



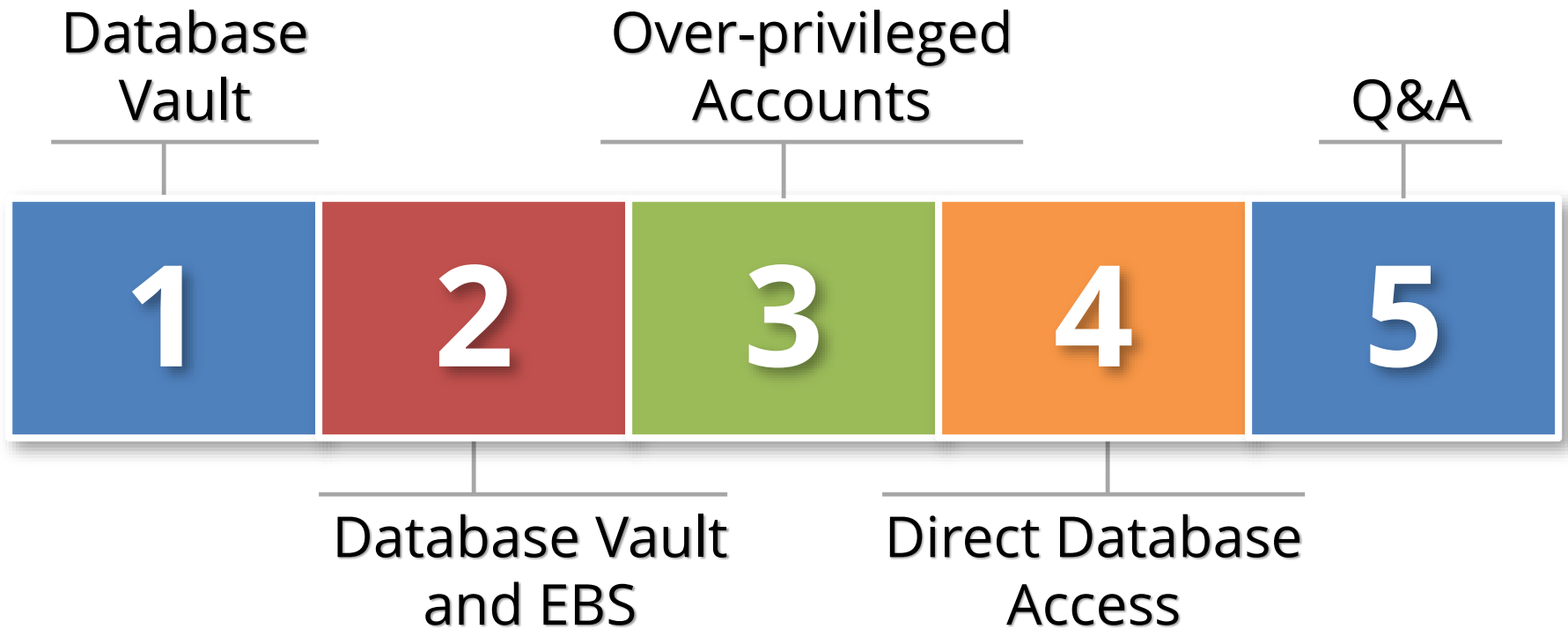
Solving Oracle E-Business Suite Security Challenges with Oracle Database Vault

December 17, 2015

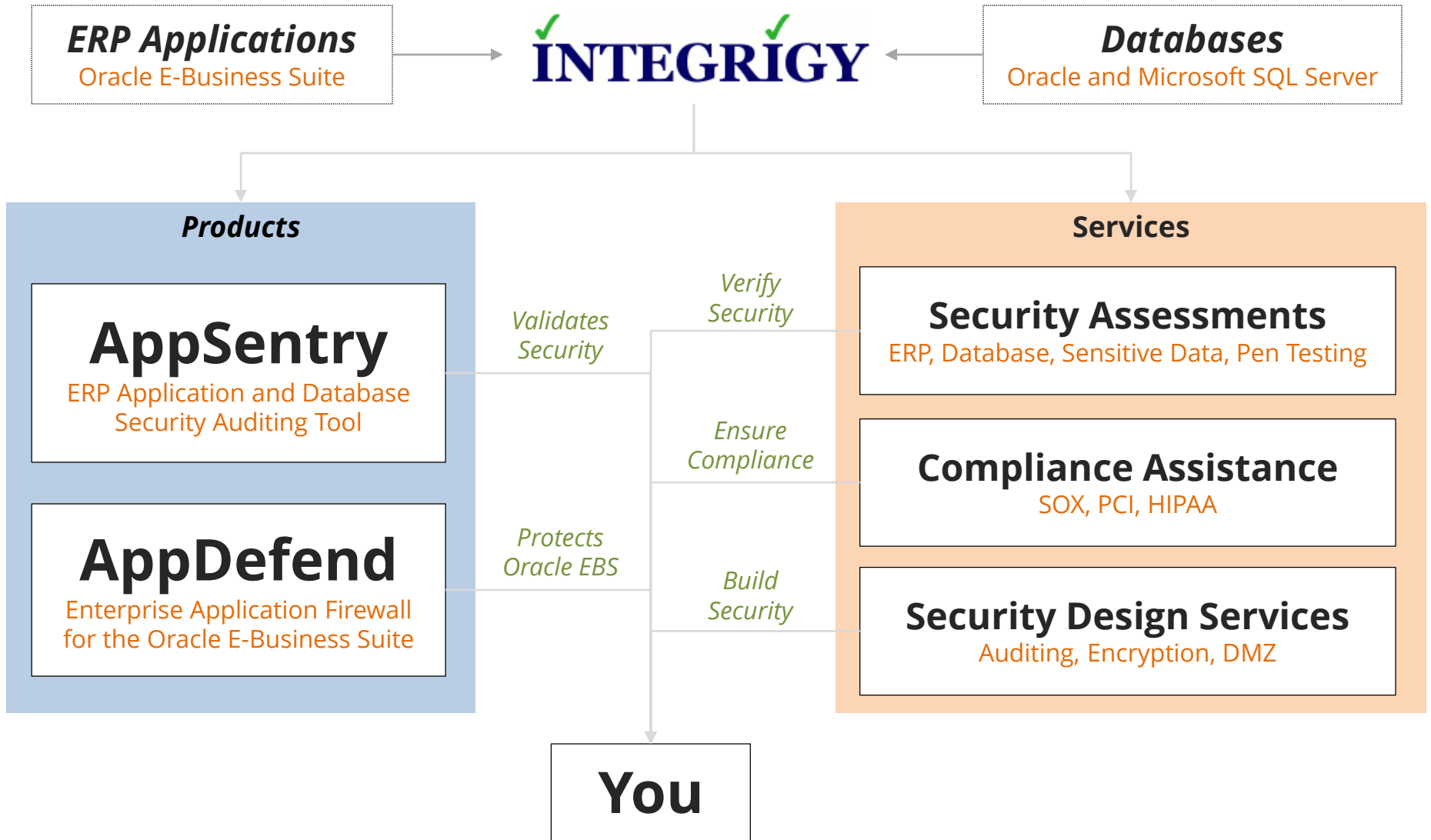
Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

