Introducing the Integrigy Cybersecurity Framework for Oracle E-Business Suite

May 17, 2022

Stephen Kost
Chief Technology Officer
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. Integrigy Security Framework for Oracle E-Business Suite
2. Access Management
3. Sensitive Data Protection
4. DevSecOps
5. Anomaly and Event Management

Oracle E-Business Suite Security Challenges

- **Oracle E-Business Suite (EBS) is a highly complex application and technology environment**
  - Oracle EBS is not well understood by IT Security
  - Often no security focus on enterprise package applications or databases
- **Entire Oracle EBS technology stack must be properly maintained and secured including the application, database, and application servers**
  - Each technology component has unique security and compliance requirements
  - General IT security controls must be adapted for the technology stack
- **Oracle EBS has limited integration with existing IT Security tools and processes**
  - Poor IT Security visibility and oversight of the application and database
- **Security vulnerabilities and issues are often introduced in Oracle EBS through customizations and extensions**
  - Oracle EBS customization is different from typical enterprise application development

NIST Cybersecurity Framework

- **The NIST Cybersecurity Framework v1.1 is a risk-based approach to managing cybersecurity risk**
  - Provides a high-level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes
  - A common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders
  - Helps to identify and prioritize actions for reducing cybersecurity risk
- **The Framework has these primary components –**
  - Governance of cybersecurity risk
  - Approaches to identifying, authenticating, and authorizing individuals to access organizational assets and systems
  - Awareness and training measures
  - Anomalous activity detection and system and assets monitoring
  - Response activities, including information sharing or other mitigation efforts

NIST Cybersecurity Framework

Identify	Protect	Detect	Respond
Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	Develop and implement appropriate safeguards to ensure delivery of critical services.	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident
Asset Management Business Environment Governance Risk Assessment Risk Management Strategy Supply Chain Risk Management	Identity Management and Access Control Awareness and Training Data Security Information Protection Processes and Procedures Maintenance Protective Technology	Anomalies and Events Security Continuous Monitoring Detection Processes	Response Planning Communications Analysis Mitigation Improvements

NIST Cybersecurity Framework v1.1 – https://www.nist.gov/cyberframework/framework

Integrigy Cybersecurity Framework for Oracle E-Business Suite

- **The Integrigy Cybersecurity Framework addresses people, processes, and technology to ensure the Oracle E-Business Suite is secure**
  - Focused on the Oracle E-Business Suite and technology stack
- **Aligned with the enterprise IT Security standards, guidelines, practices, and ecosystem as well as the business requirements, risk tolerances, and resources**
  - Enterprise Risk and Compliance
  - Cybersecurity
  - Identity and Access Governance
  - Data Protection and Privacy
- **Framework is mapped to the following standards for reference and completeness –**
  - NIST Cybersecurity Framework v1.1 and SP 800-53
  - ISO 27001/27002
  - ISACA Control Objectives for Information and Related Technologies (COBIT)
  - Center for Internet Security (CIS) Critical Security Controls
  - Cloud Security Alliance (CSA) Top 20 Critical Controls for Cloud Enterprise Resource Planning Customers
  - Open Web Application Security Project (OWASP) OWASP Application Security Verification Standard (ASVS)

Integrigy Cybersecurity Framework for Oracle E-Business Suite

Governance (G)	Protect (P)	Detect (D)	Respond (R)
Asset Management Risk Management Policies and Standards Change Management DevSecOps Service Provider Management Supply Chain Risk Management	Access Management ▪ Identity Management ▪ Access Control Secure Configuration Data Protection Vulnerability Management	Anomaly and Event Management Continuous Security Monitoring Threat Detection User Behavior Analysis Data Leakage Prevention	Response Planning Communications Analysis and Mitigation Improvements

Protect (P)

		Oracle EBS Components			
		Application	**Database**	**Application Server**	**OS/Network**
Operational Processes	**Access Management**	▪ User Management ▪ System Admin SOD	▪ Database Security ▪ DBA SOD	▪ WebLogic Security	▪ OS Security
	Secure Configuration	▪ Oracle EBS Guideline ▪ Secure Configuration Console ▪ AppSentry	▪ Oracle DB Guideline ▪ AppSentry	▪ Oracle App Server Guideline ▪ AppSentry	▪ OS Guideline
	Data Protection	▪ Native EBS Encryption ▪ Application Auditing	▪ Database Encryption ▪ Scrambling ▪ Data Masking/Redaction ▪ Database Auditing	▪ Web Encryption	▪ Network Encryption
	Vulnerability Management	▪ Application Patches ▪ AppDefend Virtual Patching	▪ Database Patches	▪ Application Servers Patches	▪ OS Patches

Agenda

1. Integrigy Security Framework for Oracle E-Business Suite
2. **Access Management**
3. Sensitive Data Protection
4. DevSecOps
5. Anomaly and Event Management

