

Risk Management in Role-based Applications

Segregation of Duties in Oracle

Sundar Venkat, *Senior Manager, Protiviti*

Tai Tam, *Accounting Manager, Electronic Arts*

Core Competencies – C23

protiviti®
Risk & Business Consulting.
Internal Audit.



Agenda

- Introductions
- Overview and Session Objectives
- Common Issues in Security Design
- Top-Down SoD, Security Design Methodology and benefits
- About Electronic Arts
- Project Meridian Background and Security Design
- Automation of Segregation of Duties (SoD) Monitoring using Oracle AACG
- Automation of Security Build
- Q & A





Introductions

Protiviti

Sundar Venkat, Senior Manager

Over 10 years of experience in ERP Implementation, Security and GRC Design

Electronic Arts

Tai Tam, Accounting Manager

Global lead for Segregation of Duties. Over 15 years of experience in the Industry, working in various capacities in Finance, Audit and Compliance



TOP-DOWN SoD AND SECURITY DESIGN METHODOLOGY AND BENEFITS



Common Issues in Security Design

Insufficient understanding of the security model of ERP systems leading to a design that is not comprehensive

Not allocating enough time in the implementation process for security design

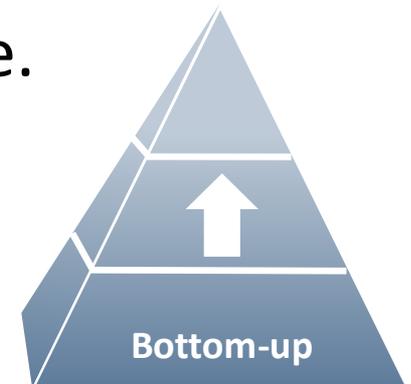
Not identifying and securing sensitive data prior to implementation

Need to define a lot of manual controls increasing audit cost

Understanding SoD Design Approaches

Bottom-up

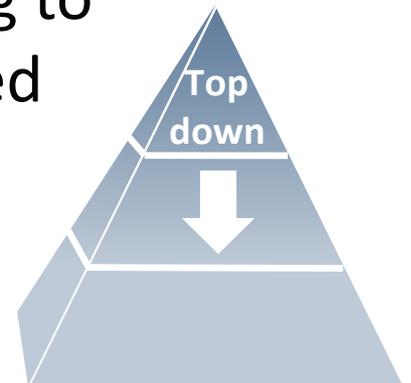
- No direct relationship between formal SoD policies and Oracle Responsibilities.
- Oracle Responsibilities are defined based on limited design of SoD rules.
- Oracle Responsibilities are not conflict-free.
- One-off results in each SoD test cycle.
- Heavy manual controls.



Alternate SoD Design Approach

Top-down

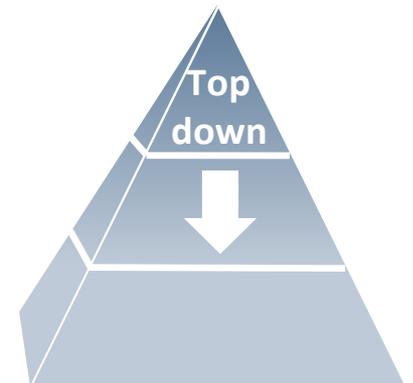
- Business process owners define formal SoD policies. These policies are used as the foundation of SoD design in Oracle ERP environment.
- "Authorized" conflicts are determined at the design level.
- Oracle functions are classified according to formal SoD policies and rules are defined by business process owners.
- Conflict-free Oracle Responsibilities are designed according to these policies.



