Understanding ERP Architectures, Security and Risk

Brandon Sprankle, Director, PwC

In-Depth Seminars – D31

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Agenda

1. Introduction
2. Overview of ERP security architecture
3. Key ERP security models
4. Building and executing ERP security audit plan
5. ERP security audit example – Oracle e-business suite R12
6. Summary
7. Questions

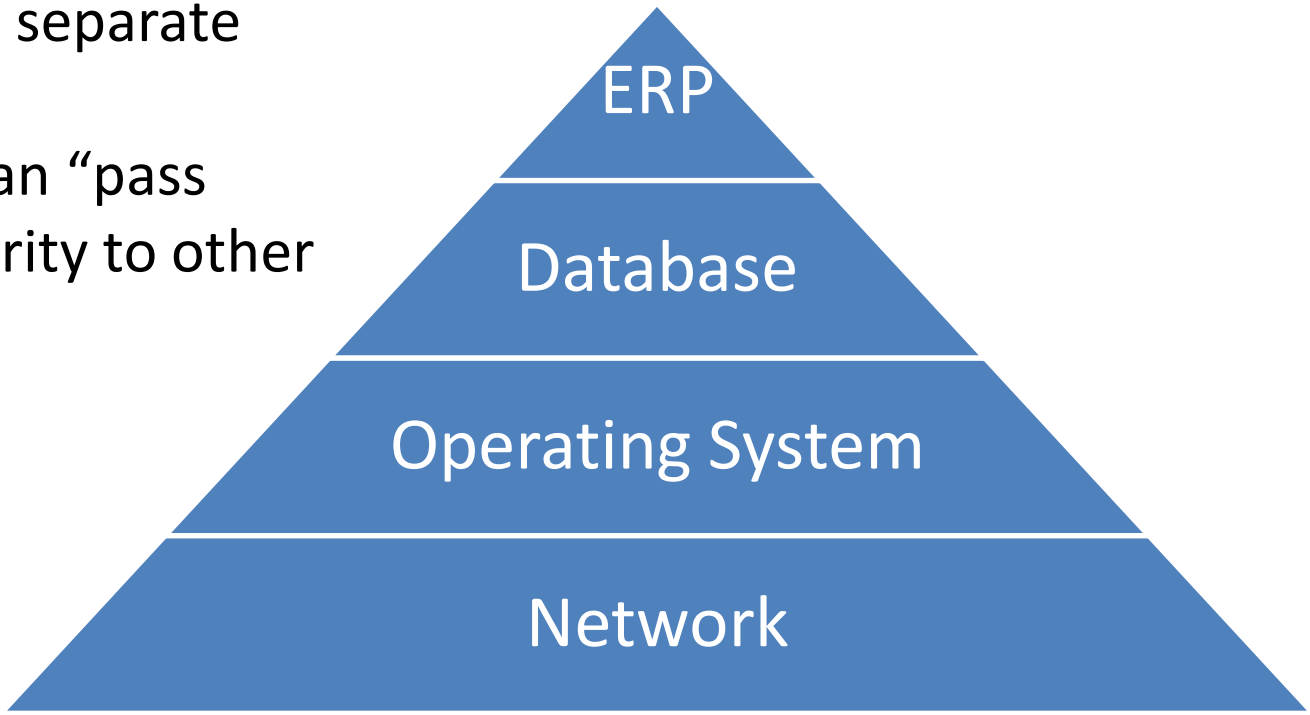
INTRODUCTION

OVERVIEW OF ERP SECURITY ARCHITECTURE

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

ERP Security Architecture Overview

- Each layer has separate security
- Some layers can “pass through” security to other layers