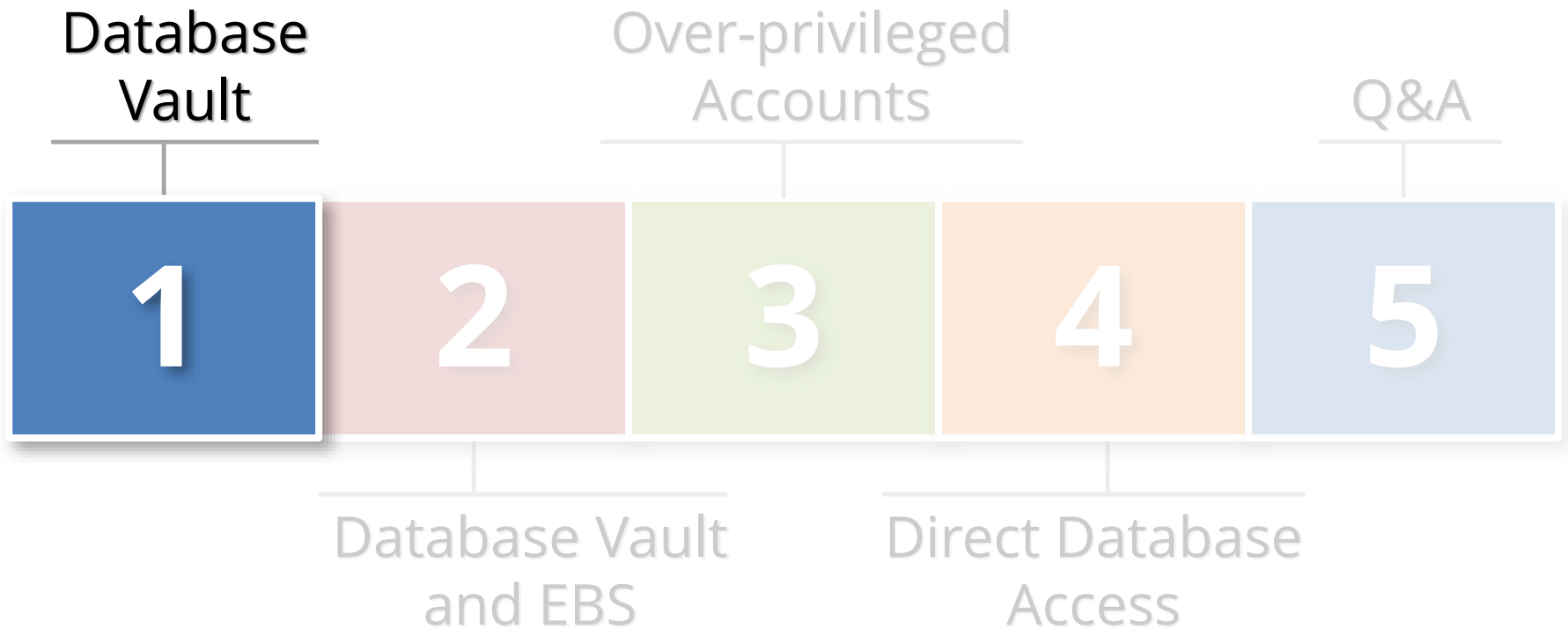
Agenda



About Integrigy



Agenda



What is Oracle Database Vault?

- **Enhanced data protection**
 - Data protection realms
 - Control by IP address, time, etc.
 - Control individual SQL commands and other database operations
- **Layer on top of existing table, system, and role privileges**
- **Provides segregation of duties between DBA and security administrator**
- **Add-on option, licensed separately**

Database Vault Capabilities

- **Database Vault taketh away, never giveth**
 - Must always have an underlying system, object, or role privilege
- **Realms control system privileges like ANY**
 - No effect on direct object privileges
 - No effect on PUBLIC object privileges
- **Command rules control execution of SQL commands**
- **Views must be explicitly protected just as with standard database access controls**