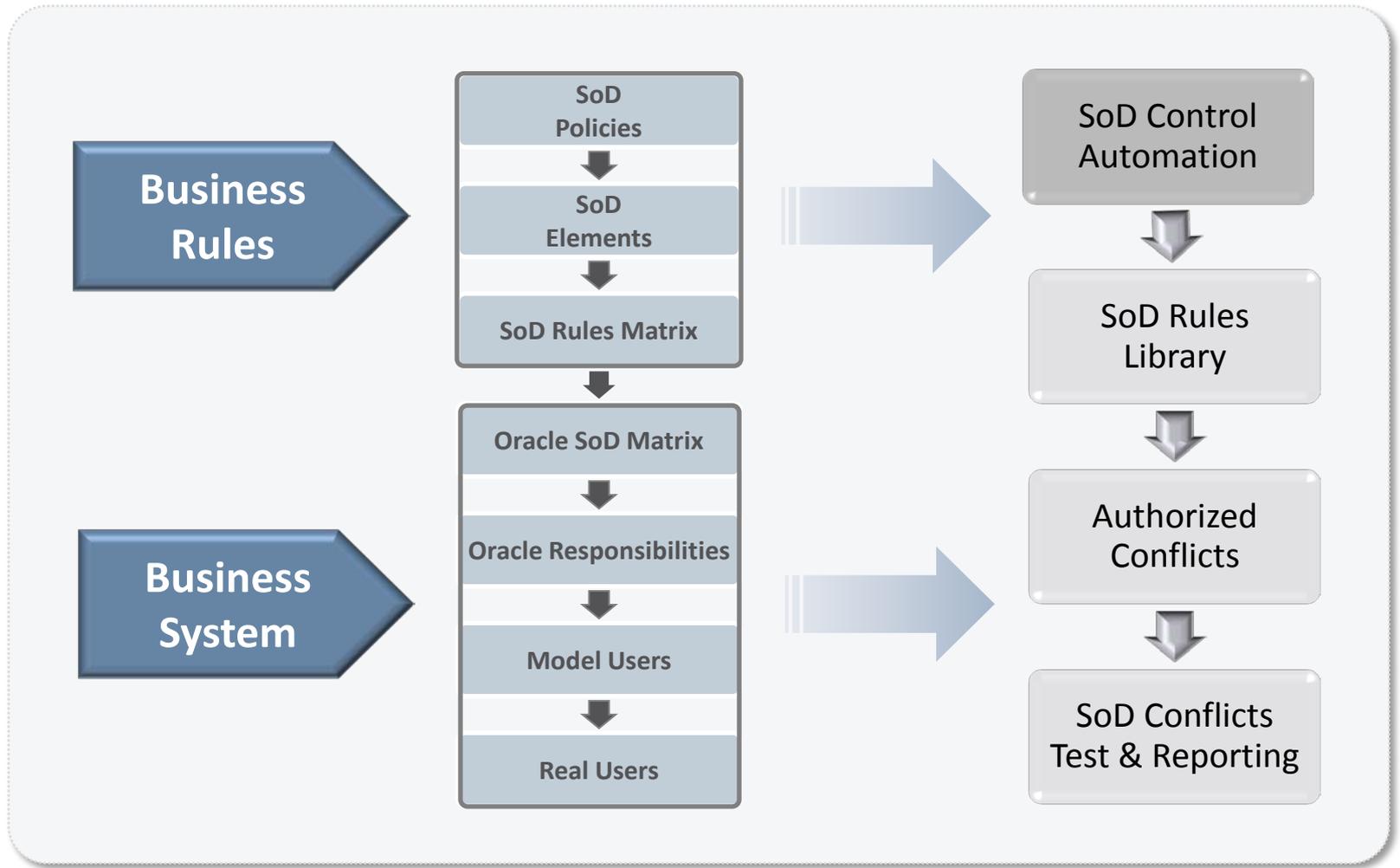
Alternate SoD Design Approach (continued)

