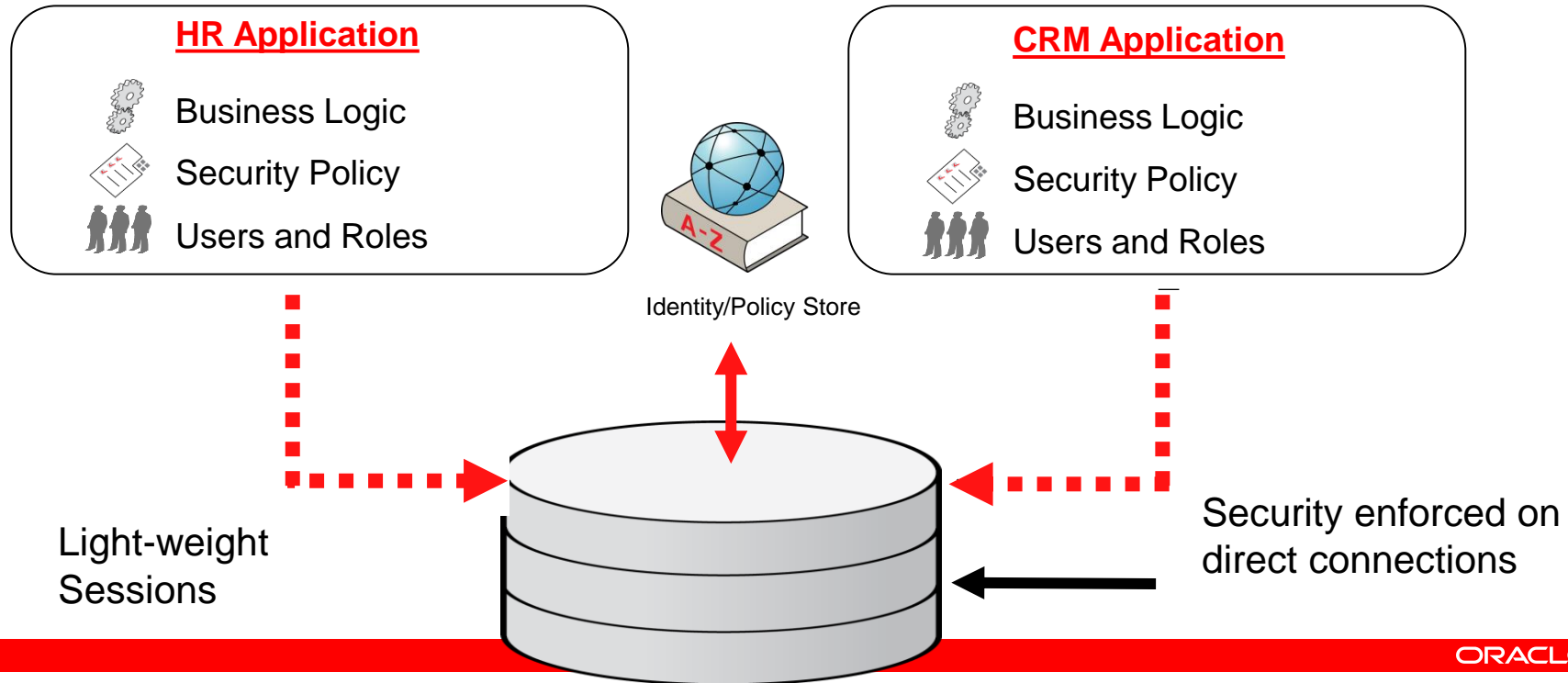
Preventive Control for Oracle Databases

Database Vault

- Realms around sensitive schemas or objects
- Restrict DBA access to realm data
- Support multi-factor SQL command rules
- Enforce separation of duties
- Block threats targeting privileged DB accounts
- Restrict all access unless explicitly authorized with Mandatory Realms (New)