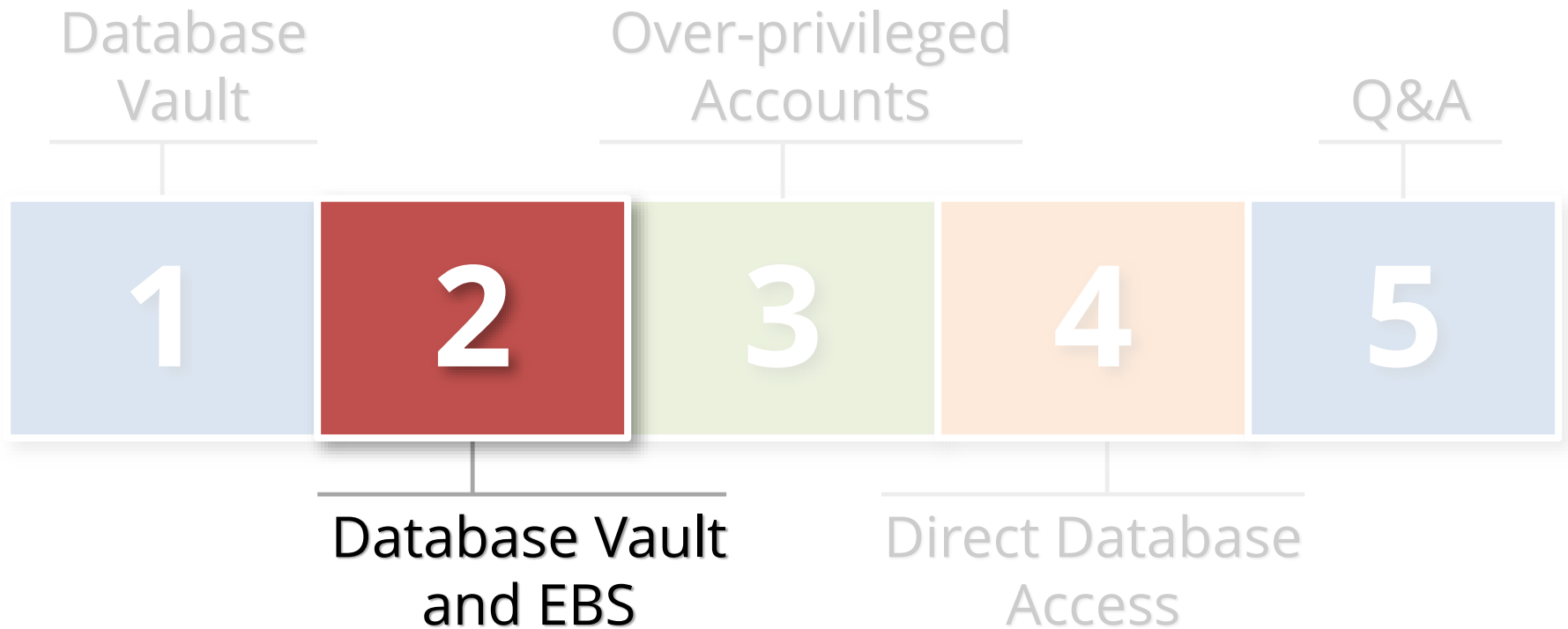
Database Vault Components

Realms	<ul style="list-style-type: none">▪ Realms control system privileges like ANY▪ No effect on direct object privileges▪ No effect on PUBLIC object privileges
Command Rules	<ul style="list-style-type: none">▪ Control execution of any SQL statement including SELECT, ALTER, DML, and DDL▪ Can be specific to SQL statement and object
Rule Sets	<ul style="list-style-type: none">▪ Collection of one or more rules to further define or restriction authorization of realms and command rules▪ Rules may be initializations or factors such as client IP address or operating system user
Factors	<ul style="list-style-type: none">▪ A session attribute or variable that can be used in rules to restrict authorization of realms and command rules▪ Factors for a session may be database user, client IP address, program name, client identifier, etc.

Database Vault Audit Data

- **Database Vault can audit all realm and command rule success or failures**
 - Writes the audit trail to the DVSYS.AUDIT_TRAIL\$
 - Most often only failures are audited
- **Database Vault console includes reporting functionality to view audit trail**

Agenda



EBS and Database Vault Certifications

Oracle Database Version	11.5.10.2	12.0.x	12.1.x	12.2.x
10.2.0.3	✓	✓	✗	(2)
10.2.0.4	✓	✓	✓	(2)
10.2.0.5	✓	✓	✓	(2)
11.1.0.7	✓	✓	✓	(2)
11.2.0.3	✓	✓	✓	(3)
11.2.0.4 (recommended)	✓	✓	✓	(3)
12.1.0.1	✗ ⁽¹⁾	?	(3)	(3)
12.1.0.2	✗ ⁽¹⁾	?	(3)	(3)

(1) Not planned

(2) Database version not certified for EBS version

(3) Certification pending as of December 2015

EBS and Database Vault Certifications

ORACLE MY ORACLE SUPPORT PowerView is Off Stephen (Not Available) (0) Contact Us Help

Certifications Systems Collector Advanced Customer Services More...

Search Results: Oracle E-Business Suite 12.1.3

Certification Search

Search Saved Recent

Compare Releases and Platforms

* Product: Oracle E-Business Suite * Release: 12.1.3 Platform: Any

Check certifications with another product

Clear Save Search

Certification Results

Displaying Oracle E-Business Suite 12.1.3 Certifications. Group by Product Category Show All Certifications

