



Oracle E-Business Suite Security for Auditors

December 17, 2020

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy

ERP Applications

Oracle E-Business Suite
and PeopleSoft

**INTEGRIGY**

Databases

Oracle, Microsoft SQL Server,
DB2, Sybase, MySQL, NoSQL

Products

AppSentry

ERP Application and Database
Security Auditing Tool

*Validates
and Audits
Security*

AppDefend

Enterprise Application Firewall
for Oracle E-Business Suite
and PeopleSoft

*Protects
Oracle EBS
& PeopleSoft*

Services

*Verify
Security*

Security Assessments

ERP, Database, Sensitive Data, Pen Testing

*Ensure
Compliance*

Compliance Assistance

SOX, PCI, HIPAA, GLBA

*Build
Security*

Security Design Services

Auditing, Encryption, DMZ

Integrigy Research Team

ERP Application and Database Security Research

ORACLE
Gold Partner

Agenda

1

Database and Application Account Risks

2

Sensitive Data Risks

3

Auditing and Logging Gaps

4

Change Management Challenges and Risks

5

Q & A

Agenda

1

Database and Application Account Risks

2

Sensitive Data Risks

3

Auditing and Logging Gaps

4

Change Management Challenges and Risks

5

Q & A

Oracle EBS Direct Database Access by Users

- **Database access is a key risk**
 - Look for accounts like **APPS_RO**, HR_READ, etc.
 - Read only accounts often created with read access to all data
- **Access to sensitive data by generic accounts**
 - Granularity of database privileges is difficult in the Oracle EBS database
 - SELECT ANY TABLE** used instead of direct table grants
 - Complexity of data model – 75,000 tables and views
 - Number of tables/views and continuous development make it difficult to create limited privilege database accounts
 - Must use individual database accounts with roles limiting access to data along with other security measures

Default Database Passwords

- **Oracle E-Business Suite database is delivered with up to 300 database accounts**
 - Default passwords (GL = GL, AP = AP)
 - Active
 - Significant privileges
- **Database accounts are often created with default or weak passwords**
 - Standard Oracle accounts (DBSNMP, CTXSYS, etc.) until Oracle 12c created with default passwords by default
 - Custom accounts for interfaces often created with weak passwords
 - Named users frequently assigned passwords like WELCOME1

Default Database Passwords Risk

- Risk of a database account with a default password is based on how well-known the account is –
 1. **Standard Oracle Database accounts (DBSNMP, etc.)**
 2. Oracle EBS standard account names (APPLSYS, GL, AP, AR, etc.)
 3. Third-party software (OEM, Vertex, etc.)
 4. Custom database accounts (organizational specific)

- **An attacker will –**
 - Scan the internal network for Oracle Databases
 - Use tools like nmap to test for default passwords
 - Most tools have between 250 to 1,500 known Oracle database accounts and passwords

If a database is compromised, this is usually the root cause

Default Oracle Password Statistics

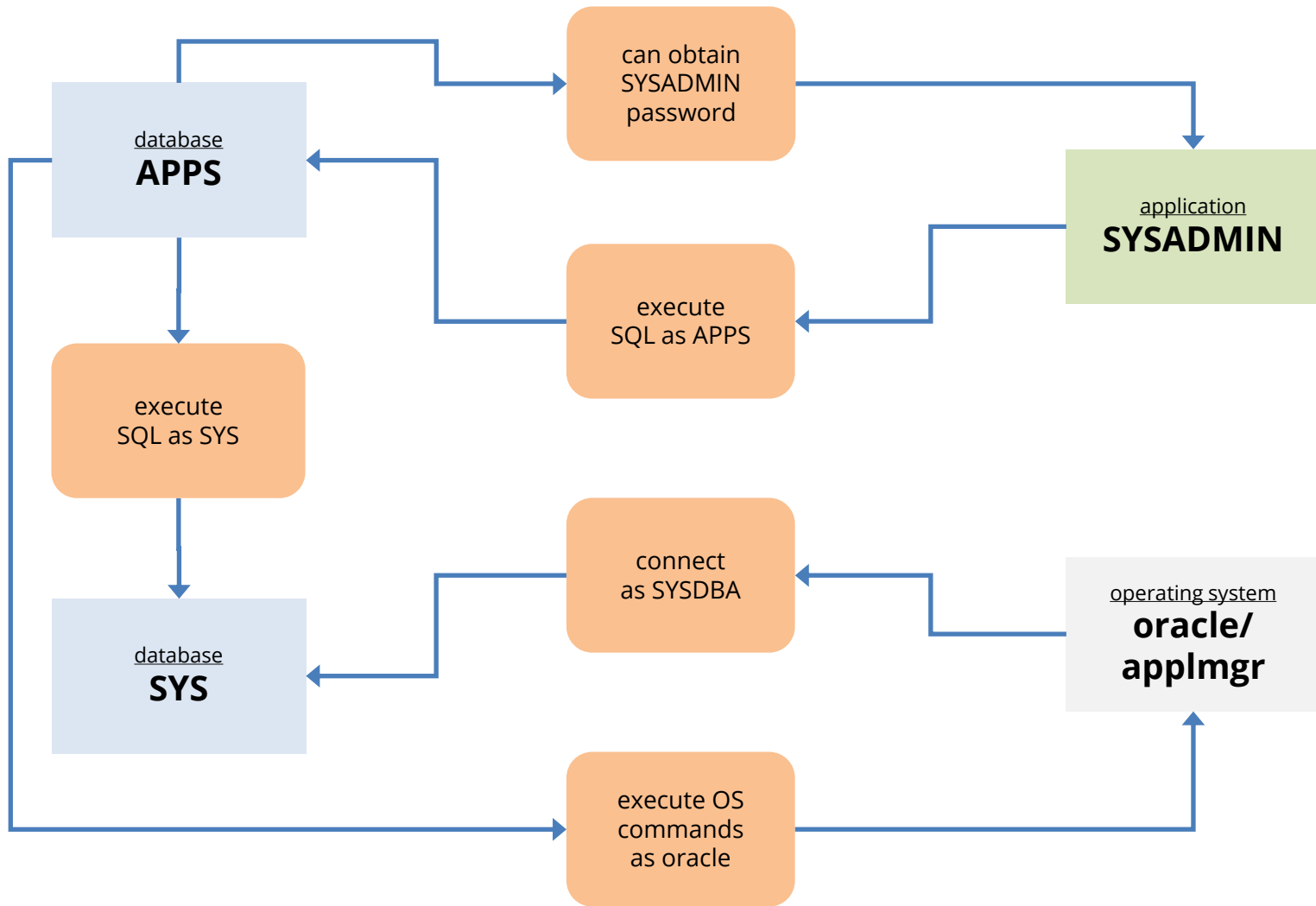
Database Account	Default Password	Exists in Database %	Default Password %
SYS	CHANGE_ON_INSTALL	100%	3%
SYSTEM	MANAGER	100%	4%
DBSNMP	DBSNMP	99%	52%
OUTLN	OUTLN	98%	43%
MDSYS	MDSYS	77%	18%
ORDPLUGINS	ORDPLUGINS	77%	16%
ORDSYS	ORDSYS	77%	16%
XDB	CHANGE_ON_INSTALL	75%	15%
DIP	DIP	63%	19%
WMSYS	WMSYS	63%	12%
CTXSYS	CTXSYS	54%	32%