Real Application Security



ORACLE DATABASE SECURITY

Maximum Security for Critical Infrastructure

PREVENTIVE

Encryption & Redaction

Masking & Subsetting

Privileged User Controls

ORACLE®



DETECTIVE

Activity Monitoring

Database Firewall

Auditing & Reporting

ORACLE®



ADMINISTRATIVE

Key Management

Privilege & Data Discovery

Configuration Management

ORACLE®



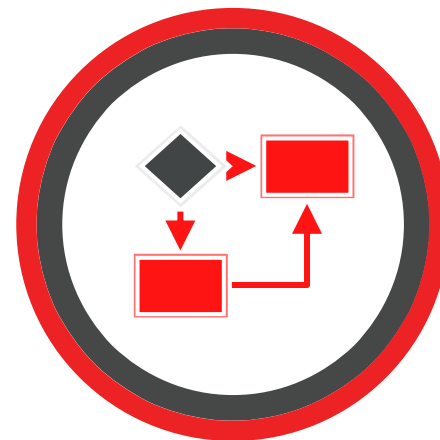
ORACLE®

New Conditional Auditing Framework

Detective Control for Oracle Database 12c

Database Auditing

- New policy and condition-based syntax
 - What: CREATE, ALTER, ALL, ...
 - Where: Set of Privileges, Roles, objects
 - When: IP_ADDRESS != "10.288.241.88"
 - Exceptions: Except HR
- Group audit settings for manageability
- New roles: Audit Viewer and Audit Admin
- Out-of-box audit policies
- Single unified database audit trail



Create Audit Policy : Privileges and Roles

* Name SENSITIVE OPERATIONS

Comments Audit sensitive operations in the database.

Privileges AVAILABLE

ADMINISTER ANY SQL TUNING SET
ADMINISTER DATABASE TRIGGER
ADMINISTER RESOURCE MANAGER
ADMINISTER SQL MANAGEMENT OBJECT
ADMINISTER SQL TUNING SET
ADVISOR
ALTER ANY ASSEMBLY
ALTER ANY CLUSTER
ALTER ANY CUBE
ALTER ANY CUBE BUILD PROC
ALTER ANY CUBE DIMENSION

SELECTED

ADMINISTER KEY MANAGEMENT
ALTER ANY PROCEDURE
ALTER ANY SQL TRANSLATION PROFILE
ALTER ANY TABLE
ALTER DATABASE
ALTER SYSTEM
AUDIT SYSTEM
CREATE ANY JOB

Roles AVAILABLE

ADM_PARALLEL_EXECUTE_TAS
APEX_ADMINISTRATOR_ROLE
APEX_GRANTS_FOR_NEW_USE
AQ_ADMINISTRATOR_ROLE

Policy Expression Builder

Oracle Database Environment

☒ Policy is in effect when session user is not APPS AND Add

Policy Expression

SYS_CONTEXT("USERENV", "SESSION_USER") != "APPS"

