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







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

orotiviti



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

protiviti[.]

TOP-DOWN SoD AND SECURITY DESIGN METHODOLOGY AND BENEFITS

protiviti°

Page 3 of 29

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

protiviti[。]

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.

Bottom-up

Alternate SoD Design Approach

Top-down

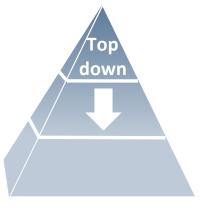
- Business process owners define formal SoD policies. These policies are used as the foundation of SoD design in Oracle ERP environment.
- "Authorized" conflicts are determined at the design level.
- Oracle functions are classified according to formal SoD policies and rules are defined by business process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

protiviti[。]

Alternate SoD Design Approach (continued)

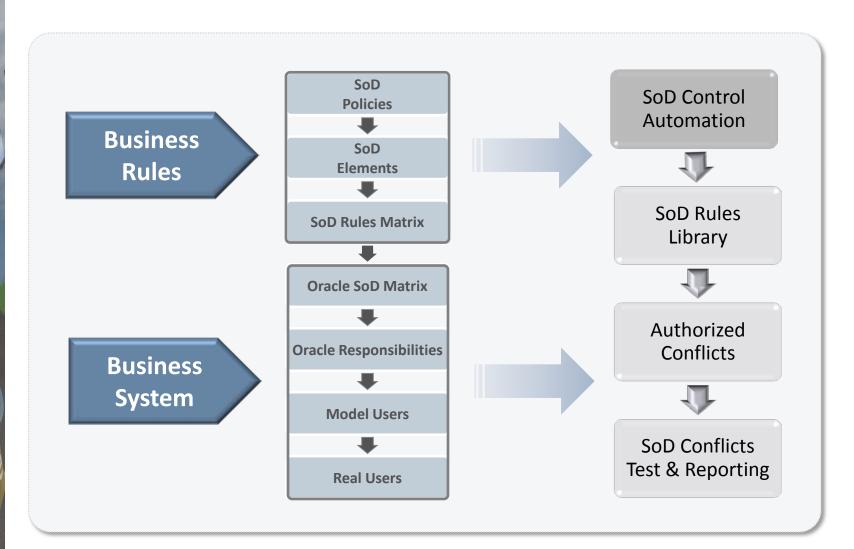
Top-down

- 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.



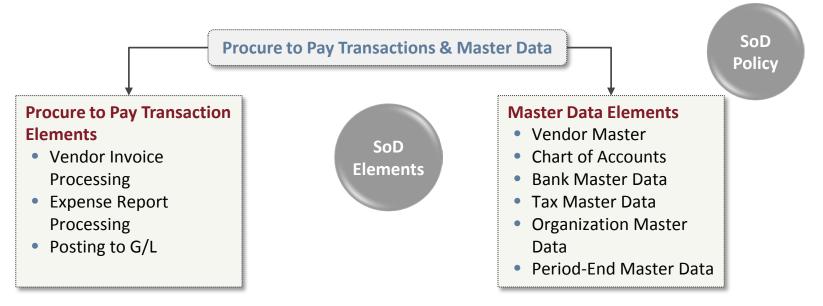
protiviti°

Security and SoD Design Approach



protiviti[®]

Example of SoD Design Elements



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

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

protiviti°

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.

protiviti°

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.





protiviti®

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.

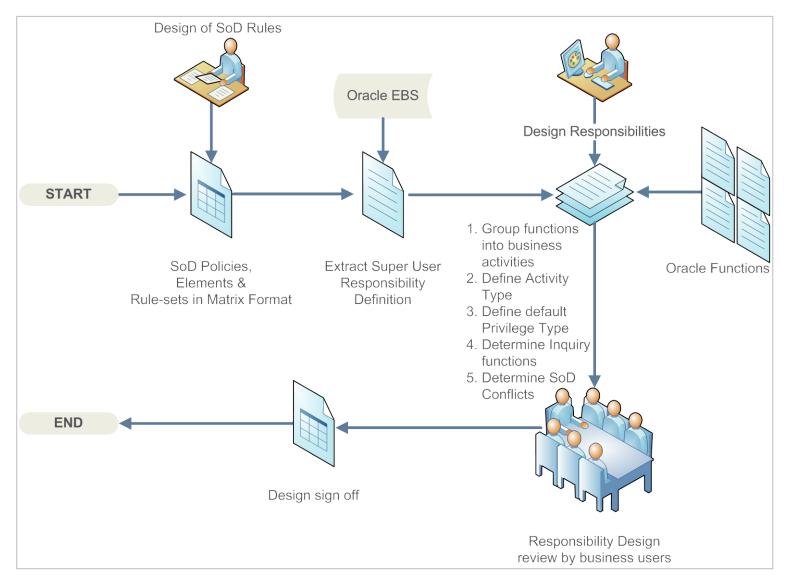


PROTIVITI'S SECURITY DESIGN & BUILD PROCESS

protiviti°

Page 13 of 29

Process Flow – Design Oracle Responsibilities



protiviti[®]

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.