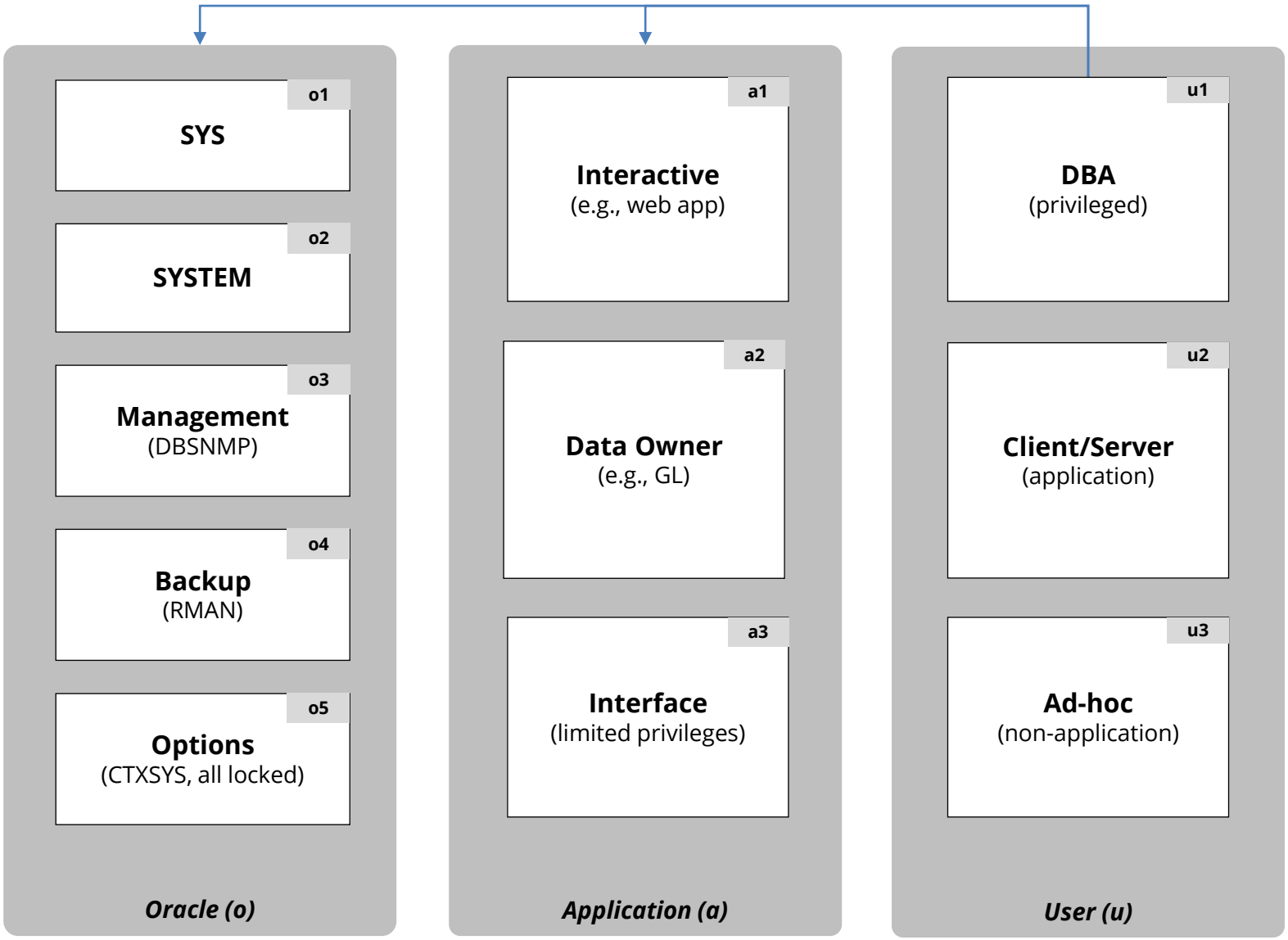
Oracle EBS Application User Populations

Internal Named Users	▪ May be defined locally or externally (SSO)
External Named Users	▪ iSupplier, iStore, iRecruitment, … ▪ Suppliers, customers, and candidates
Seeded Oracle EBS	▪ 30+ generic privileged accounts ▪ SYSADMIN and GUEST are required ▪ ASGADM, IBE_ADMIN, and others may be required by specific modules but should be end-dated and password changed
Enterprise Generic Accounts	▪ May be used to manage concurrent manager or other application functions

Oracle EBS Seeded Generic Application Accounts (30+)

Active Application Account	Default Password	Active Responsibilities
ASGADM	WELCOME	▪ SYSTEM_ADMINISTRATOR ▪ ADG_MOBILE_DEVELOPER
IBE_ADMIN	WELCOME	▪ IBE_ADMINISTRATOR
MOBADM	MOBADM	▪ MOBILE_ADMIN ▪ SYSTEM_ADMINISTRATOR
MOBILEADM	WELCOME	▪ ASG_MOBILE_ADMINISTRAOTR ▪ SYSTEM_ADMINISTRATOR
OP_CUST_CARE_ADMIN	OP_CUST_CARE_ADMIN	▪ OP_CUST_CARE_ADMIN
OP_SYSADMIN	OP_SYSADMIN	▪ OP_SYSADMIN
WIZARD	WELCOME	▪ AZ_ISETUP ▪ APPLICATIONS FINANCIALS ▪ APPLICATION IMPLEMENTATION