☐ Edit

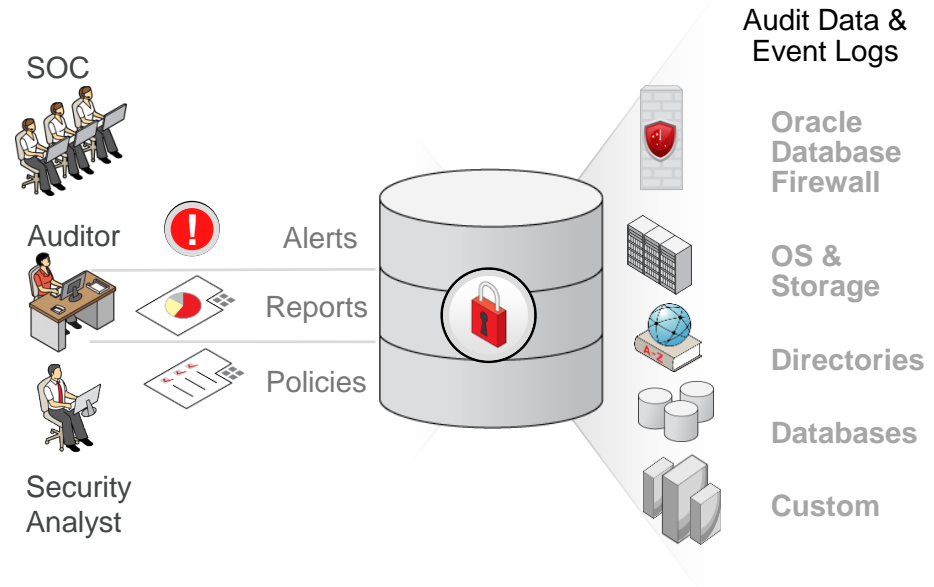
OK Cancel

Audit, Report, and Alert in Real-Time

Detective Control for Oracle and non-Oracle Databases

Audit Vault and Database Firewall

- Collect and Analyze audit/event data
- Centralized secure audit repository
- Consolidated multi-source reporting
- Out-of-the box and custom reports
- Conditional real-time alerts
- Fine-grain separation of duties
- Secure, scalable software appliance