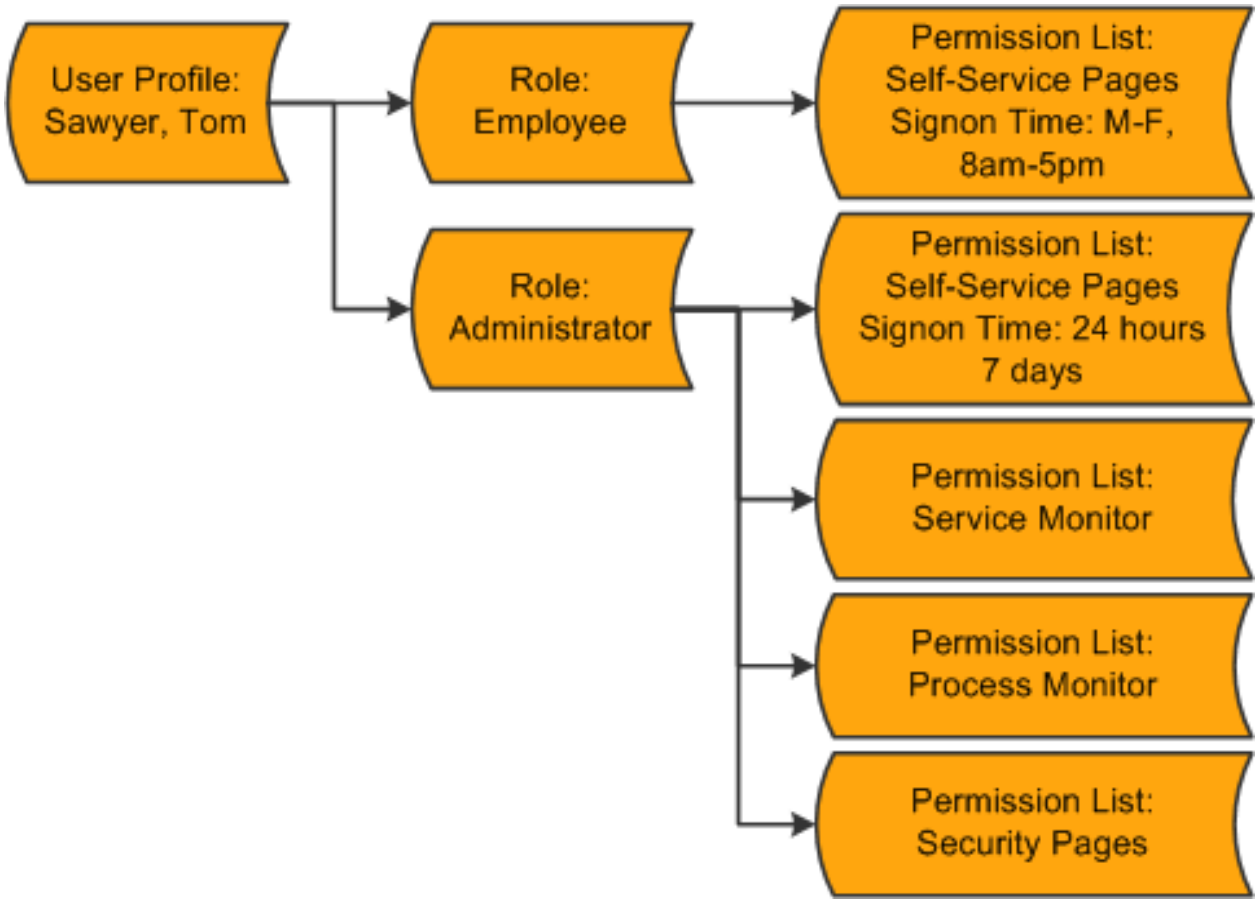


ERP Security

ERP security depends on the application for specifics, but overall each share the major traits in common:

- User accounts – superuser, admin
- Roles / responsibilities – functions, forms, data, reports
- Permissions – allowable functions within or outside roles