* Sample of 120 large ERP production databases

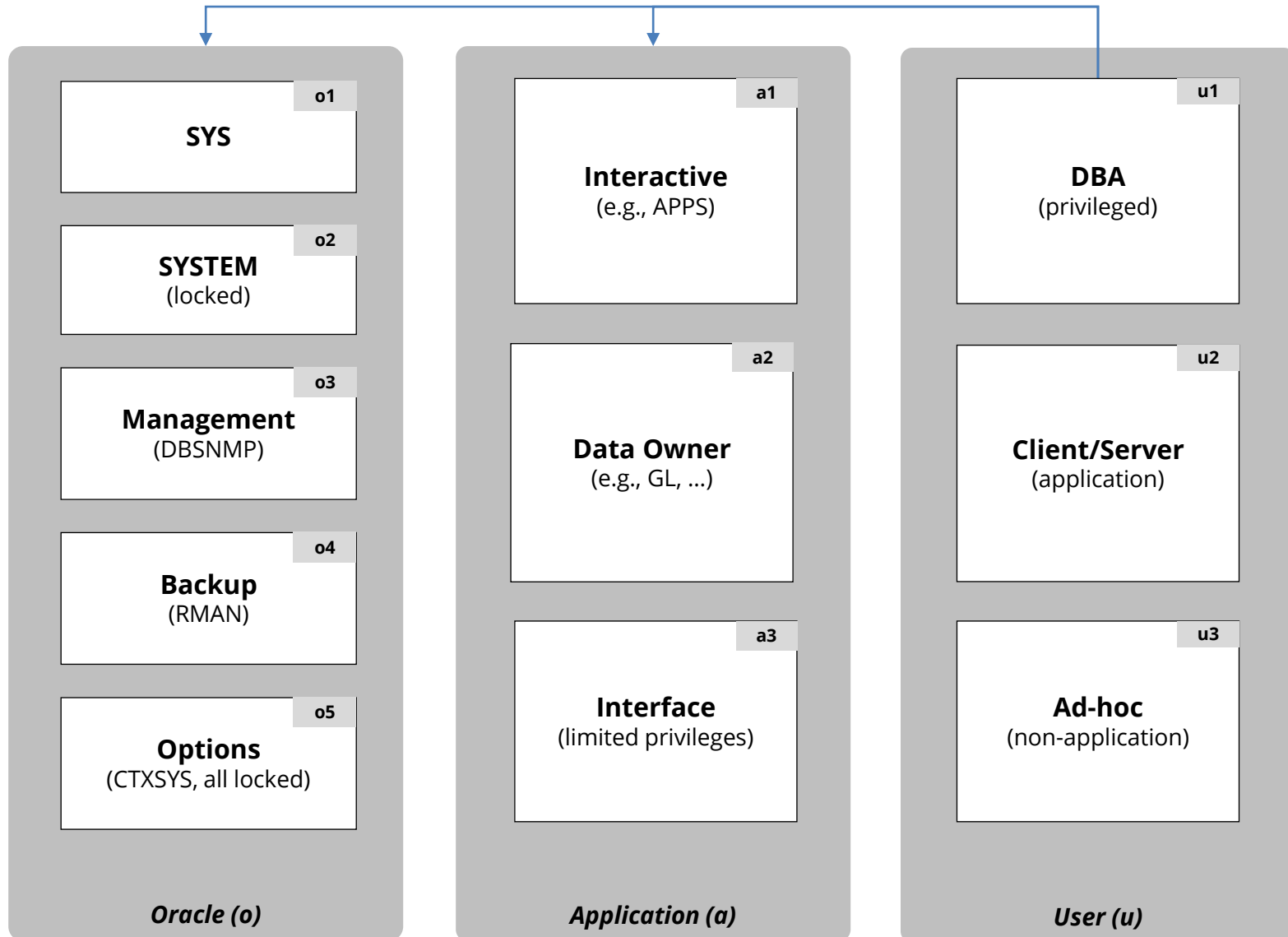
Oracle EBS Generic Privileged Accounts

<p>Oracle E-Business Suite</p>	<p><u>SYSADMIN</u> <i>seeded application accounts</i></p>
<p>Oracle Database</p>	<p><u>APPS, APPLSYS</u> <u>SYS, SYSTEM</u> <i>Oracle EBS schemas (GL, AP, ...)</i></p>
<p>Operating System <i>(Unix and Linux)</i></p>	<p><u>root</u> oracle, applmgr</p>

Generic Privileged Account Inter-Dependency



Database Account Definition (Oracle)



Database Access and Privilege Analysis (Example)

Type of Account	Access	Privileges	Auditing
o1 - SYS	How is account controlled	Fixed - highly privileged	Requires SYS operations auditing
o2 - SYSTEM	How is account controlled	Fixed - highly privileged	Audit privileged actions
o3 - Management	How is account controlled	Review privileges	Access auditing
o4 - Backup	How is account controlled	Fixed - highly privileged	Access auditing
o5 - Options	Must be disabled if possible	Fixed	Access auditing
a1 - Interactive (APPS)	How is account controlled	Fixed by application - privileged	Access auditing
a2 - Data Owner (GL, ...)	How is account controlled	Fixed by application, review custom and 3 rd party	Access auditing
a3 - Interface	How is account controlled	Review - limited privileges only	Access auditing
u1 - DBA	Access management review	Review privileges	Determine auditing required
u2 - Client/Server	Access management review	Review privileges	Determine auditing required
u3 - Ad-hoc	Access management review	Review privileges	Determine auditing required

Database Access Management

Provisioning (P)

- P1 - Identity & privilege request
- P2 - Request approval
- P3 - Identity creation
- P4 - Privilege assignment
- P5 - Communication



Authentication & Authorization (A)

- A1 - Identity authentication
- A2 - Password controls
- A3 - Privilege determination
- A4 - Identity & privilege validation
- A5 - Segregation of Duties



Administration (M)

- M1 - Password changes
- M2 - Password resets
- M3 - Account locking
- M4 - Account expiration
- M5 - Password expiration