Top-down

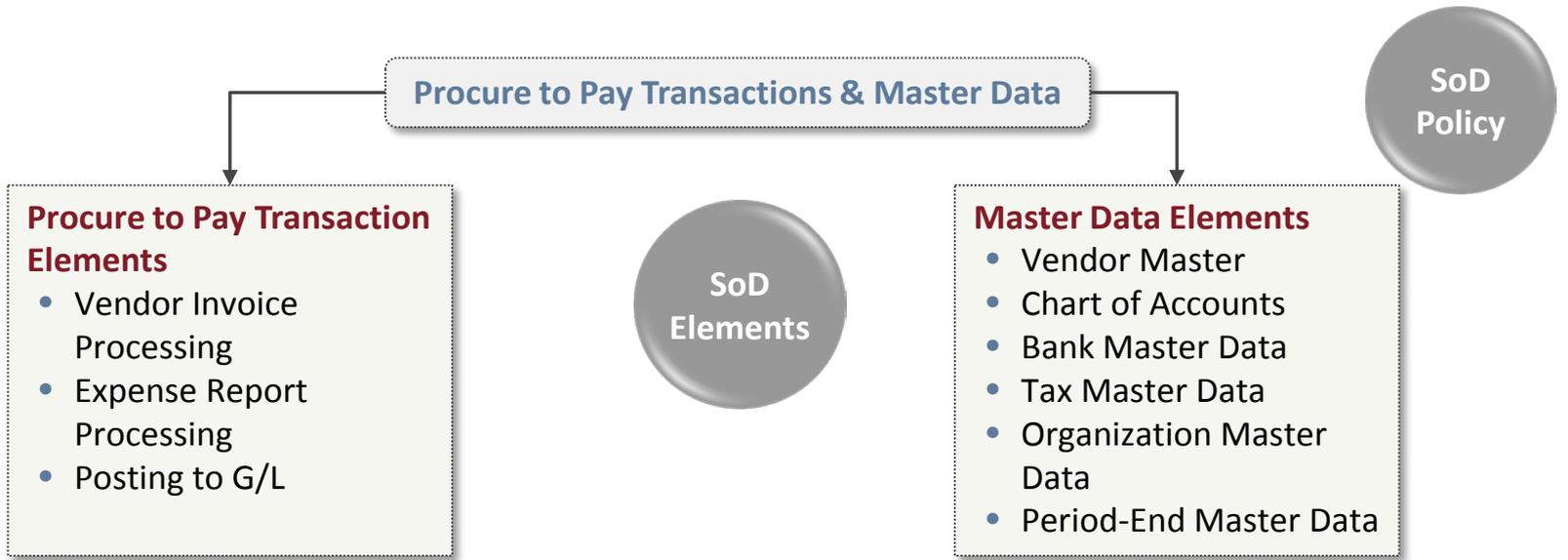
- Each Responsibility includes a set of functions defining its unique characteristics.
- Oracle functions are categorized into Business Setup, IT Setup, and Transactional setup, ensuring consistency in the separation of the functions by category.
- Good fit for automation.



Security and SoD Design Approach



Example of SoD Design Elements



SoD Policy Element 1	SoD Policy Element 2	SoD Policy Sub-element 1	SoD Policy Sub-element 2
Transactional Data	Master Data	Vendor Invoice Processing	Vendor Master
Transactional Data	Master Data	Posting to G/L	Chart of Accounts

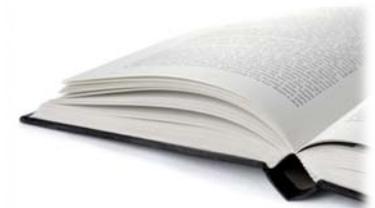


SoD Policy Element	SoD Policy Lowest-Level Element	Oracle Function	Oracle Function Description
Transactional Data	Vendor Invoice Processing	AP_APXPAWKB_CHECK_ACTIONS	Payment Actions
Master Data	Vendor Master	AP_APXVDMVD	Suppliers

Design Steps – Summary

Step 1:

Segregation of Duties (SoD) policies of the enterprise are designed. These policies are system agnostic. Client's business stakeholders provide feedback if SoD policies are relevant and if they represent risks that need to be monitored.



Step 2:

SoD Elements and Rule-set are designed based on SoD policies defined in Step 1 above. An SoD Rule comprises two policy elements that are conflicting in nature.