View Share Link

Certified With	Number of Releases / Versions
▶ Operating Systems (9 Items)	
▶ Application Servers (2 Items)	
▼ Databases (13 Items)	
Advanced Compression	8 Releases (12.1.0.2.0, 12.1.0.1.0, 11.2.0.4.0, 11.2.0.3.0, 11.2.0.2.0, 11.2.0.1.0, 11.1.0.7.0, 11.1.0.6.0)
Advanced Networking Option	9 Releases (12.1.0.2.0, 12.1.0.1.0, 11.2.0.4.0, 11.2.0.3.0, 11.2.0.2.0, 11.2.0.1.0, 11.1.0.7.0, 10.2.0.5.0, 10.2.0.4.0)
Advanced Security	9 Releases (12.1.0.2.0, 12.1.0.1.0, 11.2.0.4.0, 11.2.0.3.0, 11.2.0.2.0, 11.2.0.1.0, 11.1.0.7.0, 10.2.0.5.0, 10.2.0.4.0)
Connection Manager	9 Releases (12.1.0.1.0, 11.2.0.4.0, 11.2.0.3.0, 11.2.0.2.0, 11.2.0.1.0, 11.1.0.7.0, 11.1.0.6.0, 10.2.0.5.0, 10.2.0.4.0)
Data Guard	10 Releases (12.1.0.2.0, 12.1.0.1.0, 11.2.0.4.0, 11.2.0.3.0, 11.2.0.2.0, 11.2.0.1.0, 11.1.0.7.0, 11.1.0.6.0, 10.2.0.5.0, 10.2.0.4.0)
Database In-Memory Option	1 Release (12.1.0.2.0)
Oracle Active Data Guard	5 Releases (12.1.0.2.0, 12.1.0.1.0, 11.2.0.4.0, 11.2.0.3.0, 11.2.0.2.0)
Oracle Database	11 Releases (12.1.0.2.0, 12.1.0.1.0, 11.2.0.4.0, 11.2.0.3.0, 11.2.0.2.0, 11.2.0.1.0, 11.1.0.7.0, 11.1.0.6.0, 10.2.0.5.0, 10.2.0.4.0) and 1 other
Oracle Database Vault	7 Releases (11.2.0.4.0, 11.2.0.3.0, 11.2.0.2.0, 11.2.0.1.0, 11.1.0.7.0, 10.2.0.5.0, 10.2.0.4.0)
Oracle Real Application Clusters	11 Releases (12.1.0.2.0, 12.1.0.1.0, 11.2.0.4.0, 11.2.0.3.0, 11.2.0.2.0, 11.2.0.1.0, 11.1.0.7.0, 11.1.0.6.0, 10.2.0.5.0, 10.2.0.4.0) and 1 other
Transparent Data Encryption	9 Releases (12.1.0.2.0, 12.1.0.1.0, 11.2.0.4.0, 11.2.0.3.0, 11.2.0.2.0, 11.2.0.1.0, 11.1.0.7.0, 10.2.0.5.0, 10.2.0.4.0)
Transportable Database	9 Releases (12.1.0.2.0, 12.1.0.1.0, 11.2.0.4.0, 11.2.0.3.0, 11.2.0.2.0, 11.2.0.1.0, 11.1.0.7.0, 10.2.0.5.0, 10.2.0.4.0)

Database Vault and EBS Documentation

EBS 12.0 and 12.1	MOS Note ID 1091083.1 <i>Integrating Oracle E-Business Suite Release 12 with Oracle Database Vault 11gR2</i>
EBS 11.5.10.2	MOS Note ID 1091086.1 <i>Integrating Oracle E-Business Suite Release 11i with Oracle Database Vault 11gR2</i>
Database Vault	<i>Oracle Database Vault Administrator's Guide 11g Release 2 (11.2)</i>

DV Installation for EBS

- **Verify certification on My Oracle Support**
 - Database Vault is a separate certification for each EBS and database version
- **11.2.0.4 is strongly recommended**
 - Supported and stable

DV Installation for EBS – Database Registration

See section “Registering (Enabling) Oracle Database Vault” of the Oracle Database Vault Administrator’s Guide

1) **May need to enable DBConsole**

- Create a password file if it doesn’t exist

```
orapwd file=$ORACLE_HOME/dbs/orapw<sid>  
password=<SYS password>
```

- Create DBConsole repository

```
emca -config dbcontrol db -repos create
```

2) **Relink to include DV and Label Security**

- Relink ioracle library with DV and Label Security

```
make -f ins_rdbms.mk dv_on lbac_on ioracle
```

3) **Configure DV using Database Configuration Assistant (dbca)**

DV Installation for EBS – Database Registration

Database Configuration Assistant, Step 4 of 5 : Oracle Database Vault Credentials

Specify the Database Vault Owner and password. Optionally, you can create a separate Database Vault Account Manager to provide separation of duties between account management and security policy management.

Database Vault Owner:

Database Vault Owner Password:

Confirm Password:


Create a Separate Account Manager:

Database Vault Account Manager:

Database Vault Account Manager Password:

Confirm Password:

Cancel Help < Back Next >



DV Installation for EBS – EBS Installation

See MOS Note ID 1091086.1 (R12) or 1091083.1 (11i) for detailed instructions on installing DV for EBS

1) **Apply EBS DV patches**

- SQL scripts to create EBS realms – not included with any version of EBS

2) **Perform manual SQL steps and run `fnddbvebs.sql`**

- Need to modify privileges to allow EBS realms to be created
- Creates EBS realms

DV and EBS Limitations

- **Disable DV when applying certain EBS patches**
 - Patches that create database schemas
 - Run `fnddbvpachx` before after patching to disable some DV restrictions
 - Grants `DV_ACCTMGR` to `SYSTEM`
- **Disable DV when upgrading database**
- **Changing database and EBS passwords**
 - `FNDCPASS` must be run by an account with `DV_ACCTMGR` role
 - Use `AFPASSWRD` instead