ERP Security Example

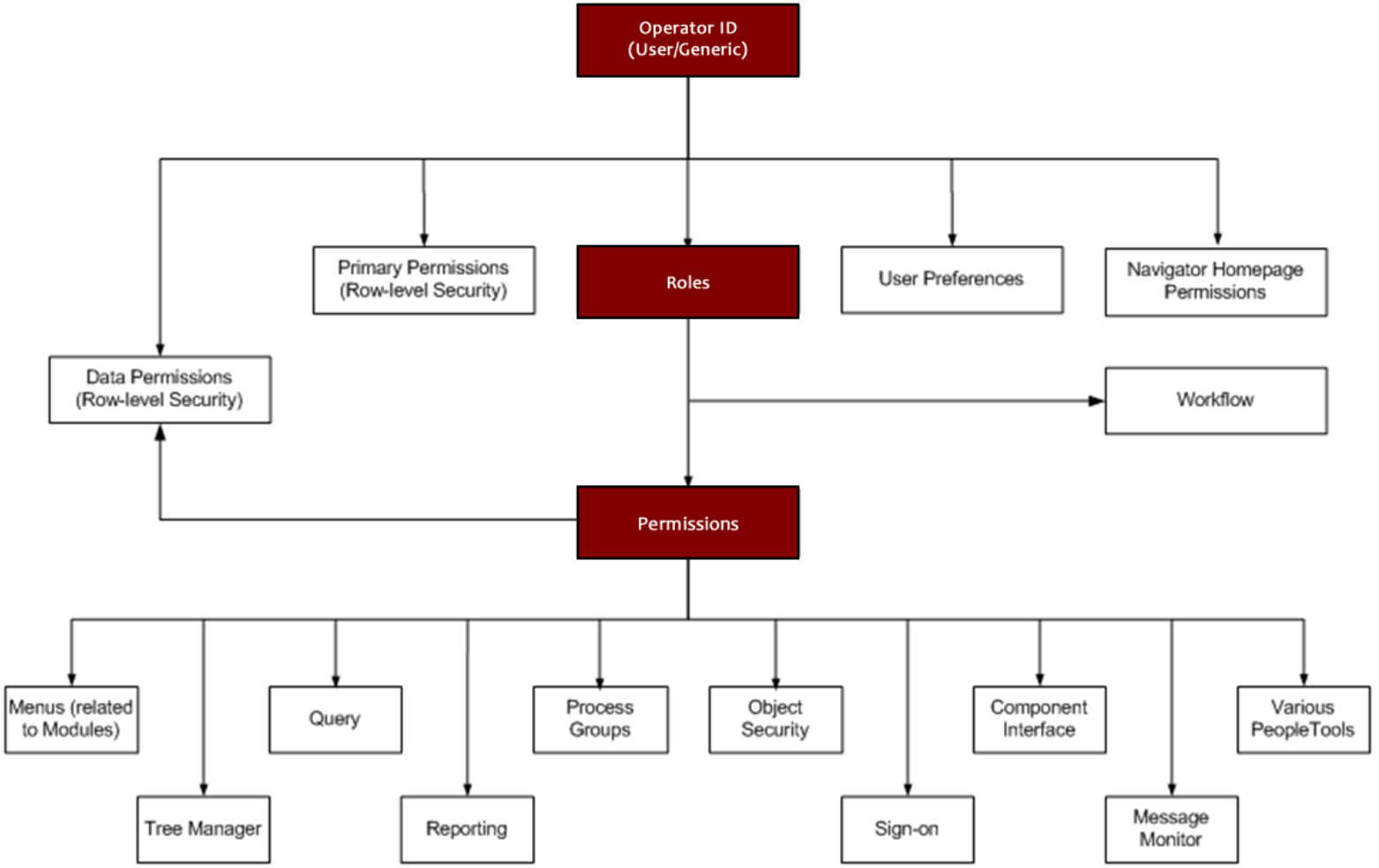


Other ERP Security Principles

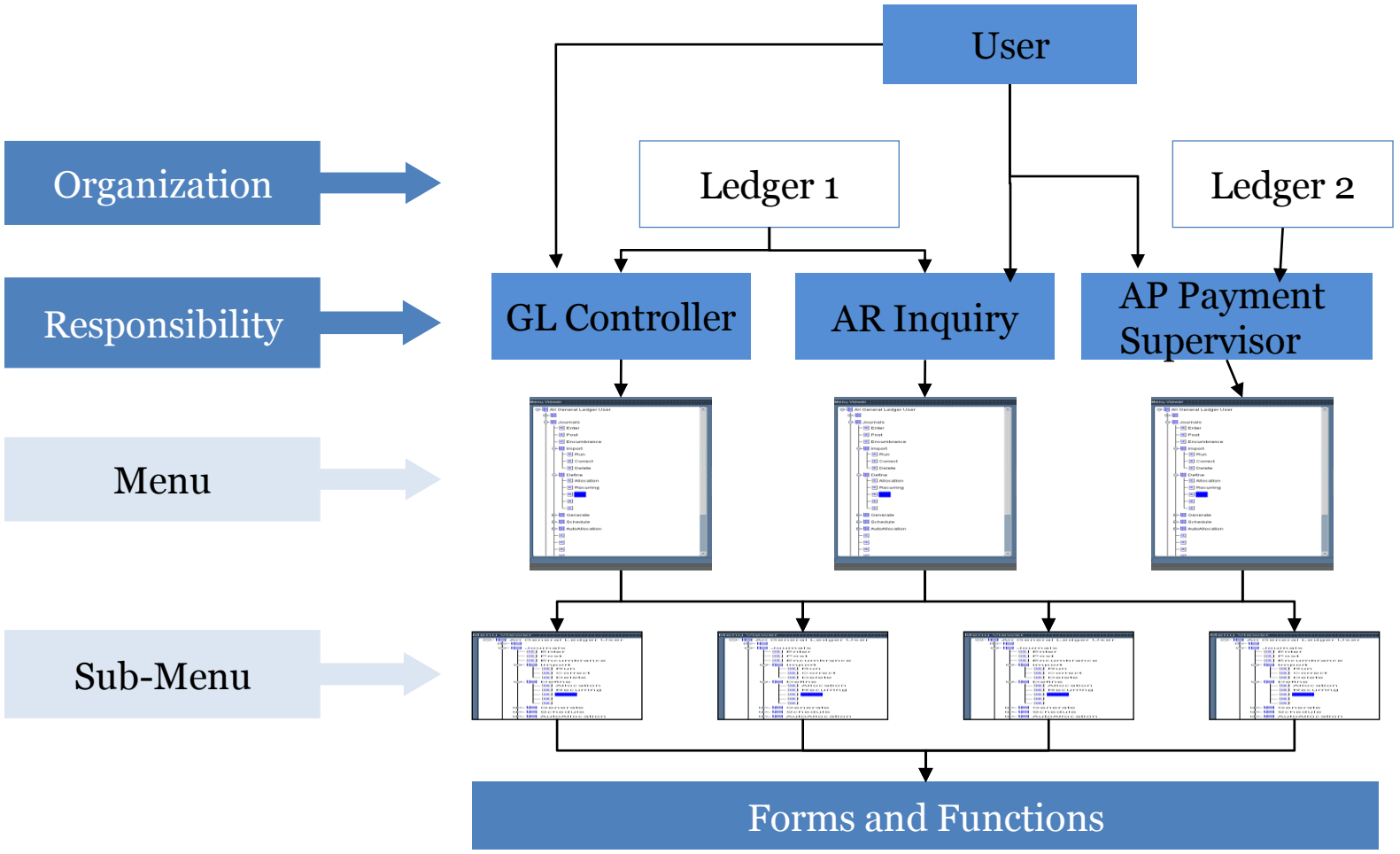
- Responsibilities usually cannot cross modules
- Multiple paths to same function
- Customizations typically effective security
- Verify how third-party modules/applications interact with ERP