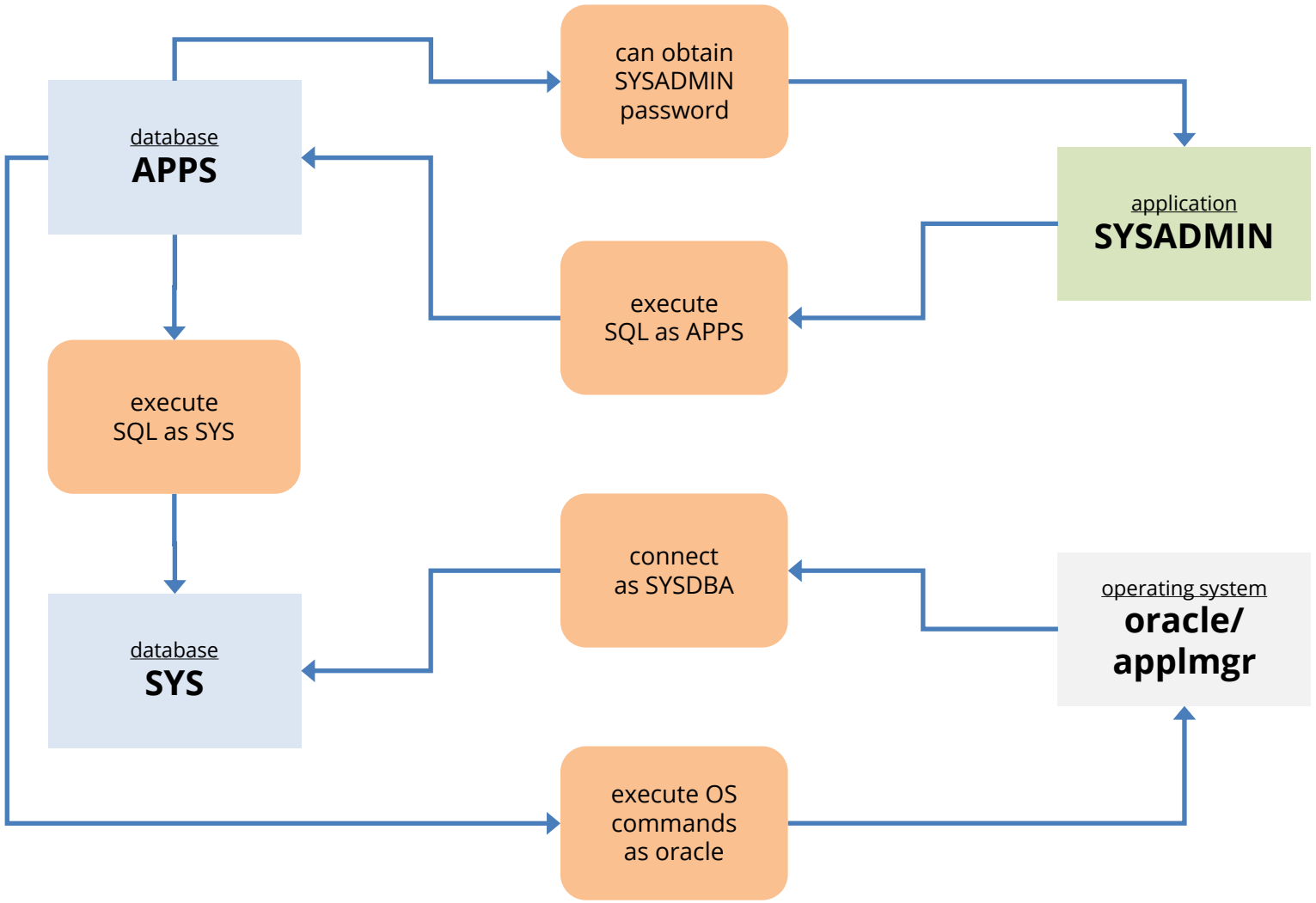
Oracle EBS Database Account Definition



Oracle EBS Generic Privileged Application Accounts

Oracle E-Business Suite	**SYSADMIN** *seeded application accounts*
Oracle Database	**APPS, APPLSYS** **SYS, SYSTEM** *Oracle EBS schemas (GL, AP, …)*
Operating System *(Unix and Linux)*	**root** **oracle, applmgr**

Generic Privileged Account Inter-Dependency



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

Provisioning (P)

ID	Process	Description	Example Controls
P1	**Identity and Privilege Request**	Process for creation or changes to an identity and/or privileges. Request should be formal and documented.	▪ Sample to ensure requests are documented
P2	**Request Approval**	Formal and documented approval of all identity and privilege requests. Requests should be approved by user management and system owners.	▪ Sample to ensure requests are approved
P3	**Identity Creation**	Identities are only created by the security-responsible administrator. Account identifiers are created according to organization policies. Unique, change on first use are assigned for all new identities.	▪ Log and review all account creation ▪ Sample account creation to request and approvals
P4	**Privilege Assignment**	Privileges are only assigned by the security-responsible administrator. Privileges are standardized across all databases. Default deny and least privilege principles are used. Privilege assignments are through roles rather than directly to identity.	▪ Log and review all privilege assignments
P5	**Communication**	Identity and authentication credentials are communicated to the user in a secure manner and conform to organization's data classification policy.	▪ Sample communication process to verify it is done securely

Authentication & Authorization (A)

ID	Process	Description	Example Controls
A1	**Identity authentication**	Identities are authenticated and validated. All users and their activity are uniquely identifiable. Authentication may be local database, operating system, or directory services.	▪ Log all database access ▪ Alert on access to unused default database accounts ▪ Alert on use of end-user accounts outside business hours
A2	**Password controls**	Password controls adhere to organization security policies.	▪ Review and test password controls ▪ Test passwords by brute forcing
A3	**Privilege determination**	Privileges are authorized and validated. Authorization may be local database roles/privileges, operating system roles, or directory services roles.	▪ Log and review security critical privilege usage ▪ Log all role selection
A4	**Identity and privilege validation**	Identifies and privileges are reviewed and validated by user management and IT management on a periodic basis.	▪ Review identities and privileges on a periodic basis ▪ Validate privileges consistent with job role
A5	**Segregation of Duties (SoD)**	Process or system used to monitor for segregation of duties for database accounts.	▪ Monitor for SoD violations

Administration (M)

ID	Process	Description	Example Controls
M1	**Password changes**	End-users are able to change passwords according to organization policy. Processes for changing service account passwords are documented and updated.	▪ Review password change functionality
M2	**Password resets**	Formal and documented process for end-user and service accounts. Passwords only reset by the security-responsible administrator. User is positively identified. Unique new password assigned and communicated securely.	▪ Log and review all non-user password resets. ▪ Sample non-user password resets for approved request.
M3	**Account locking**	Accounts are locked upon security events such as number of failed logins.	▪ Log and review all account locking
M4	**Account expiration**	Accounts are routinely expired for non-use based on organizational policy.	▪ Periodic review for stale accounts
M5	**Password expiration**	Account passwords expired and user must change passwords per organization policy. Service account passwords are changed periodically according to organization policy.	▪ Periodic review for password changes

De-Provisioning (D)

ID	Process	Description	Example Controls
D1	**Revocation notification**	Formal and documented process for pro-active and timely notification of termination or job role changes for revocation of identities or privileges.	▪ Sample terminated users to verify accounts are terminated on a timely basis
D2	**Revocation request**	Formal and documented request process to request termination of identifies or removal or privileges.	▪ Sample to ensure requests are documented, approved, and completed
D3	**Identity revocation**	Identifies are revoked on a timely basis by the security-responsible administrator. This process may include locking accounts and removing after a period of time.	▪ Sample terminated users to verify accounts are terminated on a timely basis ▪ Log and review all account locking and deletion
D4	**Privilege revocation**	Privileges are revoked on a timely basis by the security-responsible administrator.	▪ Sample privilege revocation requests to verify privileges are revoked on a timely basis ▪ Log and review all privilege revocation

Oracle EBS 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	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			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. Integrigy Security Framework for Oracle E-Business Suite
2. Access Management
3. **Sensitive Data Protection**
4. DevSecOps
5. Anomaly and Event Management

What is Sensitive Data?

Payment Card Industry Data Security Standard (PCI-DSS 3.2)	▪ Credit Card Number
	  ▪ *Primary Account Number (PAN)*
	▪ CVV/CV2/CID
	  ▪ *3 digits on the back for Visa/MC*
	  ▪ *4 digits on the front for AMEX*
	▪ Magnetic Stripe Data (very rare in applications)

Privacy Regulations (employees, customers, vendors)	▪ First and last name
	▪ Plus one of the following:
	  ▪ Social security number (SSN, Tax ID, 1099)
	  ▪ Credit card number
	  ▪ Bank account number
	  ▪ Financial account number
	  ▪ Driver license or state ID number

HIPAA (Privacy Standard and Security Rule)	▪ First and last name
	▪ Plus one of the following (Protected Health Information)
	  ▪ “the past, present, or future physical or mental health, or condition of an individual”
	  ▪ “provision of health care to an individual”
	  ▪ “payment for the provision of health care to an individual”

Where else might be Sensitive Data? (Oracle EBS)