Design Steps – Summary (continued)

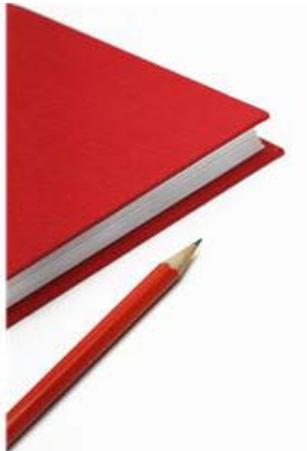
Step 3:

The Oracle SoD Rule-set represents Oracle Functions and is used as a basis to design the Oracle Responsibilities and Request Groups.



Step 4:

Responsibilities are designed in such a way that conflicting elements are not defined within the same responsibility.



Benefits

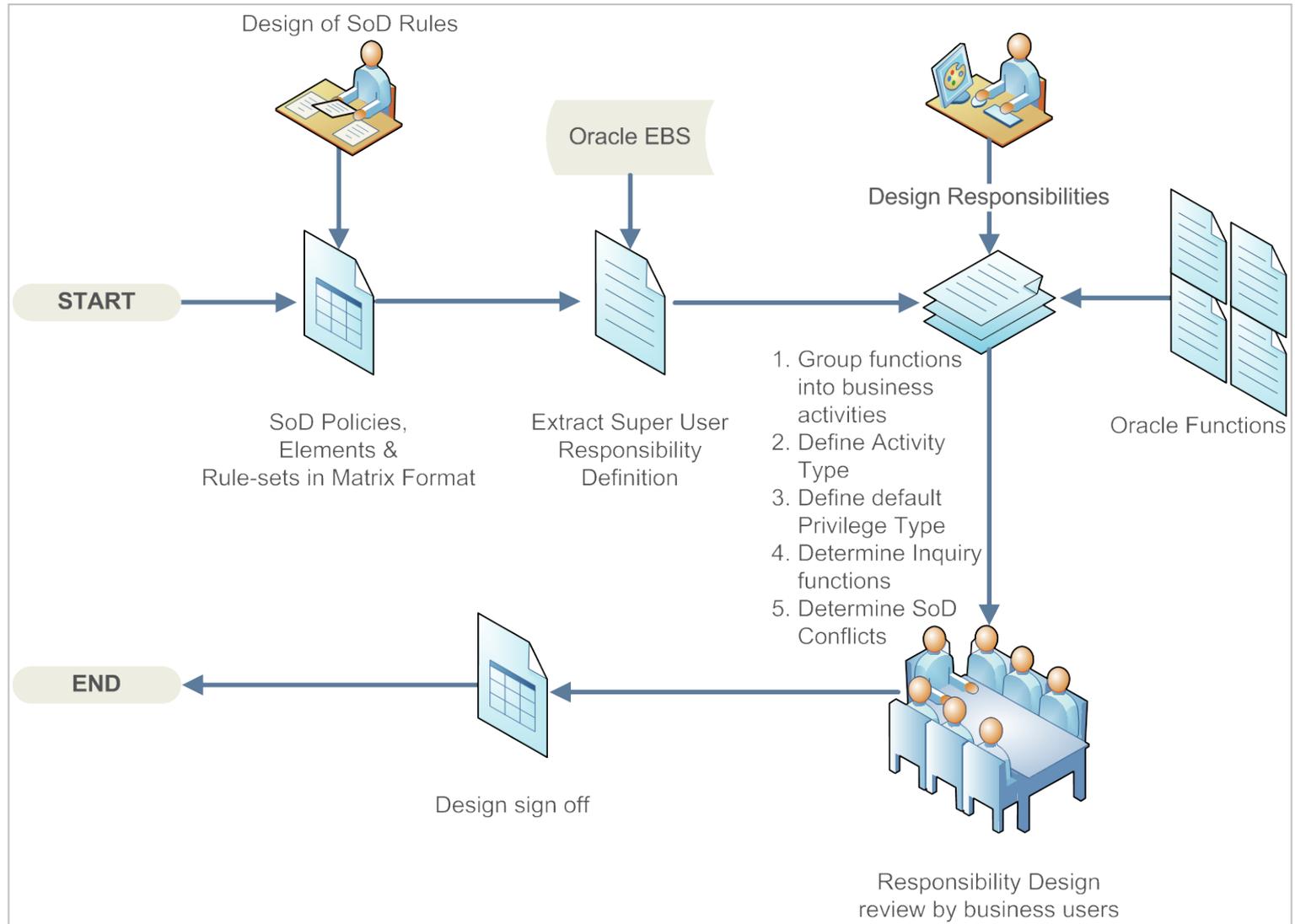
- Provides a business view of Oracle Responsibilities and uses business-user friendly language.
- Oracle Functions are grouped into a brief list of business activities.
- The Design templates provide easy drill-down to Oracle Functions from business activities.
- Custom Responsibilities and Request Groups are designed based on business activities.
- The Design includes Responsibility and Request Group matrices showing SoD conflicts.