KEY ERP SECURITY MODELS

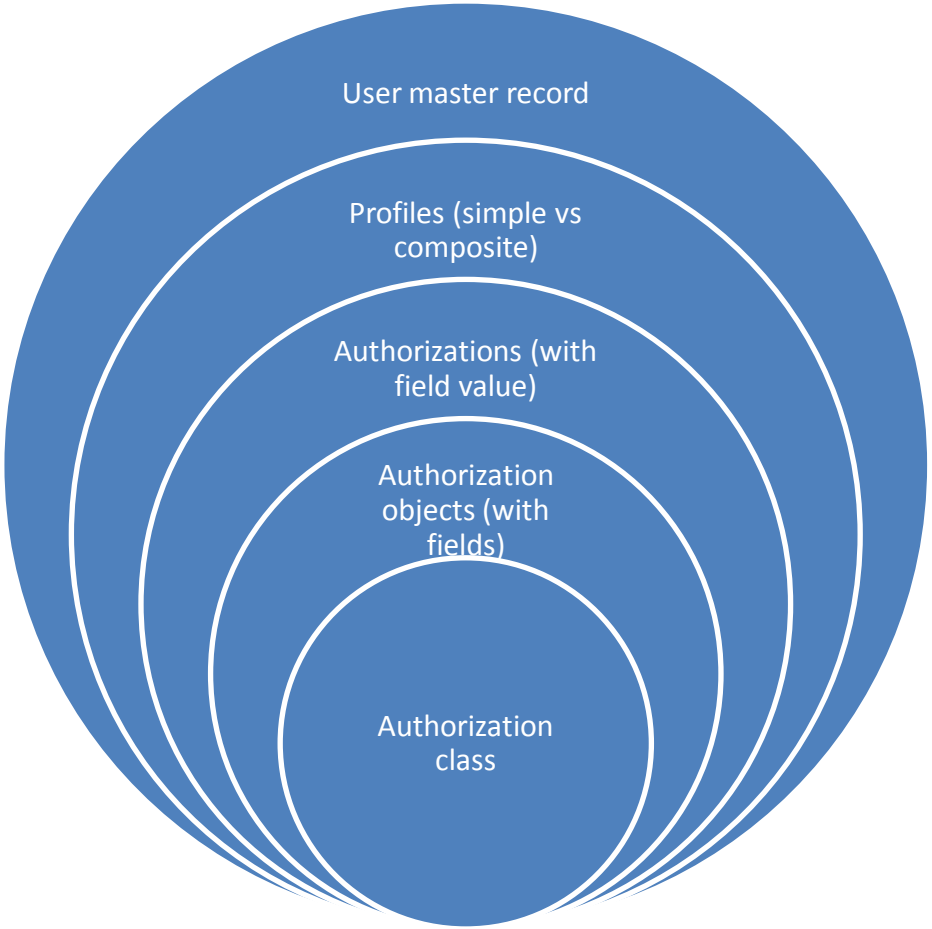
Security Model - PeopleSoft

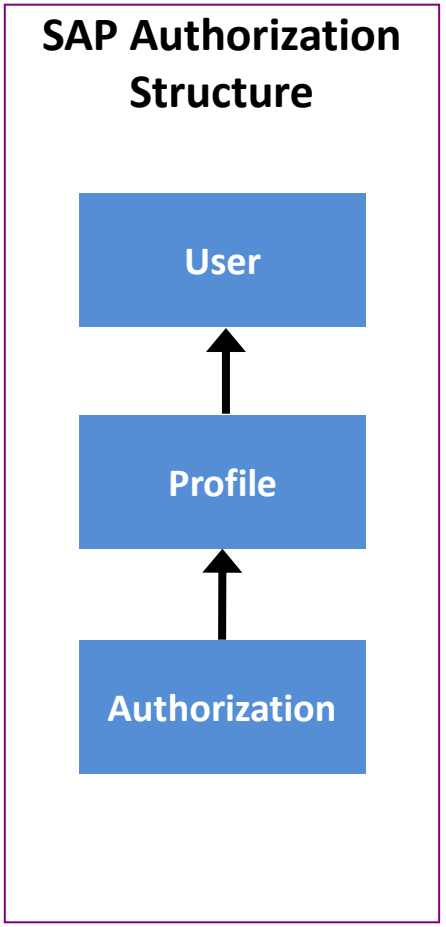


Security Model – Oracle EBS



Security Model – SAP



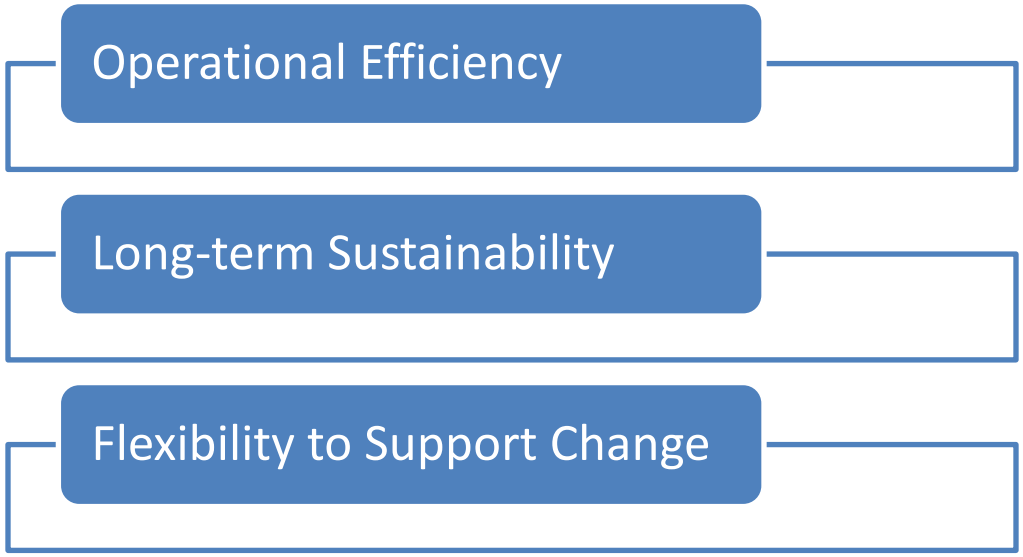


BUILD AND EXECUTE AN ERP SECURITY AUDIT PLAN

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Why Do Issues Exist with ERP Security?