De-Provisioning (D)

- D1 - Revocation notification
- D2 - Revocation request
- D3 - Identity revocation
- D4 - Privilege revocation

Database Access Management Lifecycle

Database Access Management (Example)

Type of Account	Provisioning (P)	Authentication & Authorization (A)	Administration (M)	De-Provisioning (D)
o1 - SYS	P1: Installed by default per database security standards P4: Privileges pre-defined	A1: Local authentication A2: Profile ORA_DEFAULT A3: Privileges pre-defined A4: Review of all changes A5: No SOD review	M1: Password Vault M3: No; M4: No; M5: 360d	D1: Installed by default D2: Per database security standards D3: Locked or removed per database security standards D4: Privileges pre-defined
o2 - SYSTEM			M4: Locked	
o3 - Management			M1: Password Vault M3: 6; M4: Yes; M5: 360d	
o4 - Backup			M1: Password Vault M3: 6; M4: Yes; M5: 360d	
o5 - Options			M4: Locked	
a1 - Interactive (APPS)	P1: Standard IT request workflow P2: DBA and IT Security review P3: DBA created P4: Privileges defined by app	A1: Local authentication A2: Profile APPLICATION A3: Privileges defined by app – roles when possible A4: Review of all changes – sample tickets A5: No SOD review	M1: Password Vault M3: No; M4: No; M5: 360d	D2: Standard IT request workflow D3: Locked, but never drop per standards D4: Standard IT request workflow
a2 - Data Owner (GL,...)			M4: Locked	
a3 - Interface			M1: Password Vault M3: No; M4: No; M5: 360d	
u1 - DBA	P1: Standard user request workflow P2: User manager approval/review P3: Security admin created P4: Privileges via local DB roles	A1: Active Directory authentication A2: AD password controls A3: Privileges via local DB roles A4: Quarterly manager review A5: Quarterly manager review	M1 – M5: AD controlled	D1: AD controlled D2: Standard user request workflow or per quarterly manager review process D3: Drop after 180 when locked D4: Request via quarterly manager review process
u2 - Client/Server				
u3 - Ad-hoc				

Agenda

1

Database and Application Account Risks

2

Sensitive Data Risks

3

Auditing and Logging Gaps

4

Change Management Challenges and Risks

5

Q & A

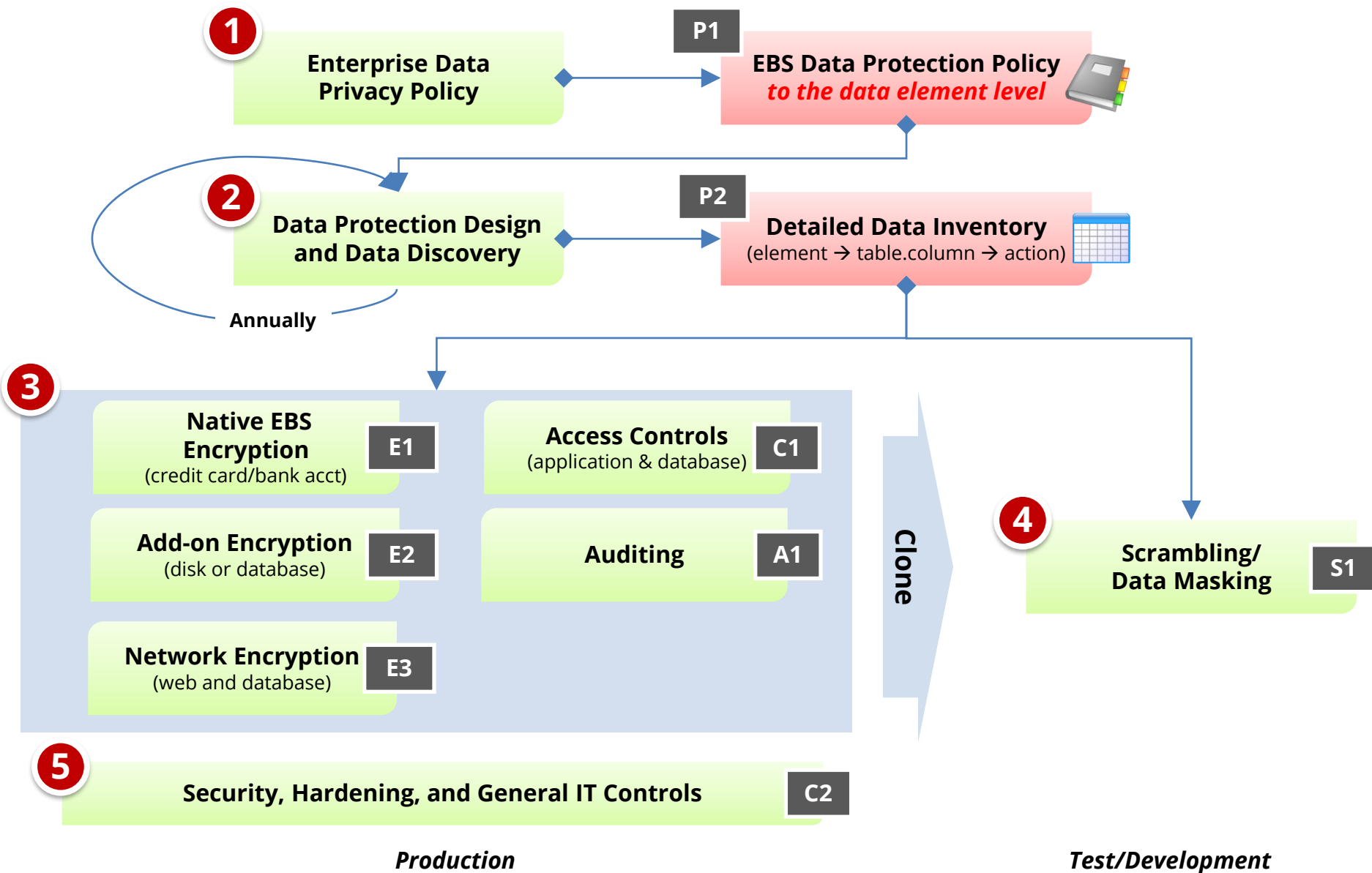
Where is Sensitive Data in Oracle E-Business Suite?