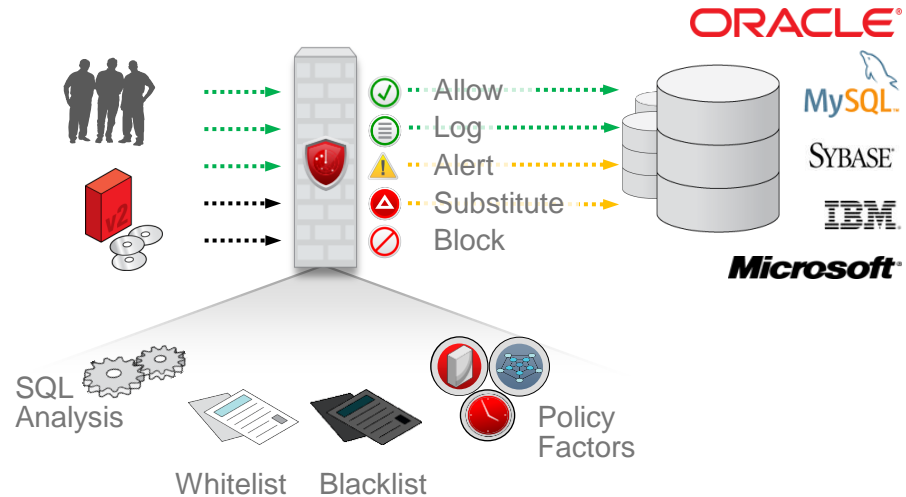


Database Activity Monitoring and Firewall

Detective Control for Oracle and non-Oracle Databases

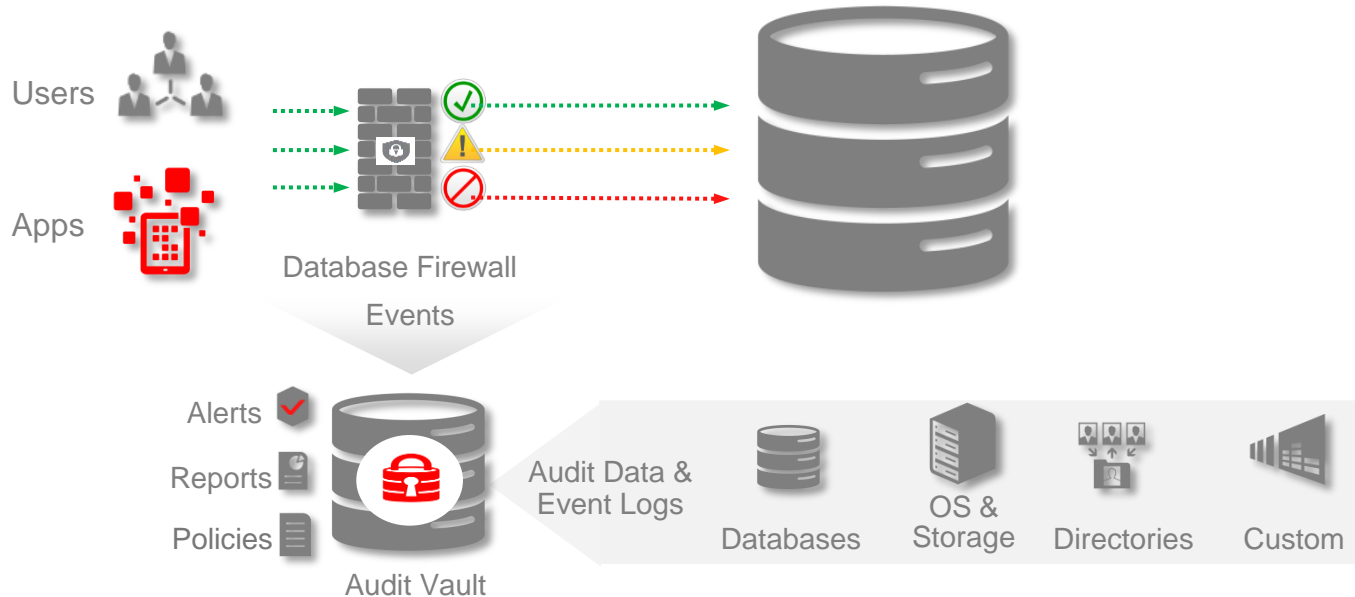
Audit Vault and Database Firewall

- Monitor network traffic, detect and block unauthorized database activity
- Detect/stop SQL injection attacks
- Highly accurate SQL grammar analysis
- Whitelist approach to enforce activity
- Blacklists for managing high risk activity
- Scalable secure software appliance



Oracle Audit Vault and Database Firewall

Detective Controls



ORACLE DATABASE SECURITY

Maximum Security for Critical Infrastructure

PREVENTIVE

Encryption & Redaction

Masking & Subsetting

Privileged User Controls

ORACLE®



DETECTIVE

Activity Monitoring

Database Firewall

Auditing & Reporting

ORACLE®



ADMINISTRATIVE

Key Management

Privilege & Data Discovery

Configuration Management

ORACLE®



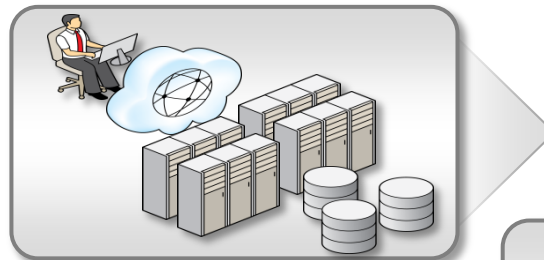
ORACLE®

Configuration Management

Administrative Control for Oracle Databases

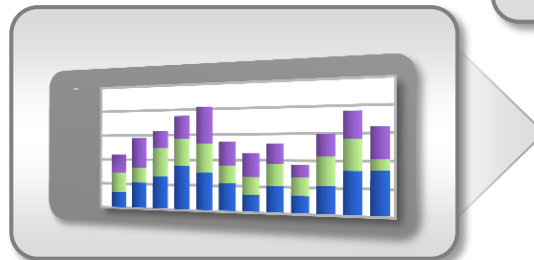
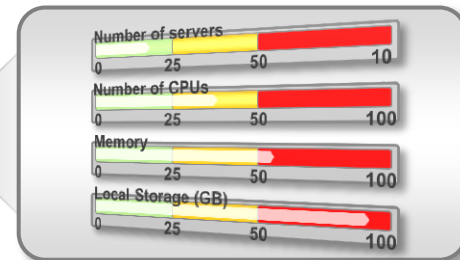
Database Lifecycle Management

- Discover and classify databases
- Scan for best practices, standards
- Detect unauthorized changes
- Patching and provisioning