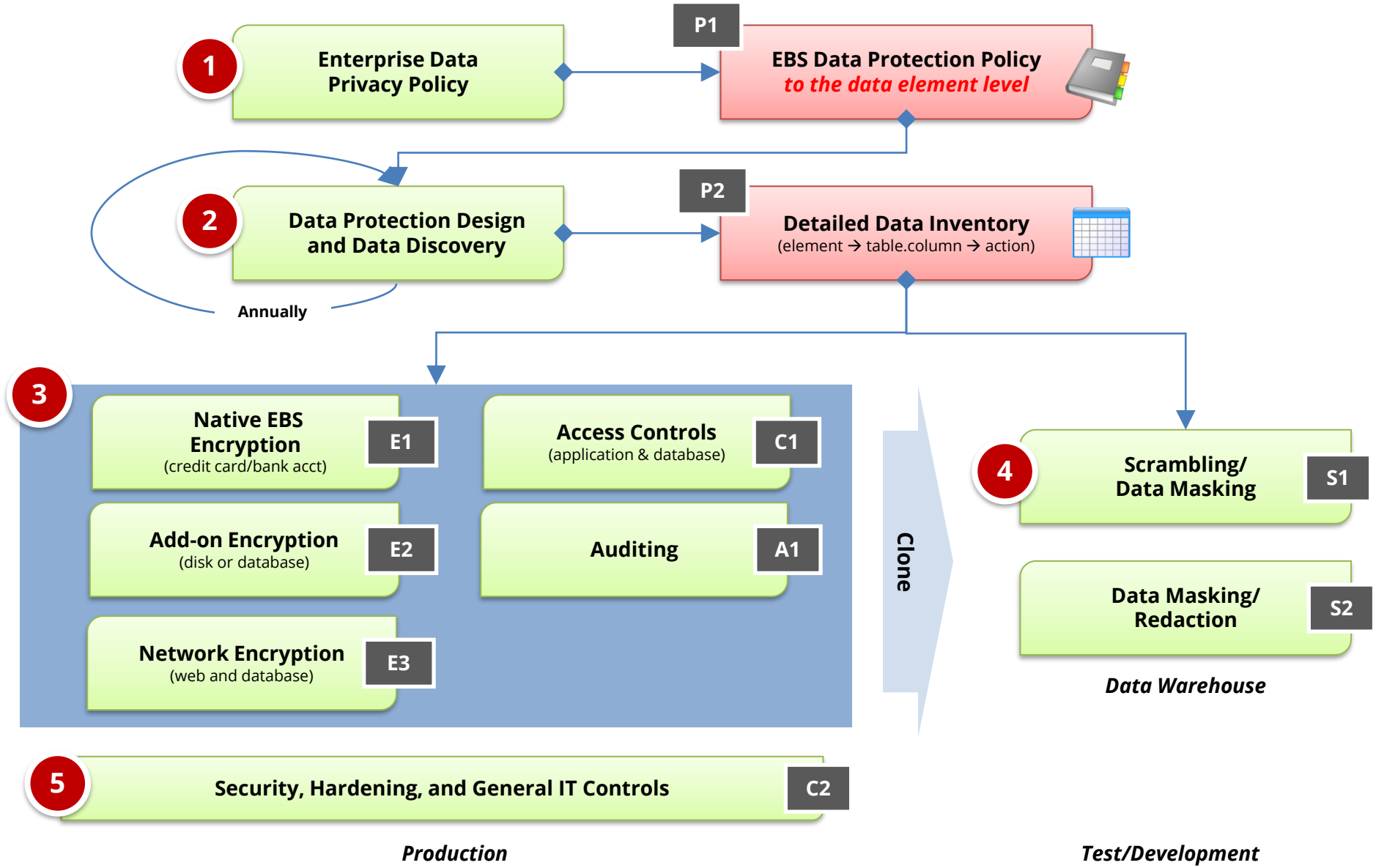
Database

- **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)