Many ERP implementers focus on the following:



Missing is **Internal Control Compliance**

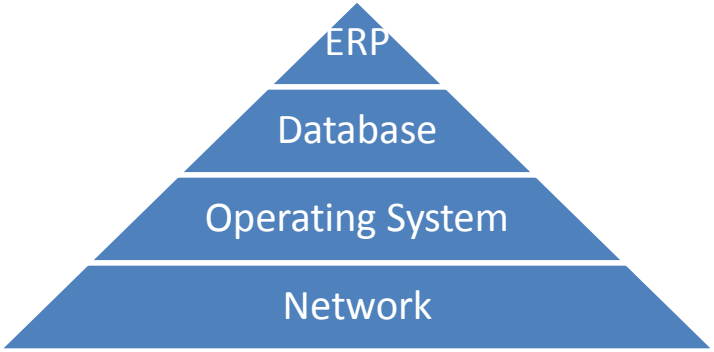
Key ERP Security Documents

- Menu/responsibility design matrices
- Role and responsibility design matrices
- Responsibility-to-Role mapping
- User-to-Role mapping
- Documented User Acceptance Test (UAT) scenarios and scripts
- Documentation of procedures for maintaining roles/responsibilities
- Configured segregation of duties (SOD) compliant roles/responsibilities

Example Design Document

Responsibility Name	Menu	User Menu Name	Menu Type	Description	Prompt	SUB_MENU	FUNCTION	Description	Exlude function at the Responsibility Level	Exclude sub-menu at the responsibility Level
PO INQUIRY	PO_INQUIRY_MENU	PO_INQUIRY	Standard Menu	PO Inquiry Menu					Releases PO Summary: Open Document PO Summary: Create New Release PO Summary: Create New PO Control Purchase Orders PO Preferences Purchase Orders	
					MPN Query-Only		Manufacturers' Part Number Query-Only	Manufacturers' Part Number Query-Only		
					Item Information	INV_INVIVATT_ALLORG	View Item Attributes	View Item Information		
					Item Search		Items Search	Item Search		
					Purchase Order Summary	Purchase Orders Summary: Subfunctions	Purchase Order Summary	Buyer Workbench		
					PO Change History		View Purchase Order History	View Purchase Order History		
					PO Change History		Purchase Order Revision History	Purchase Order Revision History		
							View Tax Details	View Tax Details		
							View Tax Details By Code	View Tax Details By Code		
					Reports	Reports:		Reports		
PO SETUP	PO_SETUP_MENU	PO_SETUP	Standard Menu	PO Setup Menu						
					Item Search		Items Search	Item Search		
					Setup	Setup:		Setup	Responsibility level Menu and/or	
					Reports	Reports:		Reports		
					Run		Requests: Submit	Submit requests		
					View		Concurrent Requests: View	View completed requests		
					Set		Request Sets (User Mode)	Define standard request sets		

ERP Security Architecture



- Closer to data represents more risk – ERP and database
- Understand if “pass through” security is enabled
  - Example: OS controls security for database
- Does network security directly interact with ERP?
  - Example: Internet sales

ERP Security Audit Considerations

- Type of ERP is important – ensure you understand how security is designed
- Workflow in ERPs can override or modify standard security – very few tools evaluate it
- Consider all access assigned to user accounts, not just individual responsibilities
- Consider tools that automate security analysis – difficult to effectively evaluate security manually

Building the ERP Security Audit Plan

- Leverage technical resources and security design documents
- Consider all access points and infrastructure
- For complex ERPs (i.e. Oracle, PeopleSoft, SAP) consider use of tools or ACL
- Understand all modules implemented and in-scope for review

Executing the ERP Security Audit Plan

- Start with a listing of user accounts
- Determine what responsibilities each user account is assigned
- Assess the access for each individual responsibility and across responsibilities
- Review any additional access outside of responsibilities (permissions)