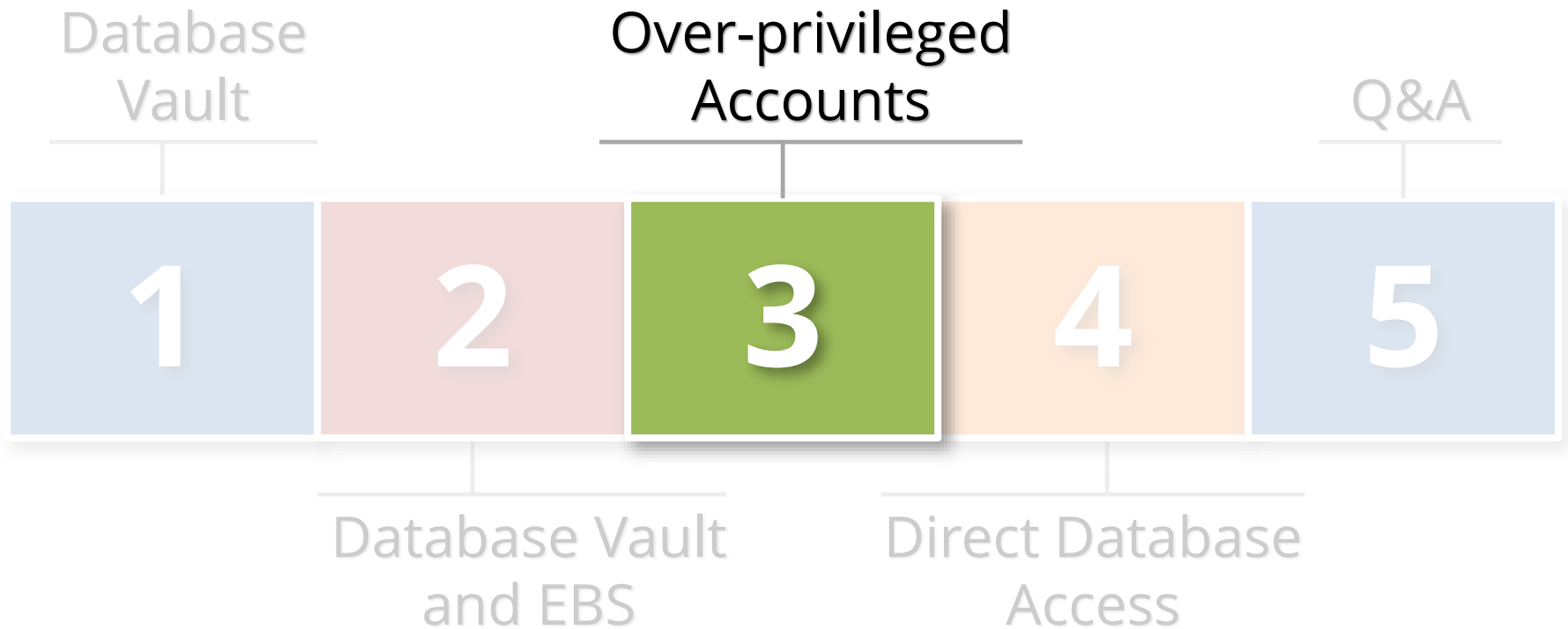
Default Oracle Database Realms

Realm Name	What is Protected?	Who is authorized to access?
Database Vault Account Management	Defines the realm for the administrators who manage and create database accounts and database profiles.	DV_ACCTMGR role
Oracle Data Dictionary	Defines the realm for the Oracle Catalog schemas: SYS, SYSTEM, DBSNMP, OUTLN, etc. This realm also controls the ability to grant system privileges and database administrator roles.	APPS, APPLSYS, SYS, SYSTEM, CTXSYS
Oracle Database Vault	Defines the realm for the Oracle Database Vault schemas (DVSYS, DVF, and LBACSYS), such as configuration and roles information.	Users: DVSYS, LBACSYS Roles: DV_ADMIN, DV_OWNER
Oracle Enterprise Manager	Defines the realm for Oracle Enterprise Manager accounts (SYSMAN and DBSNMP) to access database information.	DBSNMP, SYSMAN, SYSTEM

Default Oracle EBS Realms

Realm Name	What is Protected?	Who is authorized to access?
EBS Realm	All tables in Oracle E-Business Suite Product Schemas	All Oracle E-Business Suite Product Schemas, and APPS, APPLSYS, SYSTEM, CTXSYS
EBS Realm - Applsys Schema	Most tables in the APPLSYS Schema	APPS, APPLSYS, SYSTEM and CTXSYS
EBS Realm - Apps Schema	All objects in the APPS Schema (except the views)	APPS, APPLSYS, SYSTEM, CTXSYS and All product schemas, that uses intermedia indexes
EBS Realm - Applsypub Schema	Objects required for EBS authorization	APPS, APPLSYS, SYSTEM, APPLSYSPUB and CTXSYS
EBS Realm - MSC Schema	Tables in the MSC Schema - except those that require partitions to be exchanged	APPS, APPLSYS, SYSTEM, CTXSYS and MSC
CTXSYS Data Dictionary	Objects in the CTXSYS Schema	All Oracle E-Business Suite 11i Product Schemas and APPS, APPLSYS, SYSTEM

Agenda



Challenge – Over-privileged Database Accounts

Database accounts within Oracle EBS environments are often over-privileged with system privileges such as SELECT ANY TABLE. Frequently, these privileges can not be revoked due to business or technical constraints.

SYS, SYSTEM	<ul style="list-style-type: none">▪ Need to limit access to sensitive as much as possible▪ SYSTEM is used for many EBS maintenance activities such as patching and changing passwords
DBAs (named)	<ul style="list-style-type: none">▪ Need to limit access to sensitive data as much as possible▪ DBA role includes SELECT ANY TABLE, SELECT ANY DICTIONARY, EXECUTE ANY PROCEDURE, etc.
Non-EBS Service Accounts	<ul style="list-style-type: none">▪ Granted excessive privileges like SELECT ANY TABLE, EXECUTE ANY PROCEDURE, or even DBA▪ Unable to restrict privileges due to business constraints
Ad-hoc Users	<ul style="list-style-type: none">▪ Requires read access to many tables, but not necessarily sensitive data like HR▪ Difficult to manage individual grants (35,000+) and SELECT ANY TABLE is just so easy

Solution – Over-privileged Database Accounts

Database Vault can be used to limit privileged accounts access to sensitive data include system privileges like SELECT ANY TABLE. Standard EBS realms provide all or nothing access to EBS data.