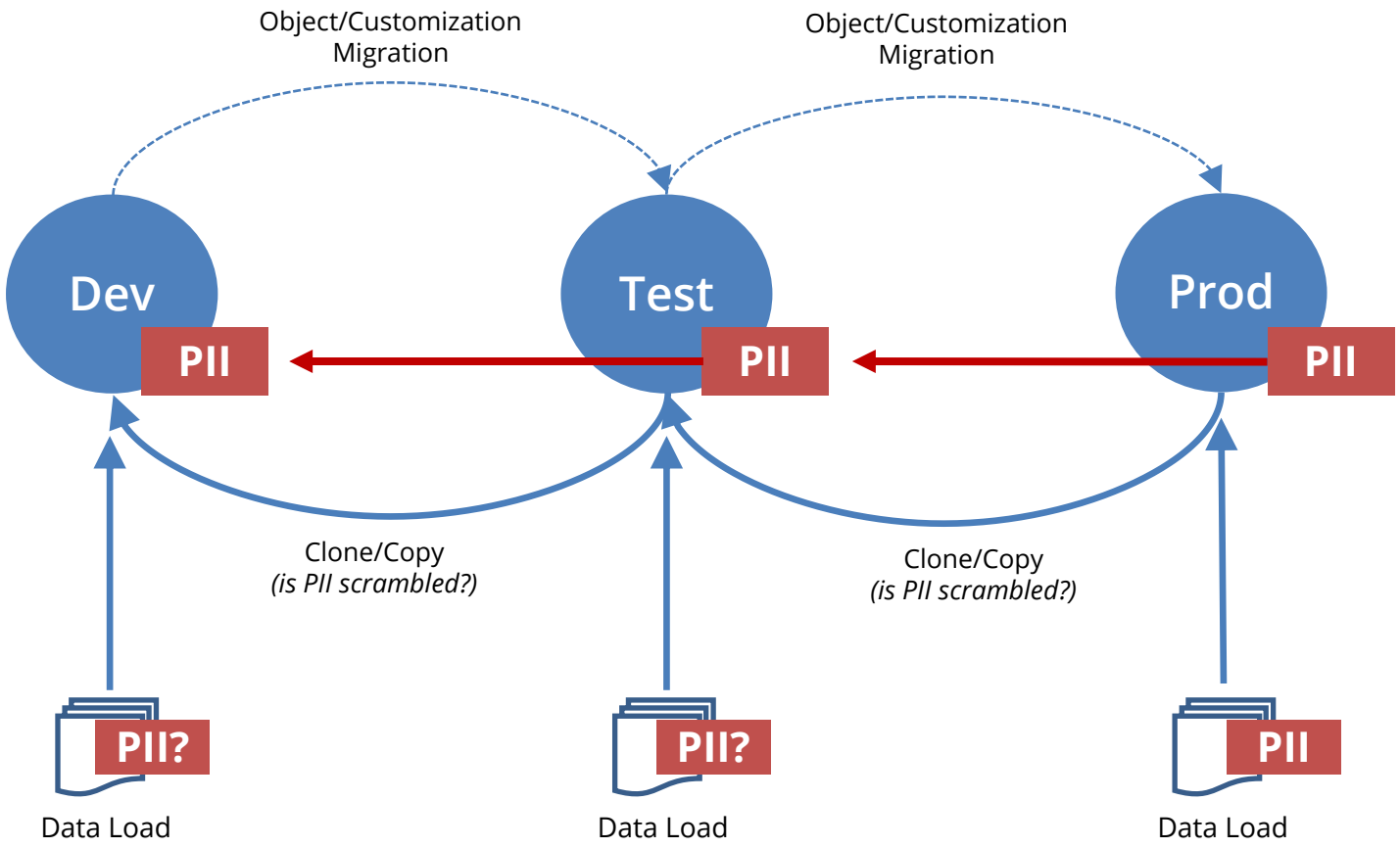
File System

- **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

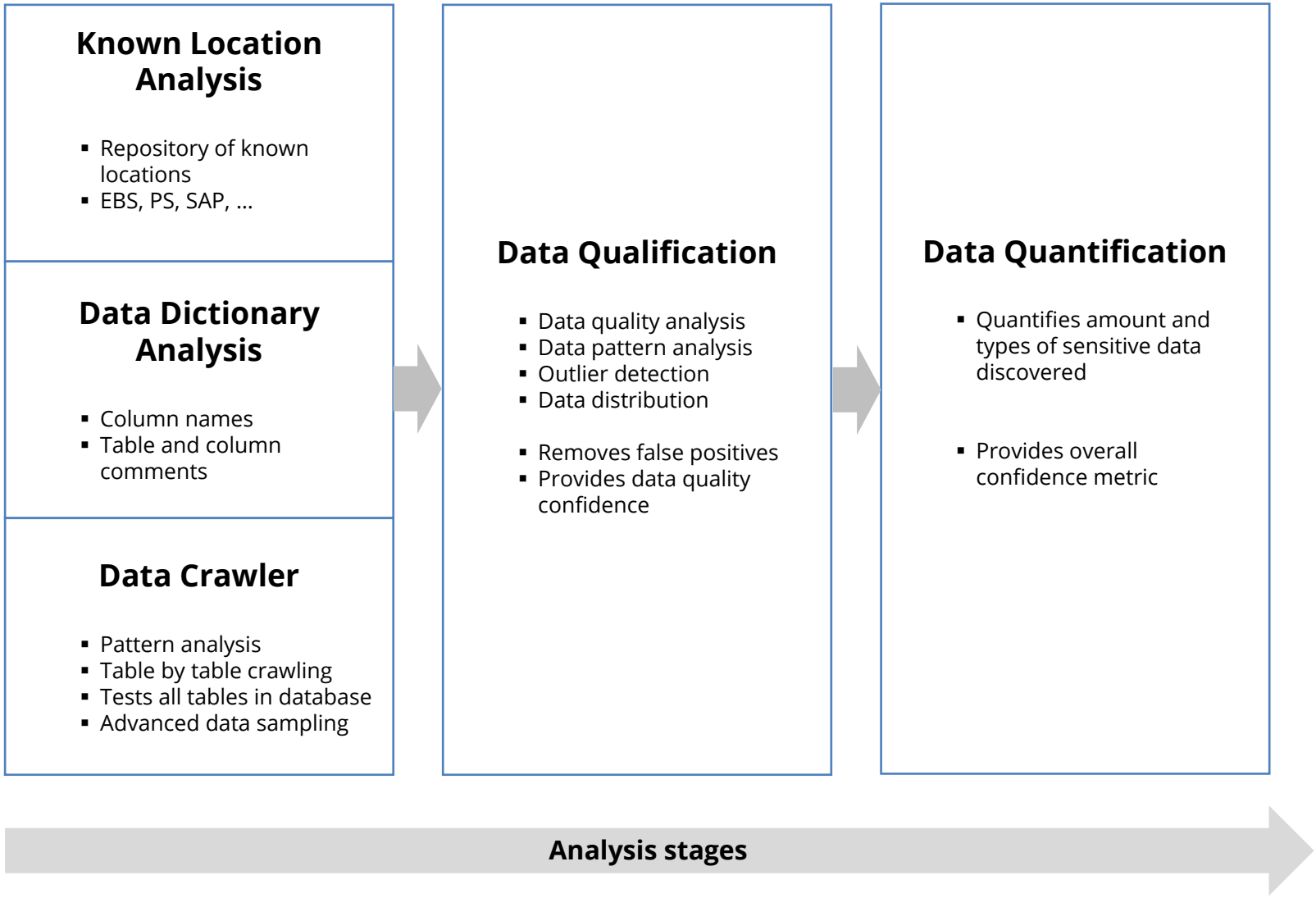


PII = Personally Identifiable Information

Sensitive Data Discovery

- **Detailed sensitive data inventory should be maintained**
  - Must be updated periodically
  - Work with development teams and DBAs to identify new locations
- **Do not rely solely on column names to find sensitive data**
  - Column names are very unreliable
  - No standard naming conventions
  - Data may be in multi-use columns such as Oracle EBS Flexfields
- **Use an automated tool to periodically scan for sensitive data**
  - Oracle DBSAT – Discoverer
  - Oracle Enterprise Manager – Quality Management -> Data Discovery
  - Oracle Cloud Data Safe – Data Discovery
  - Integrigy AppSentry Sensitive Data Discovery

Optimal Sensitive Data Discovery (SDD)



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	▪ Can be disabled	▪ 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	▪ Fixed	▪ Access auditing
a1 - Interactive	▪ How is account controlled	▪ Review privileges	▪ Access auditing
a2 – Data Owner	▪ How is account controlled	▪ Review – limited privileges only – no DBA privileges	▪ 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

Data Protection vs. Threats (Sample)