Executing the ERP Security Audit Plan Continued

- Obtain user accounts owners' job descriptions to determine appropriate access
- Identify excessive access and/or segregation of duties points
- Discuss with system administrators, process owners, data owners, etc. if access is appropriate
  - Consider other controls impact (manual controls, review controls)

ERP Security Audit – Lessons Learned

- Remember analysis is point-in-time – understand processes for continuous security
- “False positives” typically are not false
- Consider determining if excessive access was used – powerful analysis
- Collaboration with security administrators is critical

ERP SECURITY AUDIT EXAMPLE – ORACLE E-BUSINESS SUITE R12

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Oracle EBS R12 Security Architecture

Key Concepts

- Users: Each application user has an unique user ID and password.
- Responsibilities: Link a user ID to a main menu and control how a user gains access to menus, forms, functions, sub-functions, and data.
- Menus: Hierarchical arrangements of application forms and sub-functions.
- Functions: Part of an application's functionality.
- Form functions are commonly known as forms
- Non-form functions are commonly known as sub-functions

Oracle EBS R12 Security Architecture Continued

Key Concepts

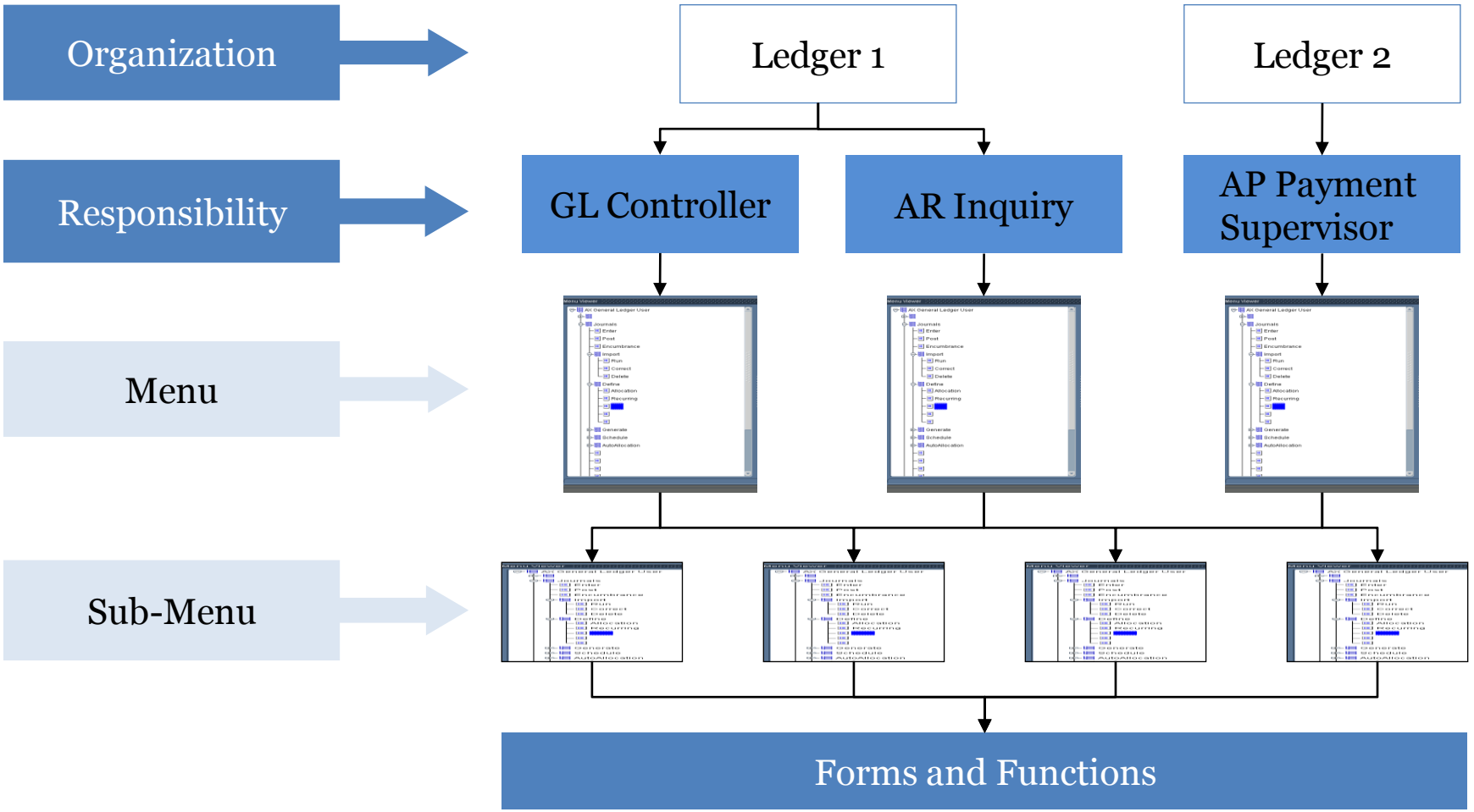
- Menu/Function Exclusions: Restrict application functionality accessible to a responsibility.
- A function exclusion excludes all occurrences of that function from the responsibility's menu
- A menu exclusion excludes all occurrences of that menu's entries (i.e. all functions, and menus of functions that it selects) from the responsibility
- Profile Options: Affect the operation of the applications and set according to the needs of the user community.