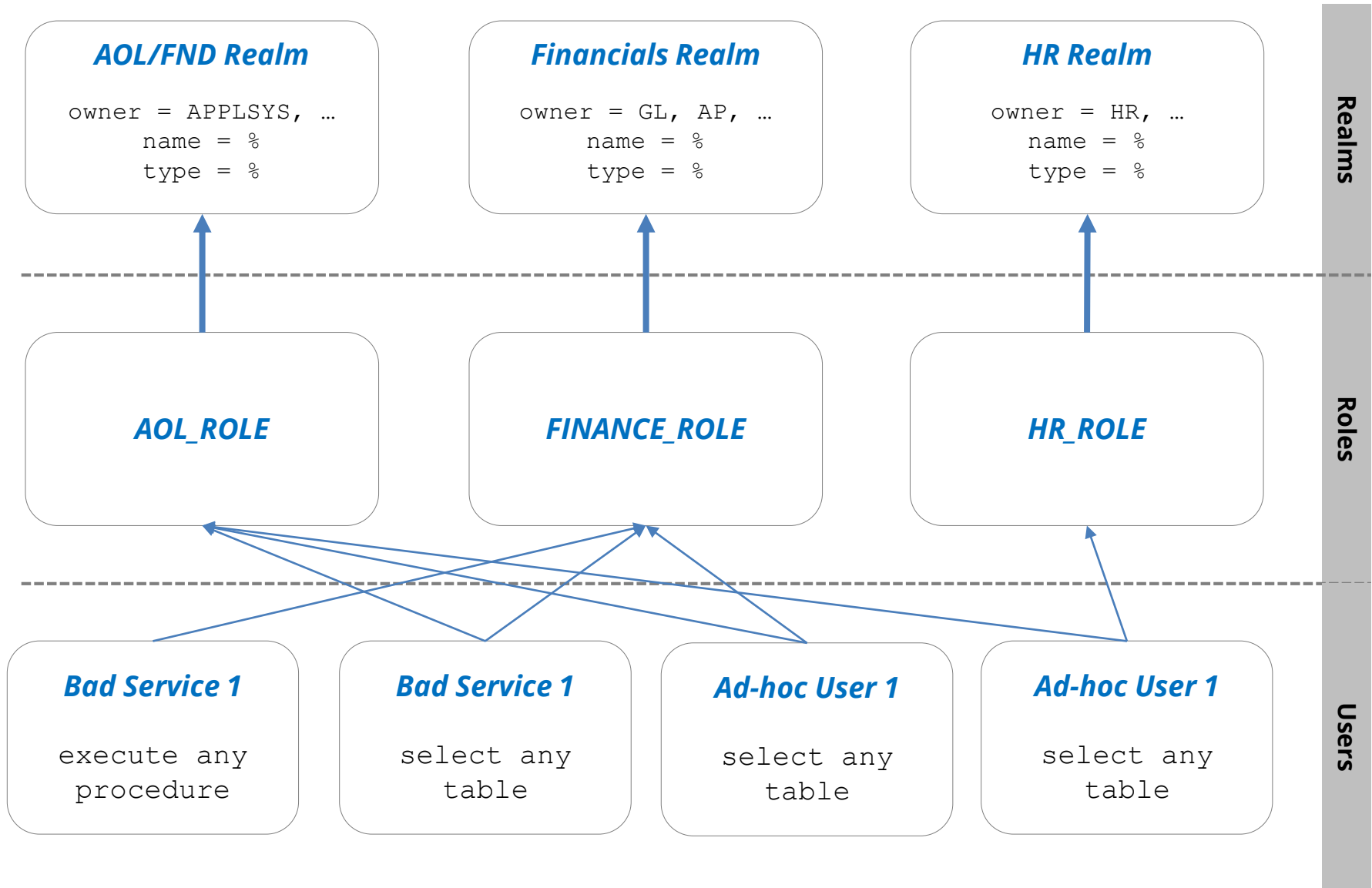
SYS, SYSTEM	<ul style="list-style-type: none">▪ No solution for SYSTEM▪ Standard EBS realms block SYS access to EBS data
DBAs (named)	<ul style="list-style-type: none">▪ Standard EBS realms block DBA access to EBS data▪ May need to add back access to FND tables
Non-EBS Service Accounts	<ul style="list-style-type: none">▪ Accounts should be least privileged whenever possible▪ Need to create custom realms to allow access to limited EBS data if account is over-privileged
Ad-hoc Users	<ul style="list-style-type: none">▪ Accounts should be least privileged whenever possible▪ Need to create custom realms to allow access to limited EBS data if account is over-privileged