PROTIVITI'S SECURITY DESIGN & BUILD PROCESS

Process Flow – Design Oracle Responsibilities





Automated Responsibility Build using proprietary tool

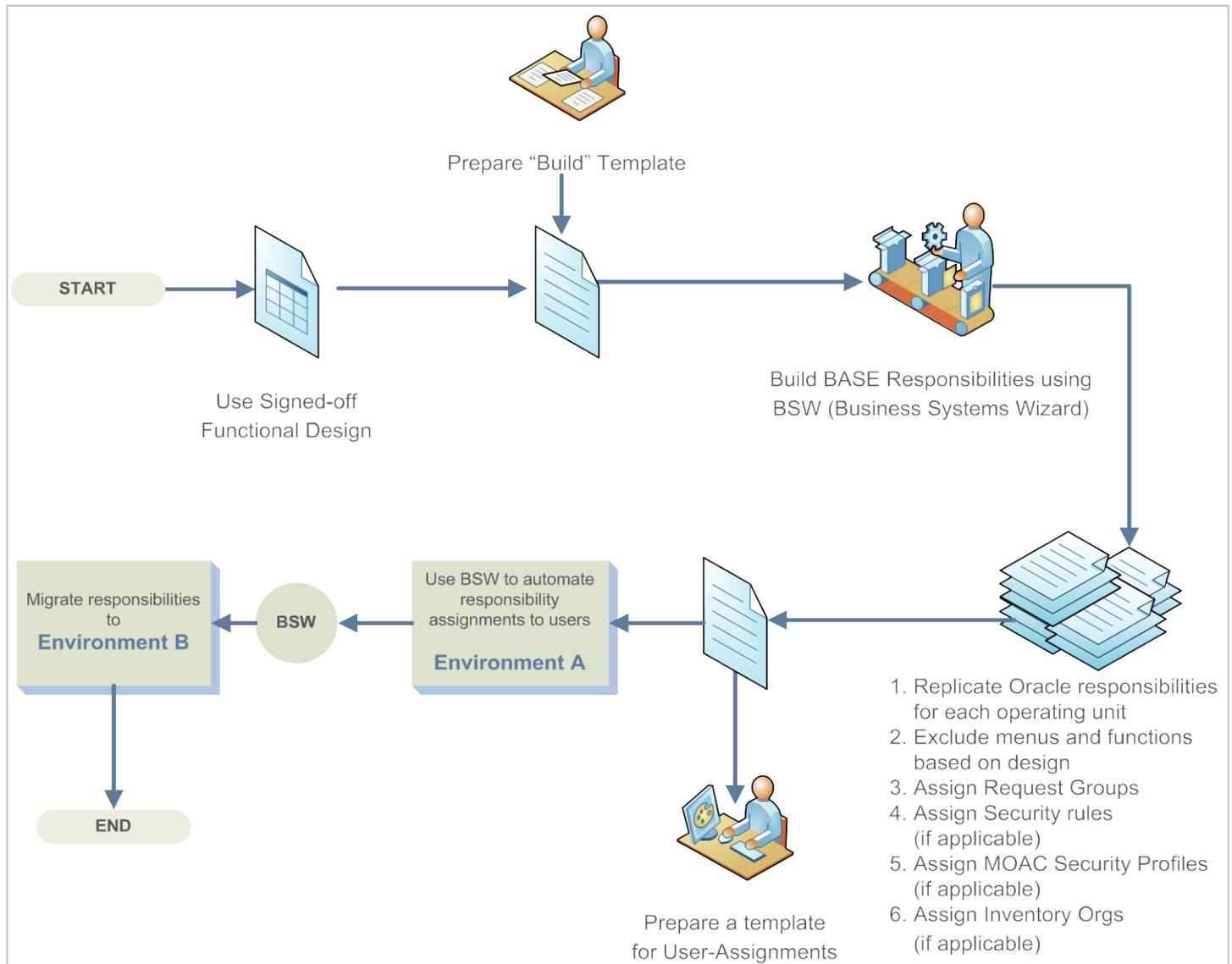
- The tool uses the System Administrator User interface on Oracle E-Business Suite to build responsibilities. No transactions are performed on the database (back-end). This minimizes risks of data inconsistencies when moving responsibilities from one environment to another.
- 'Custom' responsibilities are built using the concept of menu and function exclusions, not customizing seeded responsibilities.
- Pre-defined 'Built' templates available for various releases of Oracle E-business Suite.
- Tool processes large volumes of transactions in a few hours.