Oracle EBS R12 Security Architecture Continued

Key Concepts

- Flexfield Security Rules: Restrict the accounts users may post transactions to and run reports against.
- Request Security Groups: Define programs and reports (or request sets) that may be run by a responsibility.
- Permissions and Permission Sets: Smallest unit of securable action (maps to a menu item/function)
- Role Based Access Control (RBAC): Users are assigned multiple responsibilities through a single role.

Security Overview – Oracle EBS R12



Oracle R12 Security Audit – Company Background

- US-based company technology company with limited international transactions
- Approximately $1B in annual revenue
- 2,500 employees
- Oracle R12 modules installed were: System Administration, GL, Purchasing, AP, AR, Projects, Assets
- Third party application used for revenue recognition – directly interfaces to Oracle R12

Oracle R12 Security Audit

- Obtained listing of data from “Key Concepts” slides and put into Access database
- Joined the various fields to perform analysis over user account security
  - 82 user accounts with approximately 350 responsibilities – took 350 hours to analyze
  - Tool did analysis in approximately 10 hours
- Identified multiple issues

Oracle R12 Security Audit Issues

- 37 user accounts had excessive access
- Multiple segregation of duties issues identified
- “False positives” became reality due to backdoor access
- Following slides list more interesting issues

Issues Encountered – Delegated Administration

- Privilege model that:
  - Enables assigning of required access right to manage a specific subset of the organization's users and roles
  - Enables delegation to local administrator at division or department level or even to administrators of external organization(s)
- Following administrative privilege categories can be delegated:
  - User Administration Privileges
  - Role Administration Privileges
  - Organization Privileges

How Identified – Delegated Administration

Risk:

- Admin privileges may be granted inappropriately or excessively to Oracle users = risk of data security and violation of segregation of duties rules.

Control:

- Delegated administrative access is assigned to only authorized employees based on company policy and such scope of such access is based on their job responsibilities.

Testing procedures: Determine if…

1. Delegated administration roles are defined according to company policy.
2. Users are assigned to delegated administration roles according to company policy and their job responsibilities.

Issues Encountered – Proxy User Delegation

Oracle EBS users can nominate another user (proxy user) to act on their behalf – users no longer need to share passwords

- This gives all-or-nothing delegation capability
- Start and end dates can be defined to limit the duration of proxy access

Users with Manage Proxy access can have following functions:

- Setting up Proxy Users
- Delegating Proxy User Privileges
- Acting as a Proxy User
- Running the Proxy User Report

How Identified – Proxy User Delegation

Risk:

- Proxy users access may be granted inappropriately or excessively to Oracle users resulting in risk of data security issue and/or violation of segregation of duties.

Control:

- Proxy user related privileges are granted only on an exceptional basis based on proper approval and there is a procedure to monitor the proxy user activity. Such access delegation should also end-dated by the delegating user.

Testing procedures: Determine if…

1. The ability to delegate proxy privileges to other users is restricted and monitored following company policy.
2. The procedure is in place to review the proxy user activity by the delegating user.

Remediation Efforts

- Company accepted all findings after discussion
- Access issues were remediated in approximately two months
- Decided to implement Oracle GRC going forward to actively monitor security

SUMMARY

Remember These Items

- Technical knowledge is critical to a successful ERP audit
- Ensure a holistic understanding of security layers and other applications interfacing ERP
- Tools may be more efficient and effective – consider them for larger reviews

Questions?

- Thank you for your time