Social Security Number (National Identifier) (Tax ID) (1099)	per_all_people_f hr_h2pi_employees ben_reporting ap_suppliers ap_suppliers_int po_vendors_obs
Bank Account Number	ap_checks_all ap_invoice_payments_all ap_selected_invoice_checks_all
Credit Card Data	iby_security_segments (encrypted) ap_bank_accounts_all oe_order_headers_all aso_payments oks_k_headers_* oks_k_lines_* iby_trxn_summaries_all iby_credit_card
Electronic Protected Health Information (ePHI)	Order Management Accounts Receivables Human Resources

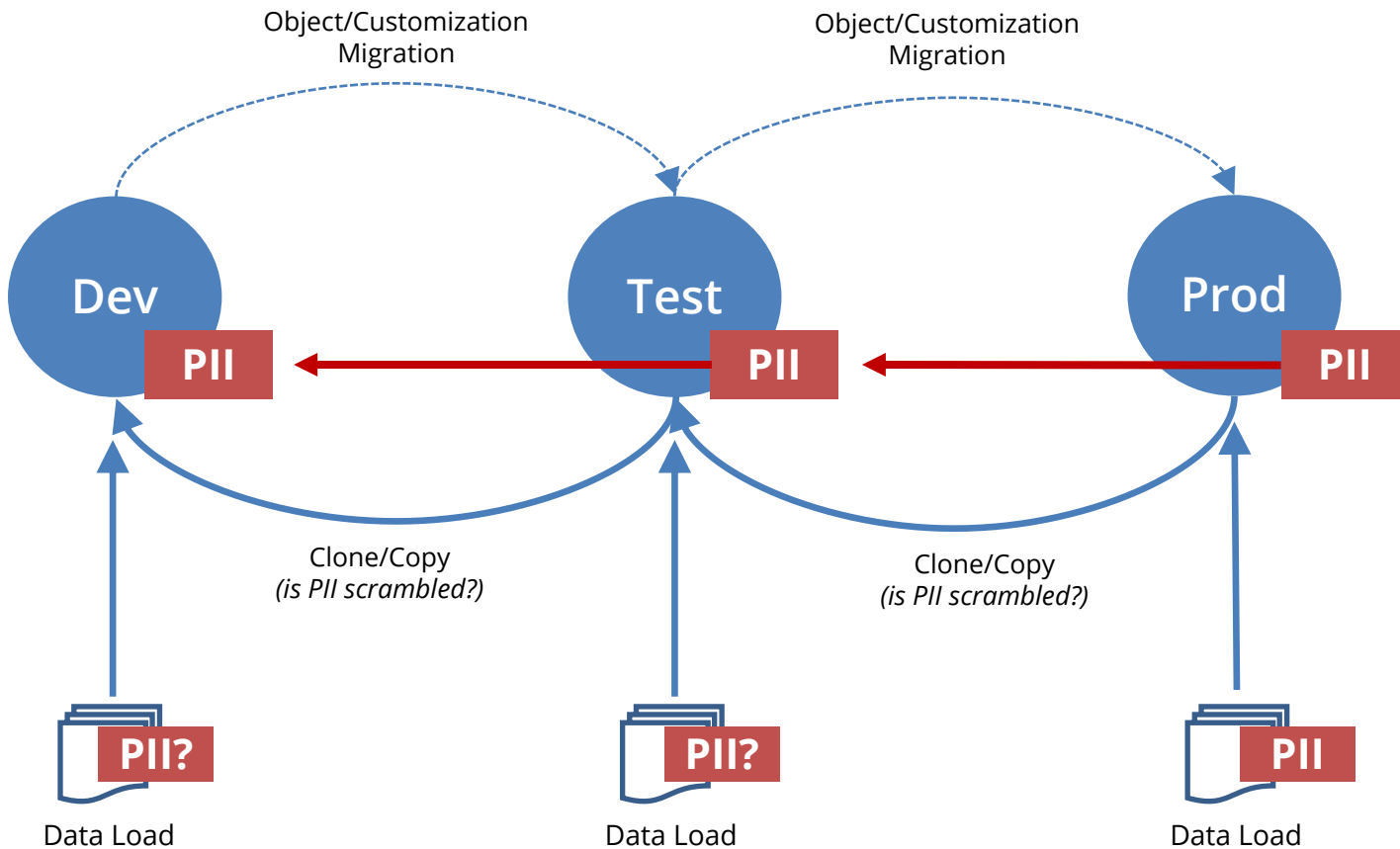
Where else might be Sensitive Data? (Oracle EBS)

- **Custom tables**
 - Customizations may be used to store or process sensitive data
 - **“Maintenance tables”**
 - DBA copies tables to make backup prior to direct SQL update
 - hr.per_all_people_f_DEC122019
 - **Interface tables**
 - Credit card numbers are often accepted in external applications and sent to Oracle EBS or processed using XML Gateway
 - **Oracle EBS Flexfields**
 - It happens – very hard to find (e.g., SEGMENT1)
-
- **Interface files**
 - Flat files used for interfaces or batch processing
 - **Log files**
 - Log files generated by the application (e.g., Oracle Payments)

Integrigy Sensitive Data Protection Process



EBS Cloning – Test and Development Sensitive Data Risk



Agenda

1

Database and Application Account Risks

2

Sensitive Data Risks

3

Auditing and Logging Gaps

4

Change Management Challenges and Risks

5

Q & A


Oracle EBS Who Columns

Almost all Oracle EBS tables have “Who Columns”, which capture creation and last update information. **Changes between creation and last update are not captured.** In Forms, use *About this Record*. In HTML, enable FND Diagnostics and use *About this Page*.

APPLSYS.FND_USER

USER_ID	CREATION_DATE	CREATED_BY	LAST_UPDATE_LOGIN	LAST_UPDATE_DATE	LAST_UPDATED_BY
1111	01-JAN-2014	123	341244	13-FEB-2014	222

Date and time row was created	User ID from FND_USER	Login ID from FND_LOGINS when updated (often purged)	Date and time row was last updated	User ID from FND_USER
-------------------------------	------------------------------	---	------------------------------------	------------------------------



Oracle EBS Auditing and Logging Methods

EBS Sign-on Audit	<ul style="list-style-type: none">▪ Captures logins, responsibility selection, and form usage.
EBS Page Access Tracking (PAT)	<ul style="list-style-type: none">▪ Tracks Oracle Applications Framework (OAF) page usage.
EBS Audit Trails	<ul style="list-style-type: none">▪ EBS managed triggers on defined tables to capture changes to specific columns.
EBS Module Specific	<ul style="list-style-type: none">▪ Certain EBS modules capture changes or information on activity. One example is HCM Date Tracking.
Snapshot/Trigger	<ul style="list-style-type: none">▪ Third-party tools to snapshot data or perform trigger-based auditing. Trigger-based is preferred as it captures all changed, however, more expensive to implement and maintain.▪ Trigger = Caosys CS*Audit, Fastpath, SafePaas, Oracle GRC▪ Snapshot = Integrigy AppSentry, ConfigSnapshot