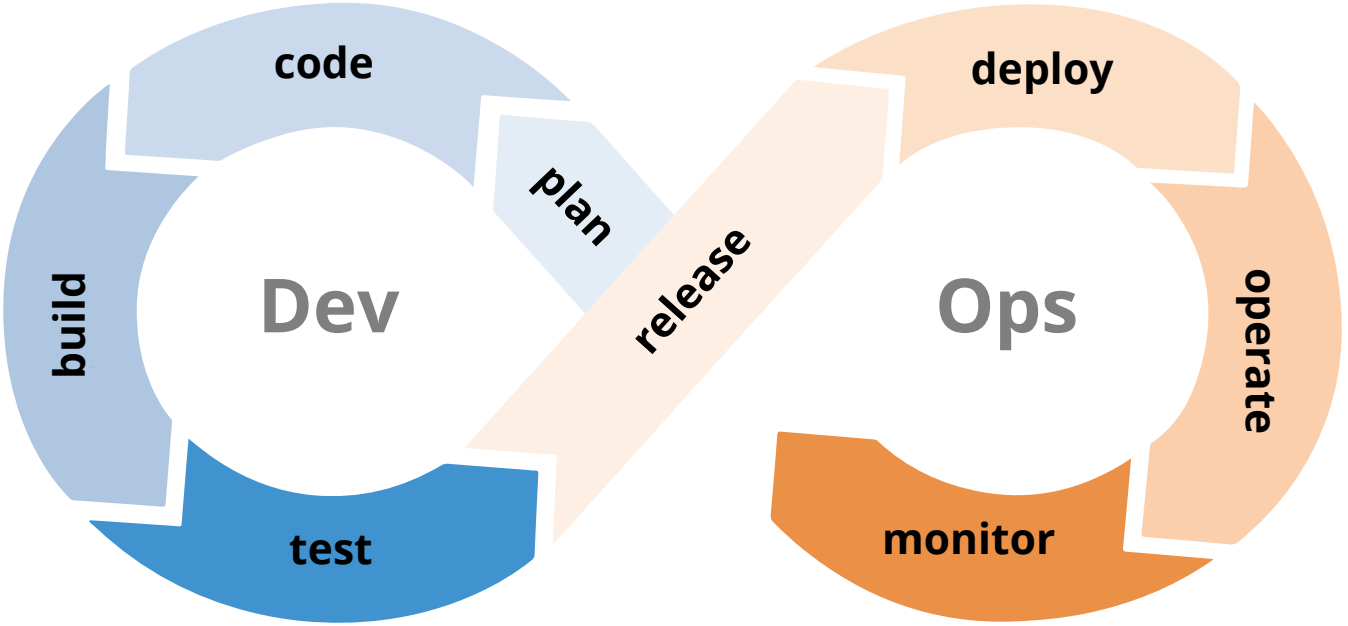
Data Access Method and Threats	Oracle Options						
	1 App Encrypt	**2** Trigger View	**3** Oracle TDE	**4a** FGAC	**4b** Internal Audit	**4c** External Audit	**3 + 4** TDE + Auditing
1. Application access by end-users (role/RBAC)	E	E		C	A	A	A
2. Application access by application administrators	E+	E-		C	A	A	A
3. Database access by DBA	E	E		C	A+	A	A
4. Database access by application DBA (SYSTEM, app)	E+	E+			A+	A+	A+
5. Database access by other database accounts	E	E		C	A	A	A
6. Operating system access to database data files	E	E	E				E
7. On-line or off-line access to database backups	E	E	E				E
8. Exploitation of applications security vulnerabilities	E-	E-		C+	A+	A+	A+
9. Exploitation of Oracle Database security vulnerabilities	E+	E+		C+	A+	A+	A+
10. Exploitation of operating system security vulnerabilities	E	E	E				E

E = Encrypted, **C** = Access Controlled, **A** = Access Audited, **+** = Mostly **-** = Partially

Agenda

1. Integrigy Security Framework for Oracle E-Business Suite
2. Access Management
3. Sensitive Data Protection
4. **DevSecOps**
5. Anomaly and Event Management

What are “DevOps” and “DevSecOps”?



DevOps	**Development – Operations** ▪ Software Development and IT Operations philosophies, practices, and tools to accelerate development, provide continuous delivery, and improve software quality
DevSecOps	**Development – Security – Operations** ▪ Incorporation of a security foundation into DevOps

Why DevSecOps for Oracle E-Business Suite?

- **Oracle E-Business Suite is a highly complex application and technology environment**
  - Oracle EBS is not well understood by IT Security
  - Often no security focus on customizations
- **Many security vulnerabilities and issues are introduced in Oracle EBS through customizations and extensions**

Types of Vulnerabilities	***Average # of Vulnerabilities per Assessment***
SQL Injection	2.4
Cross-Site Scripting (XSS)	0.5
XML Issues (e.g., XML entity attacks)	0.2
APPS Password Issues	1.4
Authorization/Authentication Issues	2.7
Other Issues	1.5

Source – Integrigy Customization Assessments 2018 – 2022

Oracle E-Business Suite DevSecOps Challenges

Highly Complex Application Environment	▪ Web, application, and database development ▪ 1,009 security vulnerabilities have been patched in Oracle code between 2005 and 2022 – if Oracle can't do it perfectly, can you?
Customization vs Development	▪ Development is focused on customizations ▪ Each customization is a small development project ▪ Pinpoint development objects created in multiple technologies and languages
Open Development Environment	▪ Development is done at multiple layers of the technology stack – web, application, database ▪ Some development is done inside the application ▪ Easy to have poor version control and weak change management