Automated Responsibility Build using proprietary tool (continued)

Examples of pre-defined templates include:

- Build 'Custom' Responsibilities and 'Custom' Menus
- Exclude Menus and Functions
- Assign seeded request groups to responsibilities
- Assign Custom Reports, Forms and Functions to responsibilities
- Assign FND Profile Options to responsibilities
- Assign Security Profiles to responsibilities
- Assign Multi Organization Access Controls (MOAC)
- Assign Inventory Organizations to responsibilities

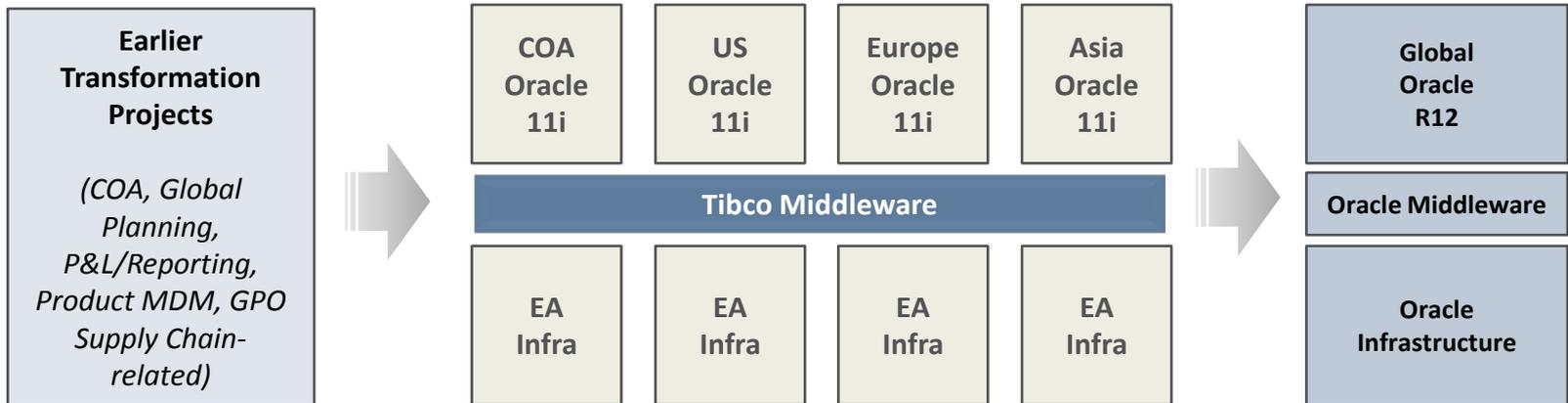
Process Flow – Build Oracle Responsibilities