Oracle EBS Other Logging

Unsuccessful Logins

EBS Report

- Signon Audit Unsuccessful Logins

EBS Tables

- APPLSYS.FND_UNSUCCESSFUL_LOGINS
- ICX.ICX_FAILURES

Concurrent Requests

EBS Report

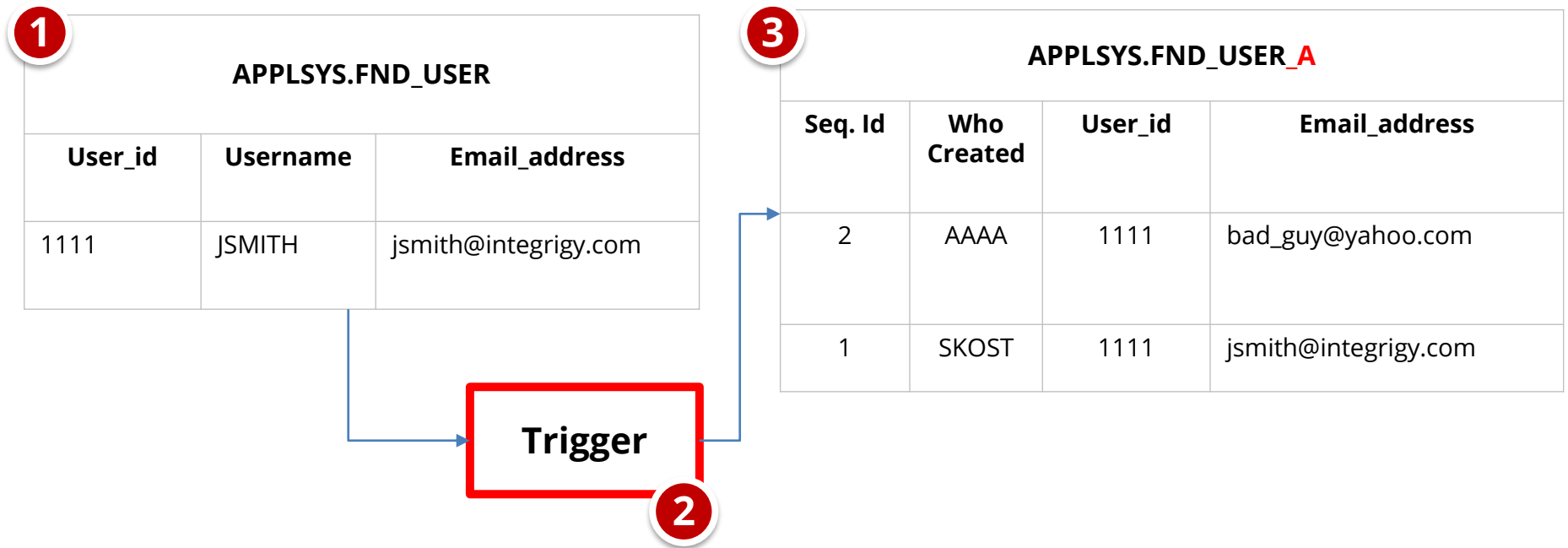
- Signon Audit Concurrent Requests

EBS Tables

- APPLSYS.FND_CONCURRENT_REQUESTS

Oracle EBS Audit Trails

EBS Audit Trails functionality stores row changes to EBS tables in **shadow tables** using database triggers. Only tracks insert, update, and deletes to tables defined in Oracle EBS. See MOS Note ID 60828.1 for more information. Audit Trails must be configured individually for each table to be audited to the column level.



Minimum Set of Oracle EBS Audit Trails Tables

Audit Trail tables

- **EBS security** – users, responsibilities, menus, functions, ...
- **EBS configuration** – system profile options
- **EBS customizations** – forms, executables, concurrent programs, alerts
- **EBS module configuration** – flex fields, data groups, ...
- **EBS Audit Trails configuration**

Inclusion criteria

- High security, compliance, or change impact
- Low volume
- Limited master data tables such as vendor bank accounts
- No transactional tables

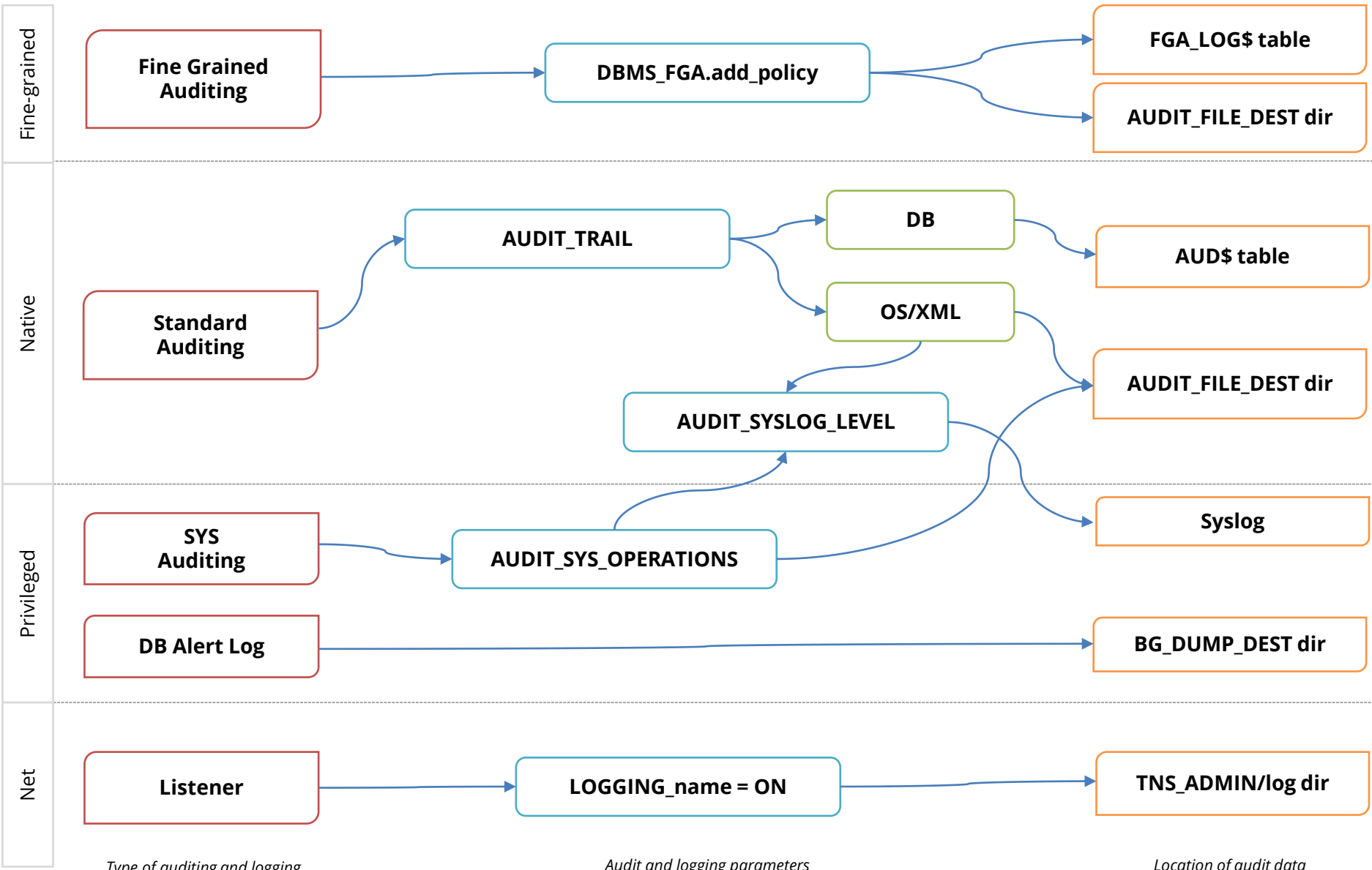
Framework Events	Oracle EBS Audit Trail Tables
E4 - Modify authentication mechanisms	FND_PROFILE_OPTIONS (also E12, E14) FND_PROFILE_OPTION_VALUES (also E12, E14)
E5 - Create user account E6 - Modify user account	FND_USER
E7 - Create role E8 - Modify role	FND_RESPONSIBILITY
E9 - Grant/revoke user privileges	WF_LOCAL_USER_ROLES WF_USER_ROLE_ASSIGNMENTS
E10 - Grant/revoke role privileges	FND_MENU FND_MENU_ENTRIES FND_REQUEST_GROUPS FND_REQUEST_GROUP_UNITS FND_RESP_FUNCTIONS FND_GRANTS FND_DATA_GROUPS FND_DATA_GROUP_UNITS FND_FLEX_VALIDATION
E11 - Privileged commands	FND_ORACLE_USERID
E12 - Modify audit and logging	ALR_ALERTS FND_AUDIT_GROUPS FND_AUDIT_SCHEMAS FND_AUDIT_TABLES FND_AUDIT_COLUMNS
E13 - Objects: Create object Modify object Delete object	FND_CONCURRENT_PROGRAMS FND_EXECUTABLES FND_FORM FND_FORM_FUNCTIONS