Solution – Over-privileged Database Accounts

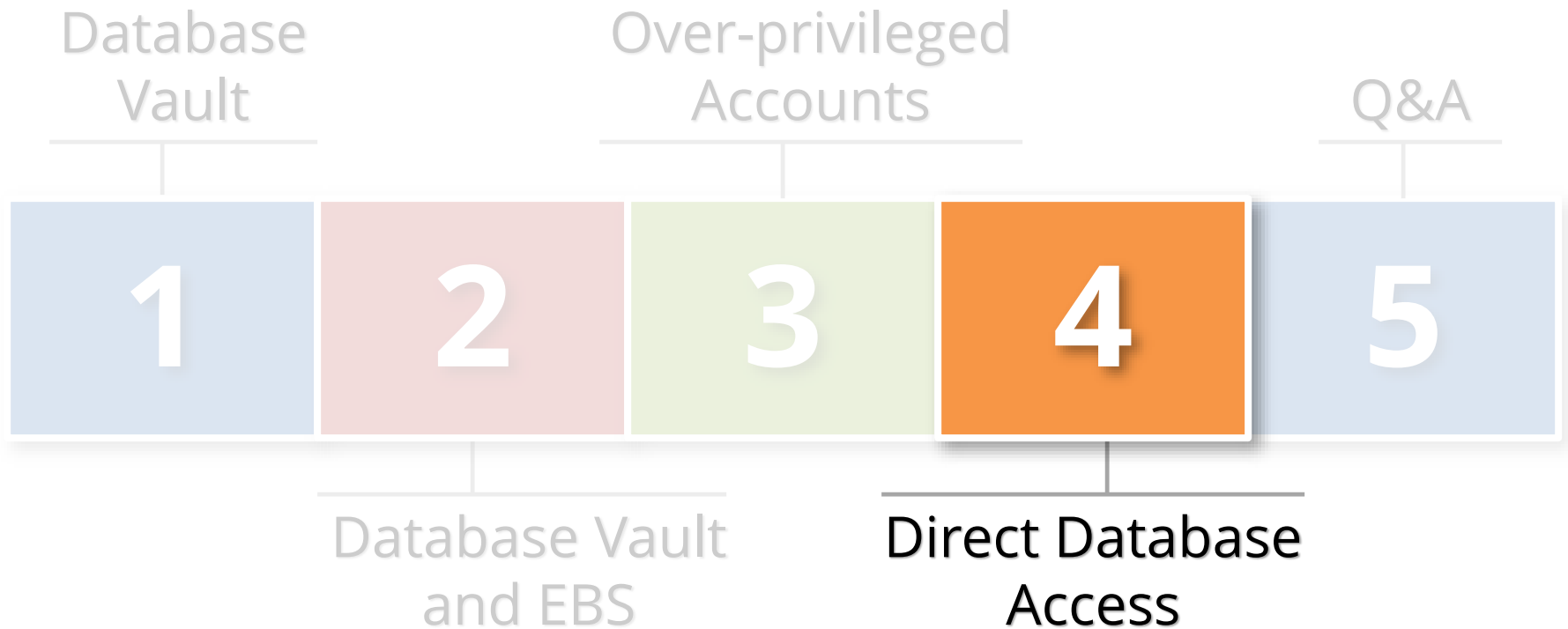
- Realms should be restricting to schemas, not individual objects when possible

Setting	Value	Notes
object_owner	HR	<ul style="list-style-type: none">Schema name
object_name	%	<ul style="list-style-type: none">% for all or a specific object, no wildcards such as "per_%"
object_type	%	<ul style="list-style-type: none">All objects or a specific object such as TABLE, VIEW, etc.

Solution – Over-privileged Database Accounts



Agenda



Challenge – Direct Database Access

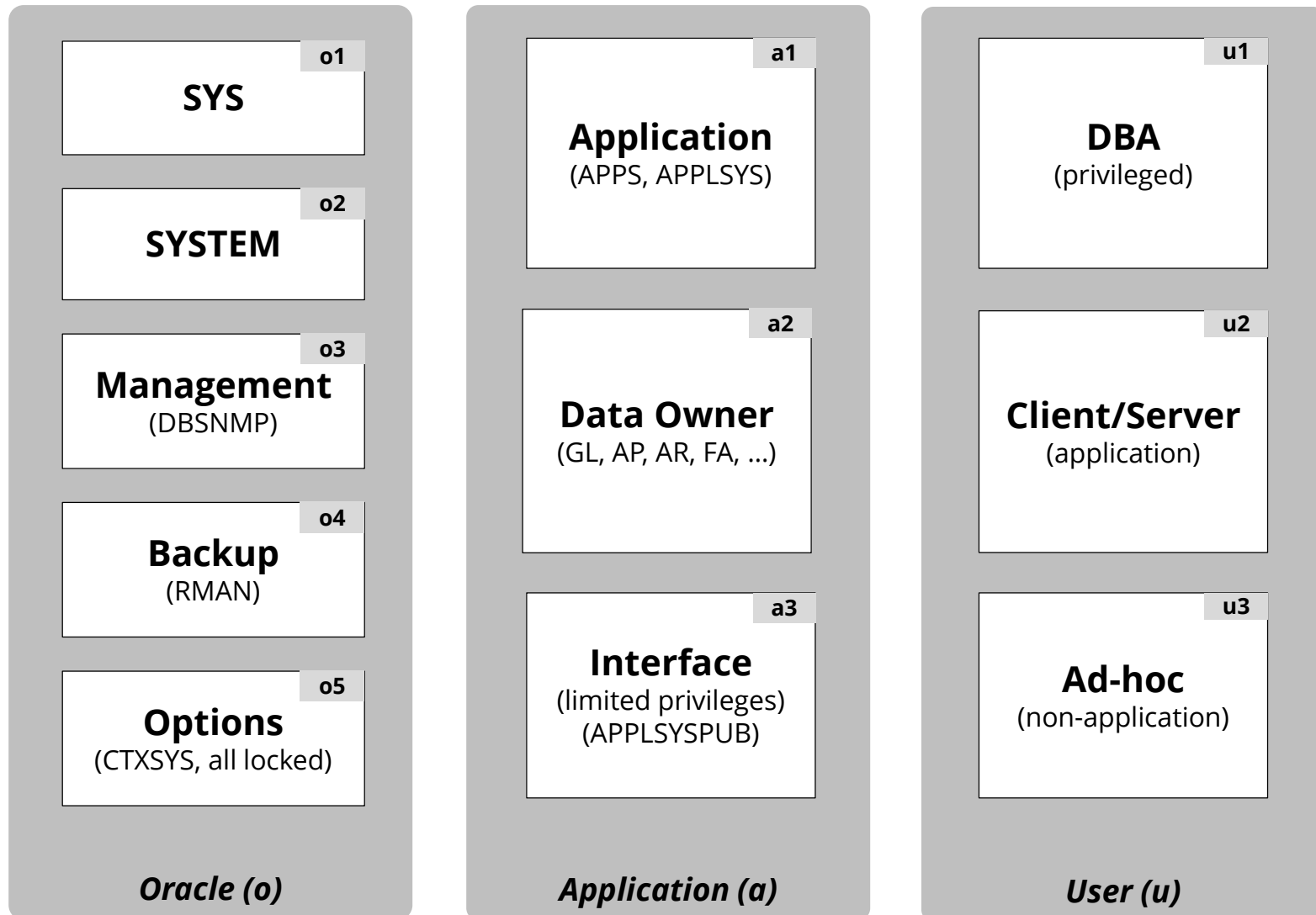
Direct database access is a significant risk in an Oracle EBS environment. There is many different types of database access required including the application, interfaces, management tools, DBAs, and ad-hoc users.