CASE STUDY: PROJECT MERIDIAN – ERP TRANSFORMATION TO ORACLE R12



Project Meridian is Part of a Larger Effort



Phase 1 – Deploy following Oracle modules in R12

Procurement: iClick + iExpense & iProcurement

Finance : General Ledger, Accounts Payable, Indirect Purchasing, Fixed Assets



Phase 2 – Deploy following Oracle modules in R12

Publishing : Inventory, Order Management, Pricing, Supply Chain

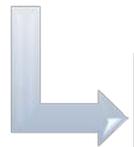
Finance: AR, Trade Management, Advanced Collection, Costing

Online Publishing (Digital Order to Cash)

Meridian will switch primary focus to revenue generation processes

Project Meridian – Objectives

Global Single Instance



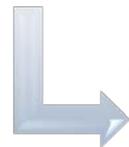
Global Business Process Standardization



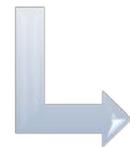
Achieve Operational Efficiency



Minimize Customization



Minimize Development Cost



Cost Efficiency



Project Meridian – Security Design Objectives

Design SoD Rule-set to address risks in new Oracle R12 modules



Minimize SoD Risks on Oracle R12 custom responsibilities using the SoD Rule-set as a basis

ORACLE SECURITY DESIGN & AUTOMATED SoD MONITORING



Automated Monitoring of SoD Using AACG

1

Identify and rank SoD risk with various Oracle access scenarios in key business process areas.

- Financial Close Process – General Ledger
- Procure to Pay Process – AP, Purchasing and Fixed Assets
- Order to Cash Process – AR, Pricing, Customer Master and Sales Invoicing

#	Process	SoD Rule Descriptions	FY11 Rankings
29	Procure to Pay	Supplier Master; AP Payments	Low
30	Procure to Pay	Supplier Master; Payables Invoice Entry; AP Payments	High
31	Procure to Pay	Supplier Master; Purchase Order Entry; Receiving Transactions	High
32	Procure to Pay	Supplier Master; Requisition Entry; Receiving Transactions	High
33	Order to Cash	AR Approve Adjustments; AR Cash Receipts	Moderate
37	Order to Cash	AR Approve Adjustments; Sales Order	Moderate
38	Order to Cash	AR Approve Adjustments; Sales Pricing	Moderate
39	Order to Cash	AR Cash Receipts; AR Customer Master	Moderate
40	Order to Cash	AR Cash Receipts; AR Debit Memo	High
41	Order to Cash	AR Cash Receipts; AR Sales Invoicing	High
42	Order to Cash	AR Cash Receipts; Sales Agreements	Low

Automated Monitoring of SoD Using AACG (continued)

2

Develop SoD rules with applicable Oracle functional elements covering the Oracle access scenarios and build them in AACG.

The screenshot displays the Oracle Governance, Risk and Compliance Controls (AACG) interface. The main window shows a list of policies with columns for Policy Name, Description, Policy Type, Priority, Status, and Effective Date. The selected policy is (ERPEUPD) - Item Master; Purchase Order Entry; Receiving Transactions. Below the list, a detailed view of this policy is shown, including a table of elements and their descriptions.

Policy Name*	Description	Policy Type*	Priority*	Status*	Effective Date*
(PEAR2I) - GL FX Rates; CE Bank Reconciliation	PEAR2I - OTC	Monitor	1	Active	08/26/2011
(PEAR2I) - TM IT Setup; AR Enter Credit Memos/Adjustments	PEAR2I - OTC	Monitor	1	Active	08/26/2011
(PEAR2I) - CE IT Setup; CE Bank Reconciliation	PEAR2I - P2P	Monitor	1	Active	08/26/2011
(ERPEUPD) - Item Master; Purchase Order Entry; Receiving Transactions	ERPEUPD - P2P	Monitor	1	Active	08/26/2011
(ERPEUPD) - Item Master; Purchase Order Entry	ERPEUPD - P2P	Monitor	1	Active	08/24/2011
(ERPEUPD) - INV - Inventory Transfer; INV Inventory Adjustme...	ERPEUPD - P2P	Monitor	1	Active	07/29/2011
(ERPEUPD) - INV - Inventory Adjustments	ERPEUPD - P2P	Monitor	1	Active	07/29/2011
(ERPEUPD) - CST - Average Cost; INV - Item Cost Update; Purc...	ERPEUPD - P2P	Monitor	1	Active	07/29/2011
(ERPEUPD) - AR Customer Credit Management; Sales Order	ERPEUPD - OTC	Monitor	1	Active	07/29/2011
(ERPUSPD) - AR Customer Master; AR Approve Adjustments	ERPUSPD - OTC	Monitor	1	Active	03/30/2010
(PEAR2I) - Supplier Master: Requisition Entry: Receiving Transac...	PEAR2I - P2P (High)	Monitor	1	Active	03/24/2010