Oracle EBS Audit Trails – Application Modules

Category	Form / Function
Application Controls – partial list	Journal Sources (GL), Journal Authorization Limits (GL), Approval Groups (PO), Adjustment Approval Limits (AR), Receivables Activities (AR), OM Holds (OM), Line Types (PO), Document Types (PO), Approval Groups (PO), Approval Group Assignments (PO), Approval Group Hierarchies (PO), Tolerances, Item Master Setups, Item Categories
Master Data	Banks / Bank Accounts, Supplier Master, Customer Master, Item Master
Fraud Related	Suppliers, Remit-To Addresses, Locations, Bank Accounts, Credit Cards
Foundational	Profile Option Values, Descriptive Flexfields, Descriptive Flexfield Segments, Key Flexfields, Key Flexfield Segments, Value Set Changes, Code Combinations, Flexfield Security Rules, Cross-Validation Rules, Business Groups, Organizations, Legal Entity Configurator, Applications, Document Sequences, Rollup Groups, Shorthand Aliases, Territories, Concurrent Managers

This is a partial list for demonstration purposes only

Oracle Database 11gR2 Auditing and Logging



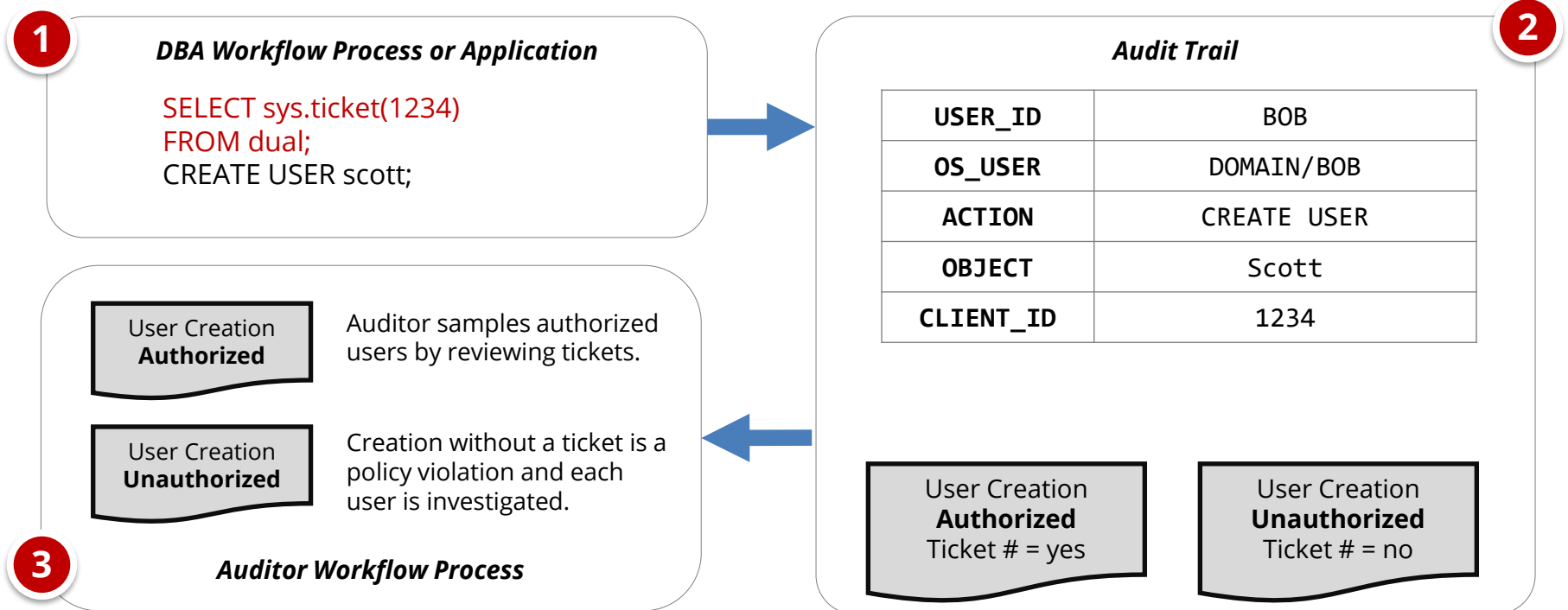
Recommended Database Logging – Security Events