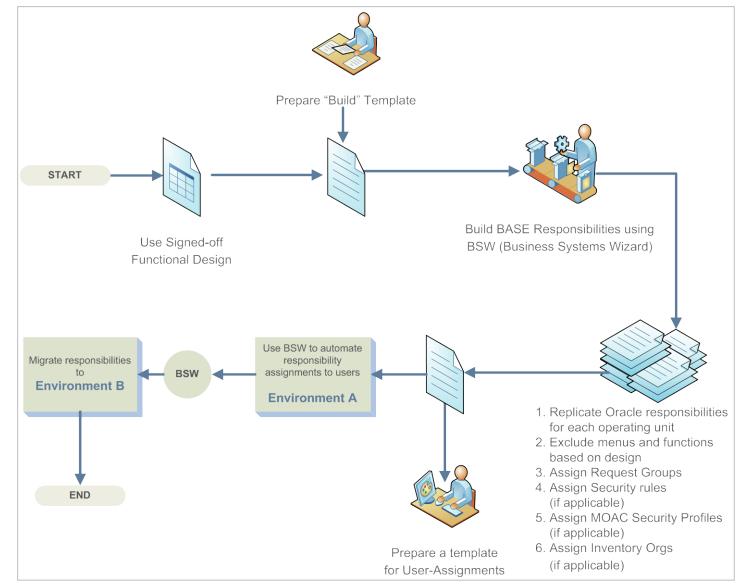
protiviti[。]

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

protiviti

Process Flow – Build Oracle Responsibilities



protiviti°

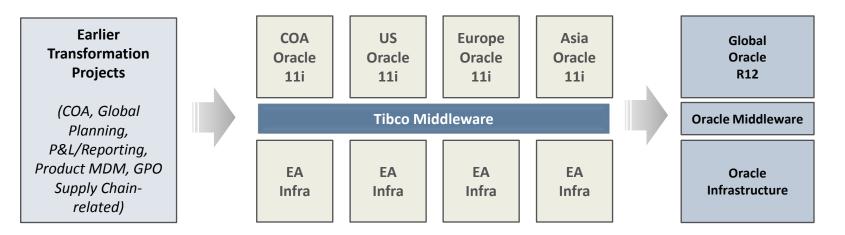
CASE STUDY: PROJECT MERIDIAN – ERP TRANSFORMATION TO ORACLE R12



protiviti°

Page 18 of 29

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



protiviti°

Page 22 of 29

Automated Monitoring of SoD Using AACG

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

protiviti°



Automated Monitoring of SoD Using AACG (continued)



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

vigation «	View - Clear View Manage View Disp	lay • Find Conflicts • Reports	Transfer 🔹	Actions - Save	Help				
- Home	Policy Name*	Description	Policy Type*	Priority* Stat	us" Ef	ffective Date*	At		
Access Governor									
Definition	(PEAR2I) - GL FX Rates; CE Bank Reconciliation	PEAR2I - OTC	Monitor	1 Acti	ve 08	8/26/2011	30		
= Entitlements	(PEAR2I) - TM IT Setup; AR Enter Credit Memos/A	Adjustments PEAR2I - OTC	Monitor	1 Acti	ve 08	8/26/2011	08		
I Global Conditions	(PEAR2I) - CE IT Setup; CE Bank Reconciliation	PEAR2I - P2P	Monitor	1 Activ	ve 08	08/26/2011			
Global Path Conditions	(ERPEUPD) - Item Master; Purchase Order Entry; F	Receiving Tran ERPEUPD - P2P	Monitor	1 Acti	ve 08				
E C Remediation	(ERPEUPD) - Item Master; Purchase Order Entry	ERPEUPD - P2P	Monitor	1 Acti	ve 08	8/24/2011	0		
🗉 🦲 User Provisioning	(ERPEUPD) - INV - Inventory Transfer; INV Invent	ory Adjustme ERPEUPD - P2P	Monitor	1 Acti	ve 07	7/29/2011	0		
Transaction Governor	(ERPEUPD) - INV - Inventory Adjustments	ERPEUPD - P2P	Monitor	1 Activ	ve 07/2	7/29/2011	30 30		
Report Center	(ERPEUPD) - CST - Average Cost; INV - Item Cost	Update; Purc ERPEUPD - P2P	Monitor	1 Acti	ve 07	7/29/2011			
Jobs	(ERPEUPD) - AR Customer Credit Management; Sa	les Order ERPEUPD - OTC	Monitor	1 Acti	ve 07	7/29/2011			
Administration	(ERPUSPD) - AR Customer Master; AR Approve Ad	justments ERPUSPD - OTC	Monitor	1 Acti	ve 03	3/30/2010	0		
	(PEAR2I) - Supplier Master: Requisition Entry: Rece	elving Transac PEAR2I - P2P (High	h) Monitor	1 Act/	ve 03	3/24/2010	0		
	Image: 1 of 23 ▶ Image: 20 of 45 Displaying 1 - 20 of 45 Displaying 1 - 20 of 45								
	(ERPEUPD) - Item Master; Purchase Order Entry; Receiving T	ransactions			00,	laying 1 - 20 0			
	IDR AND, Access Points*					Delete			
		Description	Datasource	Platform	Element Type	Control			
	E AND								
	PO Receiving Transactions - (ERPEUPD)	Access to Corrections, Shipments	, F		Entitlement				
	PO Purchase Order Entry - (ERPEUPD)	Access to PO Purchase Order Ent	ry		Entitlement				
	INV Item Master - (ERPEUPD)	Access to Item Master functions			Entitlement		1		
	4 m •								
	((([Entitlement]PO Receiving Transactions - (ERPEUPD) - (([Function]RCV_RCVRCMUR(instance: ERPEUPD)), ([Function]RCV_RCVTXECO(instance: A ERPEUPD)), ([Function]RCV_RCVTXERC(instance: ERPEUPD)), ([Funct								
	ERPEUPD)))) AND ([Entitlement]PO Purchase Ord	er Entry - (ERPEUPD) - (([Function]	PO_POXPOVPO_OP	EN(instance: ERP	EUPD)), ([Functio	in] -	-		