- **Usually impractical to restrict access purely based on network controls or IP addresses**
 - DBA and ad-hoc users a challenge
- **Limiting and restricting direct database can reduce risk of attacks and privilege escalation**
 - Any user with direct database access can exploit unpatched security vulnerabilities in public packages

Solution – Direct Database Access

- **Use DV CONNECT command rule and rule set to block access**
 - Use IP address, program and OS user factors per type of database account
- **Focus on key highly privileged, generic accounts such as APPS and SYSTEM**
- **For interfaces, limit interfaces and customizations to a specific IP addresses if possible**

Solution – Direct Database Access

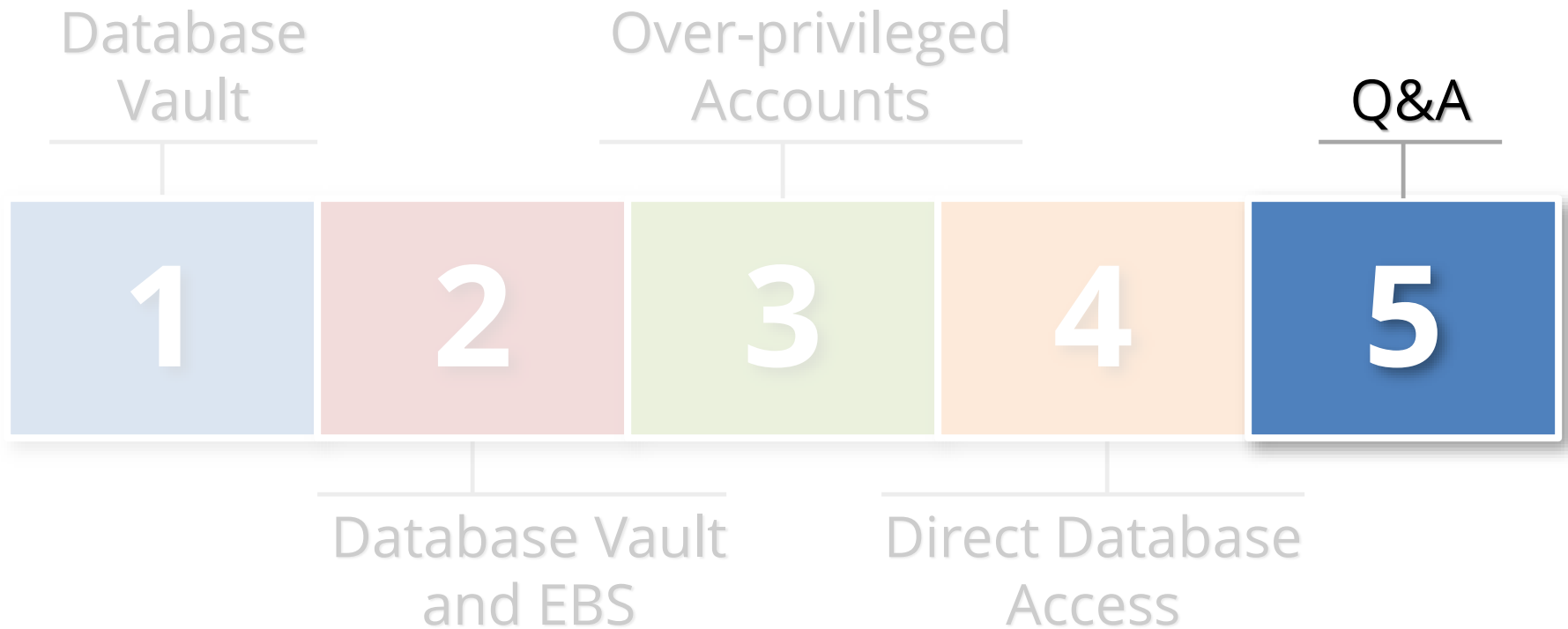


Solution – Direct Database Access (Example)

	IP Address	Program¹	OS User¹
o1 - SYS	database server	unlimited	oracle
o2 - SYSTEM	EBS server	unlimited	oracle/applmgr
o3 - Management	OEM server	unlimited	oracle
o4 - Backup	backup server	unlimited	oracle
o5 - Options	none	none	none
a1 - Interactive	EBS server	unlimited	oracle/applmgr
a2 - Data Owner	EBS server	unlimited	oracle/applmgr
a3 - Interface	per interface	per interface	per interface
u1 - DBA	EBS server & jump	unlimited	unlimited
u2 - Client/Server	none	none	none
u3 - Ad-hoc	unlimited	approved list	unlimited

¹Program and OS user may be spoofed by the client and are not fully reliable.

Agenda



Contact Information

Stephen Kost
Chief Technology Officer
Integrigy Corporation

web: www.integrigy.com

e-mail: info@integrigy.com

blog: integrigy.com/oracle-security-blog

youtube: youtube.com/integrigy