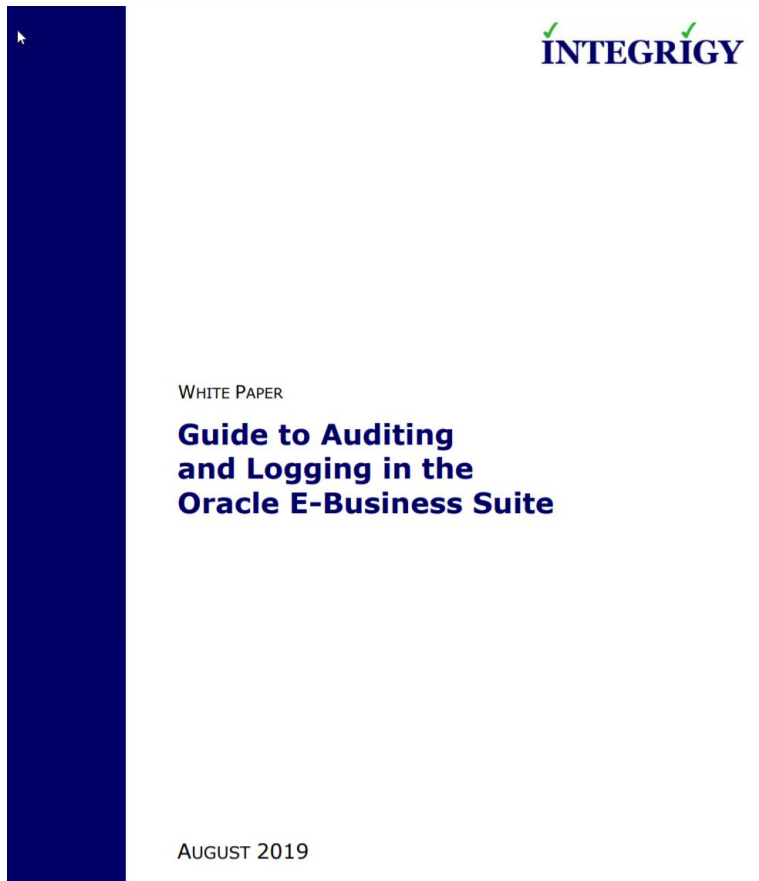
Framework Event	Object	Oracle Audit Statement	Resulting Audited SQL Statements
E1, E2, E3	Session	session	Database logons and failed logons
E5, E6	Users	user	create/alter/drop user
E7, E8	Roles	role	create/alter/drop role
E13	Database Links Public Database Links	database link public database link	create/drop database link create/drop public database link drop public database link
E11	System	alter system	alter system
E14	Database	alter database	alter database
E9, E10	Grants (system privileges and roles)	system grant	grant revoke
E4	Profiles	profile	create/alter/drop profile
E11, E14	SYSDBA and SYSOPER	sysdba sysoper	All SQL executed with sysdba and sysoper privileges

See Integrity Auditing and Logging Framework whitepaper for complete database auditing recommendations

Change Ticket Tracking – Create User Example

Capture ticket numbers and other information for a database session based on special SQL executed by database users or applications.





The Integrigy Framework for Auditing and Logging in Oracle E-Business Suite is available for download from our website.

www.integrigy.com/security-resources

Integrigy Framework Events

The foundation of the framework is a set of key security events and actions derived from and mapped to compliance and security requirements that are critical for all organizations.

<i>E1 - Login</i>	<i>E8 - Modify role</i>
<i>E2 - Logoff</i>	<i>E9 - Grant/revoke user privileges</i>
<i>E3 - Unsuccessful login</i>	<i>E10 - Grant/revoke role privileges</i>
<i>E4 - Modify auth mechanisms</i>	<i>E11 - Privileged commands</i>
<i>E5 - Create user account</i>	<i>E12 - Modify audit and logging</i>
<i>E6 - Modify user account</i>	<i>E13 - Create, Modify or Delete object</i>
<i>E7 - Create role</i>	<i>E14 - Modify configuration settings</i>

AppSentry Insights

AppSentry Insights **centralizes audit and log data** for the Oracle E-Business Suite, Oracle Database, and application server. All audit data locations are automatically found and dynamically adjusts to changes in the application and database. Auditing configuration is continually verified, and recommendations are provided for any missing audits or gaps in auditing according to policy.

AppSentry Insights Features

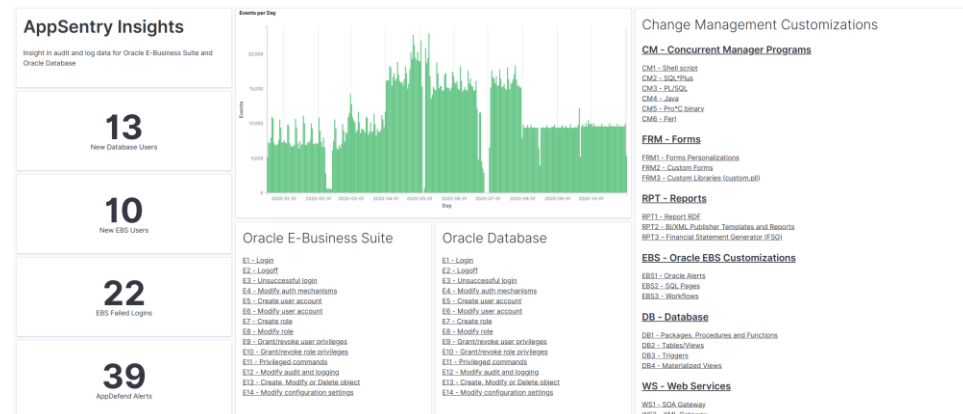
- One-step configuration – a database account
- Pre-configured dashboards, reports, and alerts optimized for Oracle EBS and Oracle Database
- Automatic discovery of Oracle EBS audit and log data locations
- Validation of organizational policy and best practice audit and log configuration

AppSentry Insights Benefits

- Improved security and compliance visibility
- Protection, retention, reporting, and alerting of Oracle EBS and Oracle Database audit data
- Audit data analytics and ad-hoc analysis

AppSentry Insights Scope

- Oracle E-Business Suite
- Oracle Database
- Oracle WebLogic (with AppDefend)



Agenda

1

Database and Application Account Risks

2

Sensitive Data Risks

3

Auditing and Logging Gaps

4

Change Management Challenges and Risks

5

Q & A

Changes in Oracle E-Business Suite

- **Oracle EBS changes can be classified as one of five unique types all with different risks and processes –**
 - Application security changes
 - Application changes and patches
 - Database security changes
 - Database changes and patches
 - Customizations and development changes