Discover

Scan & Monitor



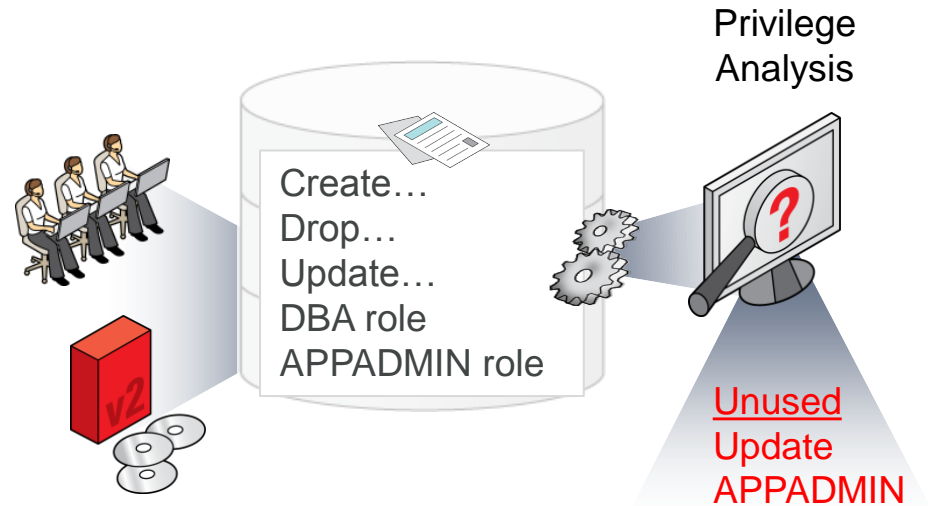
Patch

Discover Use of Privileges and Roles

Administrative Control for Oracle Database 12c

Database Vault

- Capture privileges used per session, across sessions, per specific context, or full database
- Report on privileges/roles used/unused
- Help revoke unnecessary privileges
- Enforce least privilege and reduce risks
- Increase security without disruption



New Oracle Enterprise Manager Security Menu

Enterprise ▾ Targets ▾ Favorites ▾ History ▾ Search Target Name ▾

dbsec01.us.oracle.com ⓘ DBSec-OW-13.us.

Oracle Database ▾ Performance ▾ Availability ▾ Security ▾ Schema ▾ Administration ▾

Page Refreshed Aug 26, 2013 3:12:12 PM

Auto Refresh Off

Summary

Status

Up Time 4 days, 2 hrs
Version 12.1.0.1.0
Load 0.00 average active sessions
Total Sessions 57
Last Backup N/A
Available Space 0.10 GB
Used Space 2.34 GB
Total SGA 597.31 MB

Diagnostics

ADDM Findings 0
Incidents 0 1 0 0

Compliance Summary

Compliance Standards

View Trends

Security Menu

- Home
- Reports
- Users
- Roles
- Profiles
- Audit Settings
- Enterprise Data Discovery
- Application Data Models
- Configuration Compliance
- Data Masking
- Data Redaction
- Transparent Data Encryption
- Database Vault
- Privilege Analysis
- Label Security
- Virtual Private Database
- Application Contexts
- Enterprise User Security

Services

Legend: SYS\$BACKGROUND, SYS\$USERS, dbsec01XDB, dbsec01.us.oracle.com, CPU Cores

Last Hour

Duration	SQL ID	Session ID	Parallel	Database Time
123.00 s	7gbccvcns5fmg	77		48.31 s
6.00 s	7wgks43wrjtrz	68		6.21 s
19.00 s	8szmwam7fysa3	68		19.36 s

ORACLE DATABASE SECURITY

Maximum Security for Critical Infrastructure

PREVENTIVE

Encryption & Redaction

Masking & Subsetting

Privileged User Controls

ORACLE®



DETECTIVE

Activity Monitoring

Database Firewall

Auditing & Reporting

ORACLE®



ADMINISTRATIVE

Key Management

Privilege & Data Discovery

Configuration Management

ORACLE®



ORACLE®

Oracle Database Maximum Security Architecture