Element Name	Description	Datasource	Platform	Element Type	Control
AND					
<input type="checkbox"/> PO Receiving Transactions - (ERPEUPD)	Access to Corrections, Shipments, F			Entitlement	
<input type="checkbox"/> PO Purchase Order Entry - (ERPEUPD)	Access to PO Purchase Order Entry			Entitlement	
<input type="checkbox"/> INV Item Master - (ERPEUPD)	Access to Item Master functions			Entitlement	

Oracle Governance, Risk and Compliance Controls - Copyright© 2008, Oracle and/or its affiliates. All Rights Reserved. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Automated Monitoring of SoD Using AACG (continued)

3

Set up the AACG Global Conditions and Global Path Conditions to automatically exclude certain operating units, responsibilities, users or functions from being included in the conflict analysis.

4

Run AACG conflict analysis on selected key SoD rules to detect SoD violations on a regular basis (e.g., quarterly or annual).



The screenshot shows the Oracle Governance, Risk and Compliance Controls interface. The left navigation pane is expanded to 'Global Path Conditions' > 'PEAR21'. The main content area displays a table with the following data:

Registered Instances	Conditions Exists?	Types	Values	Same	Comments
<input type="checkbox"/>	Yes	Users			
<input type="checkbox"/>		Data Group		No	
<input type="checkbox"/>		MO: Operating Unit	AO DE BOOKS;AO DK BOC	No	
<input type="checkbox"/>		Set of Books	EA Poland Reporting;EA Iri	No	
<input type="checkbox"/>		Prompt			
<input type="checkbox"/>		Submenu Grant Flag			
<input type="checkbox"/>		AK Region Code		No	
<input type="checkbox"/>		Query Only			
<input type="checkbox"/>		Function Grant Flag			
<input type="checkbox"/>		Responsibility	PT AP Vendor Maint-Payab		
<input type="checkbox"/>		Menu			
<input type="checkbox"/>		Function			
<input type="checkbox"/>		Role			
<input type="checkbox"/>		Responsibility End Date	Inactive		
<input type="checkbox"/>		User End Date	Inactive		
<input type="checkbox"/>		User Responsibility End Date	Inactive		

Benefits from Monitoring SoD Using AACG

- ➡ AACG provides an auditable framework and process for SoD control
- ➡ Automated process in assessing SoD conflicts raises confidence level of the external auditors
- ➡ Discover SoD conflicts related to hidden functions which manual reviews won't likely detect
- ➡ SoD rule-set provides solid guidelines for business owners to consider when approving user access
- ➡ SoD rules can be set up with any combination of functions or access points to fit different business scenarios
- ➡ Detect any type of conflicts at any time

Benefits of Automated SoD Monitoring Using Oracle AACG

Policy Listing

Stores a repository of SoD rules for Oracle E-business suite across Financials, Procure to Pay, Order to Cash, Human Resources, etc.

SoD Detection

Identifies SoD conflicts based on Oracle ERP environment

Authorized Conflicts

Provides the ability to configure exceptions

Reporting

Detects what access users have and what users can do; generates conflict reports for both within Oracle responsibility and multiple responsibilities assigned to users

Continuous Monitoring

Acts as an effective monitoring tool and helps prevent fraud by limiting what users can do



Q & A