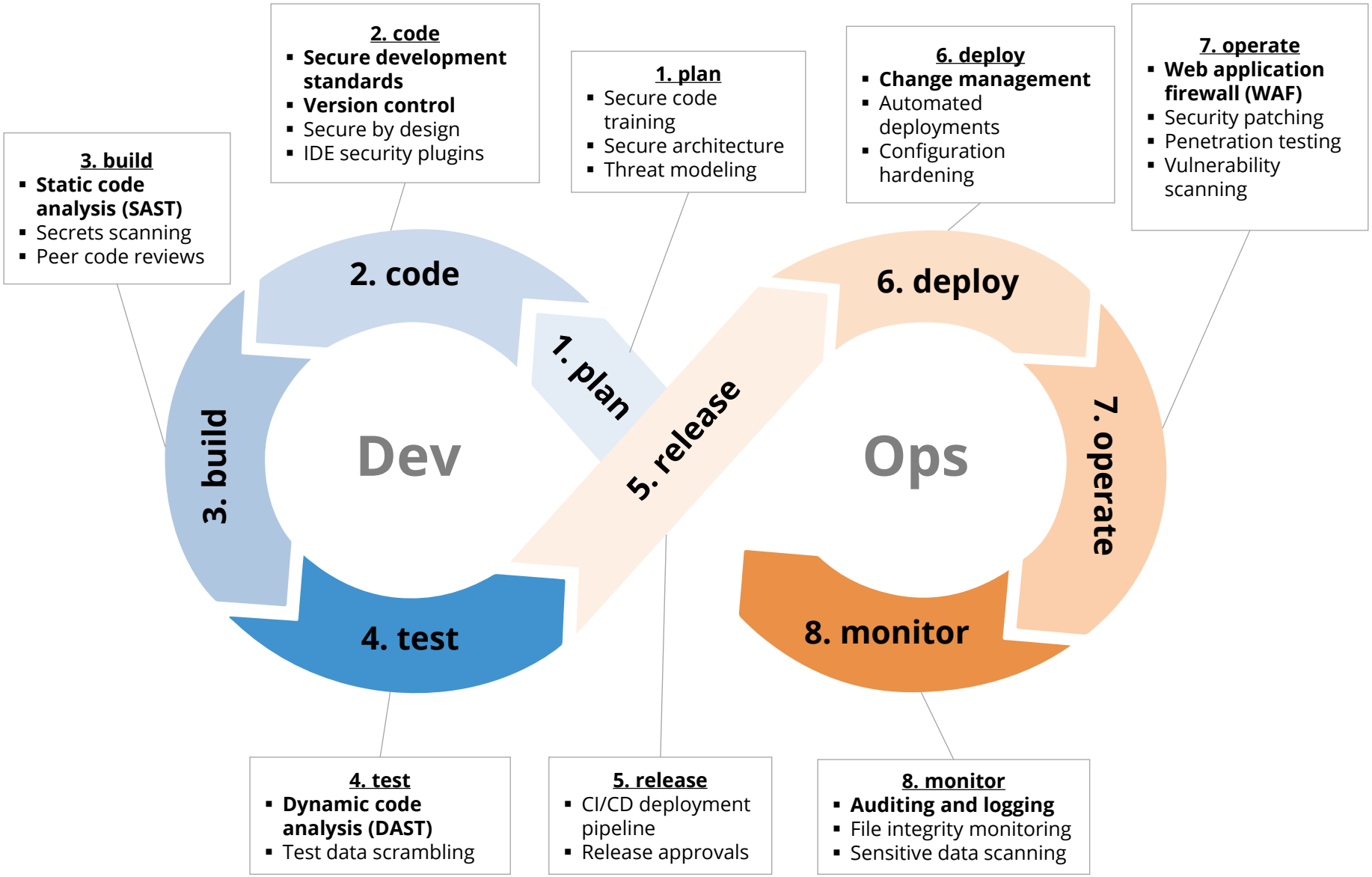
DevSecOps Principles

Shift Left	▪ "Shifting left" is moving security to earlier stages of the development cycle ▪ Ensure security standards and best practices are met when code is first developed
Automation	▪ Automated code analysis, security testing, and compliance verification ▪ Automation reduces the burden on IT Security
Continuous Feedback	▪ Security is evaluated at multiple points in the development cycle through both automated and manual processes ▪ Security vulnerabilities are fixed immediately early in the development cycle

DevSecOps Benefits

Improve Security	▪ Identify and eliminate security vulnerabilities ▪ Automate security vulnerability identification processes to allow IT Security to focus on design, implementation, and infrastructure ▪ Security end-to-end rather than an afterthought
Speed Delivery	▪ Minimize security bottlenecks in the development process ▪ Extend security into development
Reduce Time and Effort to Fix	▪ Identify and fix security vulnerabilities early in the development cycle ▪ Fix during development rather than during testing ▪ Security testing and feedback when code is committed instead of just when tested

Oracle E-Business Suite DevSecOps



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)

- **RICE**
  - **R**eports, **I**nterfaces, **C**onversions and **E**nhancements
- **CEMLI**
  - **C**onfigurations, **E**xtensions, **M**odifications, **L**ocalizations, **I**ntegrations

- **RICEW**
  - **R**eports, **I**nterfaces, **C**onversions, **E**nhancements, and **W**orkflows
- **FRICE**
  - **F**orms, **R**eports, **I**nterfaces, **C**onversions and **E**nhancements

Oracle EBS Customization Documentation

Oracle Applications Framework Personalization Guide

Oracle Applications Framework Developers Guide (1,093 pages)

Oracle E-Business Suite Developer’s Guide

Oracle Integrated SOA Gateway Developers Guide

Oracle Workflow Developer’s Guide

Oracle E-Business Suite Module Apps Developer’s Guide

Oracle E-Business Suite Desktop Integration Framework Developer’s Guide

Oracle Configurator Developer’s Guide

Customization in Oracle Applications (Doc ID 743490.1)

Developing and Deploying Customizations in Oracle E-Business Suite Release 12.2 (Doc ID 1577661.1)

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 - Application Express (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

Oracle EBS Customizations

Type	Customization	Language	Deployment	Secrets?	Key Issues
Concurrent Manager Programs	CM1 - Shell script	Shell	File (.prog)	Yes	echo APPS password, injection
	CM2 - SQL*Plus	SQL	File (.sql)		SQL injection
	CM3 - PL/SQL	PL/SQL	File (.pl*)	Yes	SQL injection
	CM4 - Java	Java	File (.java)	Yes	SQL injection
	CM5 - Pro*C binary	C	File (.c)		SQL injection, buffer overflow
	CM6 - Perl	Perl	File (.pl)	Yes	Injection
Forms	FRM1 - Forms Personalizations	PLSQL	Database		SQL injection, authorization
	FRM2 - Custom Forms	PLSQL	File (.fm*)		SQL injection, authorization
	FRM3 - Custom Libraries (custom.pll)	PLSQL	File (.pl*)		SQL injection
Reports	RPT1 - Report RDF	SQL, JS	File (.rdf)		SQL injection
	RPT2 - BI/XML Publisher Templates and Reports	SQL	File (.xml)		SQL injection
	RPT3 - Financial Statement Generator (FSG)		Database		
EBS Customizations	EBS1 - Oracle Alerts	SQL	Database		unauthorized SQL
	EBS2 - SQL Pages	SQL	Database		unauthorized SQL
	EBS3 - Workflows	XML	File (.wtf)		

Oracle EBS Customizations

Type	Customization	Language	Deployment	Secrets?	Key Issues
Web Pages	WEB1 - Java Server Pages (JSP)	JSP	File (.jsp)		SQL injection, authorization
	WEB2 - Servlets	Java	File (.java)	Yes	SQL injection, authorization
	WEB3 - OA Framework (OAF) Pages	Java	File (.java,.xml)		SQL injection
	WEB4 - OA Framework Personalizations	XML	Database File (.xml)		
	WEB5 - Modplsql	PLSQL	Database		SQL injection
	WEB6 - Application Express (APEX)	SQL	Database File (.sql)		SQL injection
	WEB7 - ADF applications	Java	File (.java)	Yes	SQL injection
Database	DB1 - Packages, Procedures, and Functions	PLSQL	Database File (.sql)	Yes	SQL injection, authorization
	DB2 - Tables/Views	SQL	Database File (.sql)		
	DB3 - Triggers	SQL	Database File (.sql)		authorization
	DB4 - Materialized Views	SQL	Database File (.sql)		
Web Services	WS1 - SOA Gateway	Multiple	Database	Yes	SQL injection, authorization
	WS2 - XML Gateway		Database		

Customization Development

Version Control	▪ A version control system such as Git should be used for all custom code that resides on the operating system ▪ Dev and test environments are not a version control system ▪ Some customizations reside only in the database and must be handled separately
Secure Development Standards	▪ Oracle EBS development standards must also address secure code development in order to eliminate SQL injection, Java deserialization, and other common Oracle EBS vulnerabilities ▪ Development standard must cover all types of Oracle EBS customizations include Oracle Forms, APEX, shell scripts, etc.
IDE Security Plugins	▪ Use IDE security plugins to help eliminate vulnerabilities during code creation and unit testing ▪ JDeveloper supports PMD plugin for Java and PL/SQL security checks