- **There is no master list of types of EBS changes as it depends on the following –**
 - Oracle EBS installed modules and application usage
 - Organizational change management policies and procedures
 - Type of EBS customizations and development

Oracle EBS Application Security Changes

- **User Security**

- Users
- Roles and role assignments
- Responsibilities and responsibility assignments

- **Function Security**

- Menus, submenus, and menu entries
- Request groups and request group units
- Functions and responsibility functions
- Grants
- Data groups and data units

Oracle EBS Application Changes – Examples

Category	Form / Function
Application Controls	Journal Sources (GL), Journal Authorization Limits (GL), Approval Groups (PO), Adjustment Approval Limits (AR), Receivables Activities (AR), OM Holds (OM), Line Types (PO), Document Types (PO), Approval Groups (PO), Approval Group Assignments (PO), Approval Group Hierarchies (PO), Tolerances, Item Master Setups, Item Categories
Foundational	Profile Option Values, Descriptive Flexfields, Descriptive Flexfield Segments, Key Flexfields, Key Flexfield Segments, Value Set Changes, Code Combinations, Flexfield Security Rules, Cross-Validation Rules, Business Groups, Organizations, Legal Entity Configurator, Applications, Document Sequences, Rollup Groups, Shorthand Aliases, Territories, Concurrent Managers

Oracle EBS Database Security Changes

- **Database users**
 - Creation of users
 - Dropping of users
 - Alerting of users (password, profile, default tablespace, etc.)
- **Profiles (password and resource controls)**
- **Roles**
- **Role and system privileges**
 - Granting to users and roles
 - Revoking from users and roles
- **Table and object privileges**
 - Granting and revoking of select, insert, update, delete, execute, etc. privileges
- **Auditing**
 - Audit, noaudit
 - Fine-grained auditing (FGA) policies, Unified auditing policies, etc.
 - Purging of auditing tables
- **Oracle Database Vault configuration and policies**

Change Management Challenges

- Many changes are made by generic, privileged accounts and difficult to determine the named DBA
- Database and application patches may result in database security changes

Oracle EBS Database Changes

- Oracle Database patches
- Initialization parameters
- Packages, procedures and functions (PL/SQL code objects)
- Tables/Views/Indexes
- Triggers
- Materialized Views
- Database storage (tablespaces, data files, etc.)
- Other database objects (sequences, types, etc.)

Change Management Challenges

- Some database changes are made by automated application processes as part of standard transaction processing
- Many changes are made by generic, privileged accounts and difficult to determine the named DBA
- Database and application patches may result in hundreds of database changes
- Initialization parameters may be changed in the database or operating system files

Oracle EBS Customizations/Development Objects

Oracle EBS is highly customizable, and customization and development can be done in the application, in the database, and on the application servers (web, forms, and concurrent manager)

- **CEMLI**
 - Configurations, Extensions, Modifications, Localizations, Integrations

- **RICE**
 - Reports, Interfaces, Conversions and Enhancements

Change Management Challenges

Development is done in the application UI, in the database using SQL statements, and in the operating system with many different types of files (SQL scripts, PL/SQL code, forms, web pages, shell scripts, etc.)

Oracle EBS Customizations

CM - Concurrent Manager Programs

CM1 - Shell script
CM2 - SQL*Plus
CM3 - PL/SQL
CM4 - Java
CM5 - Pro*C binary
CM6 - Perl

FRM - Forms

FRM1 - Forms Personalizations
FRM2 - Custom Forms
FRM3 - Custom Libraries (custom.pll)

RPT - Reports

RPT1 - Report RDF
RPT2 - BI/XML Publisher Templates and Reports
RPT3 - Financial Statement Generator (FSG)

EBS - Oracle EBS Customizations

EBS1 - Oracle Alerts
EBS2 - SQL Pages
EBS3 - Workflows

WEB - Web Pages

WEB1 - Java Server Pages (JSP)
WEB2 - Servlets
WEB3 - OA Framework (OAF) Pages
WEB4 - OA Framework Personalizations
WEB5 - Modplsql
WEB6 - APEX
WEB7 - ADF applications

DB - Database

DB1 - Packages, Procedures and Functions
DB2 - Tables/Views
DB3 - Triggers
DB4 - Materialized Views

WS - Web Services

WS1 - SOA Gateway
WS2 - XML Gateway

Other Oracle EBS Changes

- Oracle EBS Application Server patches
- Java patches – application server, database, OS
- Oracle stack patches
 - Exadata patches
 - BI Publisher
 - OBIEE
 - Oracle Identity Management (OID, Access Manager, etc.)
- Operating system
 - Patches
 - User security
 - File permissions, storage, etc.
- Networking
- Hardware

Agenda

1

Database and Application Account Risks

2

Sensitive Data Risks

3

Auditing and Logging Gaps

4

Change Management Challenges and Risks

5

Bonus – Oracle E-Business Suite Security Patches

Oracle E-Business Suite Version Support

Version	Premier Support End Date	Extended Support End Date (1)	CPU Support End Date	References MOS Note ID
EBS 12.2 (3)	December 2030	TBD	October 2030	Lifetime Support
EBS 12.1	December 2021	N/A	October 2021 (2)	1495337.1
EBS 12.0	January 2012	January 2015	January 2015	
EBS 11.5.10	November 2010	November 2013	January 2016 (2)	1596629.1
EBS 11.5.9	June 2008	N/A	July 2008	
EBS 11.5.8	November 2007	N/A	October 2007	
EBS 11.5.7	May 2007	N/A	April 2007	

1. Extended support requires a minimum baseline patch level – see MOS Note ID 1195034.1.
2. CPUs are available after end date for customers with Market Driven Support Contracts – see MOS Note ID 1596629.1/1495337.1.
3. 12.2 end dates are a rolling 10 years and are being extended every year for the foreseeable future.

Database Versions and CPU Support

Major Releases	Extended Support End Date	Patchsets	CPU Support End Date
Oracle 19c	April 2027	19.x	April 2027
Oracle 12c R1	August 2022	12.1.0.2	July 2022
		12.1.0.1	July 2016 (extended from July 2015)
Oracle 11g R2	December 2020	11.2.0.4	October 2020 (extended from October 2018)
		11.2.0.3	July 2015
		11.2.0.2	January 2013
		11.2.0.1	July 2011
Oracle 11g R1	August 2015	11.1.0.7	July 2015
Oracle 10g R2	July 2013	10.2.0.5	July 2013

Agenda

1

Database and Application Account Risks

2

Sensitive Data Risks

3

Auditing and Logging Gaps

4

Change Management Challenges and Risks

5

Q & A

Integrigy 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**

linkedin – **linkedin.com/company/integrigy**

twitter – **twitter.com/integrigy**