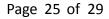
Automated Monitoring of SoD Using AACG (continued)

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.

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

ORACLE Governan		phance contro	15	Home P	ofile Help Abou	it Logout User Name: He
= Home	Registered Instances	Conditions Exists?	Types	Values	Same	Comments
Access Governor		Yes	Types	values	Same	continents
= C Policy	E PEAR2I	Yes				
Definition			Users			
Entitlements			Data Group	AO DE BOOKS:AO DK BOC	No	
Global Conditions			MO: Operating Unit			
ERPEUPD			Set of Books	EA Poland Reporting;EA In	No	11
ERPUSPD ERPUSRP			Prompt			
E PEAR2I			Submenu Grant Flag			11
+I Global Path Conditions			AK Region Code		No	
- Remediation			Query Only			
Conflict Analysis			Function Grant Flag			
=] Simulation			Responsibility	PT AP Vendor Maint-Payab		
= Work Queue			Menu			
= SOD Heatmap			Function			10 0
🛨 🦲 User Provisioning			Role			
Transaction Governor			Responsibility End Date	Inactive		
E Report Center			User End Date	Inactive		
Conflict Reports	0		User Responsibility End Da	Inactive		
Policy Reports User Provisioning Reports Jobs Administration						





Automated Monitoring of SoD Using AACG (continued)

Analyze the conflict extract reports to eliminate false positives and identify true intra and inter responsibility conflicts.

Work with the business owners to determine proper remediation actions such as remove certain functions from the responsibilities and/or change the user assignments.

- A		c	D	1	Γ.	6	H	1	1
ccess Con	flicts Extract Report								
	inter Exclusion response								
port Parameter									
Inflict Run Confi	ct Run 01403(2011 05 59 05 PM								
NorName lizead	N-payables invoice entry supplier								
Cobal User	User full Name	Bole	Policy Name	Dakey Description	Public Tone	Bulley Clabo	Dalley Drivert	Palicy Effective Data	Entitionent Names
-	User Full Name						-	-	
		EU NHUS 1 AP Invoice Entry-Payables	(FEAR2t) - Payables Invoice Entry Supplier Master	PEAR21+P2P((H4ph)	Monitor	4:5+0	1.	5242015	AP Supplier Master - (PEAR21)(2
		EU 144001 AP INVICE ENTY-Payables		PEAR3 - P2P (High)	NOVOR	A(3)(8	- T	3/24/2010	AP Supplier Matter + (PEAR21)(2)
		EU NAMON AP Invoice Entry-Payables	PEAR20 - Pavables Invoice Entry Supplier	PEARS - PSP 04um	Mandaur	4.9.4		5/24/2010	AP Supplier Master - (PEAR21)/2
			Master			~~~	12		
		EU NHUST AP Invoice Entry-Payables	(PEAR2I) - Payables Invoice Entry, Supplier	PEAR21-P2P(High)	Mondor	Active		3242010	AP Supplier Master - (PEAR2I)(2
		EU NHUS 1 AP Invoice Entry-Payables	(FEAR2t) - Payables Invoice Entry: Supplier	PEAR21-P2P (High)	Monitor	Adlve	1	3242030	AP Supplier Master + (PEAR21)/2
		EU NAUS1 AP INGICE ENTY-Payables	Master (PEAR20 - Paysoles Invoice Entry, Supplier	PEAR2 - P2P 08050	Monthly	Active		3/24/2010	AP Supplier Mainer - (PEAR21)/2
			Magier					1.000	
		EU NHuh 1 AP Invoice Entry-Payables	(PEAR2t) - Payables Invoice Entry, Supplier Master	PEAR21 - P2P (High)	Monifor	Active		3/24/2010	AP Supplier Masher - (PEAR2I)(2
		EU HHUST AP INVOICE ENTY-Payables	(PEAR2I) - Payables Invoice Entry, Supplier	PEARS - PSP (HIP)	Monitor	Active	1	3/24/2010	AP Supplier Master - (PEAR2))2
		EU NANUS 1 AP Invoice Entry Payables	Master (PEAR20 - Pavaties Invoice Entry Supplier	PEARS - P2P (Han)	Mandar	Active		3040010	AP Supplier Master - (PEAR21v2
		EU fanus 1 Ar Invoice Entry Prayables	UptAV20 - Pavaties Invoice Entry, Subdiver	PEAKS - P2P (High)	Monitor	ACEVE		3242010	AP Supplier Master - (PSAR2152
		EU NHUO LAP Imoice Entry-Payables		PEAR21-P2P(HgP)	Monifor	Active	1	3/24/2010	AP Supplier Master - (PEAR2()(2
		EU NEWD1 AP Invoice Entry-Parables	Vapler (FEAR2) - Parables Invoice Entry Supplier	PEARSI-PSP (High)	Monitor	Active		3242010	AP Supplier Master - (PEAR2112
		EU takent all process Entry-Paraties	Matter		Monthly	470.0		3/24/2018	#P Support Master - (PE #R21x)
		ED JIHOUT NY BROICE END/-P 30 2045	(PEAR2) - Payables Invoice Entry, Supplier Master	PEAR3 - P2P (High)	montor	4(5)4		9/24/2010	we problem matter - (werecht)
		EU NHAD1 AP Invoice Entry Payables	(FEAR2t) - Payables Invoice Entry: Supplier	PEAR21 - P2P (High)	Monitor	Active	1	3/24/2010	AF Supplier Masher - (PEAR25)2
		EU hHub1 AP invoice Entry-Payables	(FEAR20 - Parables Invoice Entry, Supplier	PEAR21-P2P (High)	Monitor	Active		3242010	AP Supplier Master - (PEAR202
			Master						
		EU NHUS1 AP Invoice Entry Payables	(PEAR20 - Pauables Invoice Entry, Supplier Master	PEARS P2P (High)	Montor	Adhre		3242010	AP Supplier Master - (PEAR21)2
		EU Meuo 1 AP monce Entry-Payables	(FEAR2I) - Payaties Invoice Evity, Supplier	PEARD - P2P (High)	Monitor	A(Sve	1	3/24/2010	AP Supplier Master - (PEAR20)2
		EU NHUST AP Invoice Entry-Payables	Master (PEAR20 - Pavaties Invoice Entry, Supplier	PEARS-PSP (Hotel)	Monday	Active		3/24/2010	AP Supplier Master - (PEAR2552
			Master						
		EU NHUS 1 AP Invoice Entry-Payables	(PEAR2I) - Payables Invoice Entry, Supplier Master	PEAR21-P2P (High)	Montor	Active	1	3242010	AF Supplier Master - (PEAR20)2
		EU NHub1 AP Invoice Entry Parables		PEAR21 - P2P (High)	Montor	Adive	1	3/24/2010	AP Subdier Master - (PEAR21)/2
		EU Meso 1 AF Invoice EntruFacebles	Vaster (FEAR20 - Paratites Invoice Entry, Sopplier	PEARS - P2P 04ch0	Months	4:0+0		5040010	AP Supplier Master - (PEAR21)2
		and the second second second	Masler	Contraction (1997)			- 18		
B. Arrant File	ficts Extract Report	and Bernhammer Research and Bernhammer	and the second se		THE R.				

6



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

Stores a repository of SoD rules for Oracle E-**Policy Listing** business suite across Financials, Procure to Pay, Order to Cash, Human Resources, etc. Identifies SoD conflicts based on Oracle ERP **SoD Detection** environment Authorized Provides the ability to configure exceptions **Conflicts** Detects what access users have and what users can do; generates conflict reports for both within Reporting 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





protiviti[。]