Note: See “OA Framework: How to Identify Required Oracle JDeveloper Patches For Oracle E-Business Release 12.x or 11i” (Doc ID 416708.1)

Customization Testing

SAST (Static Code Analysis)	▪ All source code and custom database code (PL/SQL, APEX, etc.) must be periodically scanned for security vulnerabilities ▪ Problem with Oracle EBS customizations is that there are at least nine languages that may be used ▪ Use tools like PMD (Java, PL/SQL), FindSecBugs, SonarCube, Checkmarx to scan source code repository ▪ **AppSentry Code** uses open source and proprietary libraries to scan all Oracle EBS languages includes Oracle Forms/Reports and APEX
Secrets Scanning	▪ Eliminate hard-coded secrets including passwords, credentials, encryption keys, cloud keys, and certificates ▪ Use a tool such as **AppSentry Code** to scan source code and database for secrets – scan all deployment packages using both regex and entropy ▪ Wrapped PL/SQL code may contain credentials and secrets such as DBMS_CRYPTO encryption keys

Customization Deployment

Change Management	▪ ALL changes to Oracle EBS production must go through the change management process ▪ The organization must clearly define what is an Oracle EBS change ▪ Only authorized users may be allowed to make changes or migrate code into production ▪ Developers should only have read access to production at most ▪ An automated tool should be used to migrate and deploy all customizations into production
Configuration Hardening	▪ The Oracle EBS configuration and technology stack must be hardened to ensure all application and database security control operate effectively and cannot be bypassed ▪ Use the “Secure Configuration Guide for Oracle E-Business Suite” as a starting point ▪ Use **AppSentry** to validate the configuration of Oracle EBS, WebLogic, and Oracle Database

Operate and Maintain

Web Application Firewall (WAF)	▪ Implement a WAF to protect Oracle EBS from web vulnerabilities such as SQL injection, XSS, Java deserialization ▪ General purpose WAFs do not adequately protect Oracle EBS ▪ **AppDefend** provides full protection for Oracle EBS including for many 0-day vulnerabilities
Security Patching	▪ Regularly apply Critical Patch Updates to Oracle EBS, WebLogic, and Database ▪ If unable to regularly apply security patches, use **AppDefend** for virtual patching
Vulnerability Scanning/ Penetration Testing	▪ Must periodically validate the configuration of the entire Oracle EBS technology stack to ensure there are no misconfigurations, open vulnerabilities, missing security patches, etc. ▪ Use both periodic automated scanning and in-depth annual manual penetration testing for comprehensive testing ▪ **AppSentry** can automate vulnerability assessment and assist with penetration testing

Operate and Maintain

Web Application Firewall (WAF)	▪ Implement a WAF to protect Oracle EBS from web vulnerabilities such as SQL injection, XSS, Java deserialization ▪ General purpose WAFs do not adequately protect Oracle EBS ▪ **AppDefend** provides full protection for Oracle EBS including for many 0-day vulnerabilities
Security Patching	▪ Regularly apply Critical Patch Updates to Oracle EBS, WebLogic, and Database ▪ If unable to regularly apply security patches, use **AppDefend** for virtual patching
Vulnerability Scanning/ Penetration Testing	▪ Must periodically validate the configuration of the entire Oracle EBS technology stack to ensure there are no misconfigurations, open vulnerabilities, missing security patches, etc. ▪ Use both periodic automated scanning and in-depth annual manual penetration testing for comprehensive testing ▪ **AppSentry** can automate vulnerability assessment and assist with penetration testing

Identifying Security Vulnerabilities in Customizations

Manual Code Review	▪ All source code and customizations should undergo a peer code review when migrated from development to test ▪ Enhance code review process with findings from SAST tools ▪ Use standard code review methodologies modified for Oracle EBS ▪ OWASP Code Review Guide 2.0 ▪ https://owasp.org/www-project-code-review-guide/
Automated Code Review	▪ Perform SAST scans for all code migration from development to test ▪ Perform SAST scans of code repository and/or commits ▪ Multiple SAST tools are required for Oracle EBS customizations ▪ Commercial vs open-source tools ▪ Leverage currently used SAST tools whenever possible ▪ Be prepared for lots of false positives with EBS customizations

Oracle EBS Customizations

Type	Open Source SAST Tools	SAST Issues	AppSentry Code*	Oracle Key Issues
Shell Scripts	Shellcheck		Yes [1]	echo APPS password, injection
Java	PMD, FindSecBugs	source vs compiled	Yes [2]	SQL injection, authorization
Java – Database	PMD, FindSecBugs	OS file only	Yes [2]	SQL injection
JSP	PMD		Yes [2]	Authorization, SQL injection
OA Framework	none		Yes [1/2]	Authorization, SQL injection
Pro*C	Flawfinder		Yes [1]	Buffer overflow
Perl	none		Yes [1]	Print APPS password, injection
SQL*Plus	PMD		Yes [1/2]	DML, grants
SQL	PMD		Yes [1/2]	DML, grants
PL/SQL	PMD	wrapped code	Yes [1/2]	SQL injection, wrapped code
APEX SQL	APEX-SERT	database vs file	Yes [1]	SQL injection
Forms (fmb)	none	source vs compiled	Yes [1]	SQL injection
Forms Libraries (pll)	none	source vs compiled	Yes [1]	SQL injection, authorization
Reports (rdf)	none		Yes [1]	Autonomous transaction

* AppSentry Code uses (1) proprietary scan engine or (2) open-source scanner with custom EBS rules

Host Concurrent Manager Program (Shell Script)

Common Oracle EBS Issues	▪ Display of APPS password in output or log ▪ Concurrent Program Execution Options – Blank = passed as $1 ENCRYPT = passed as $FCP_LOGIN SECURE = not passed ▪ Injection of concurrent request parameter executed in OS command

Code Review	`echo $1`
	`-`
	`echo $FCP_LOGIN`
	`-`
	`PASS=$1`
	`echo $PASS`

SQL/SQL*Plus Scripts – Concurrent Program, Install, Data Fix, …

Common Oracle EBS Issues	▪ SQL injection through concurrent request parameters ▪ Execution of rouge SQL statements to perform malicious activities ▪ Inappropriate granting of database privileges such as to PUBLIC

Code Review	`GRANT EXECUTE ON xxacme.update_salary TO PUBLIC WITH GRANT OPTION;`
	`-`
	`SELECT * FROM sys.dba_objects`
	`WHERE owner ='&1';`
	`-`
	`GRANT DBA TO jane;`

PL/SQL – Concurrent Program, Custom Packages, …

Common Oracle EBS Issues	▪ SQL injection through concurrent request parameters ▪ SQL injection through custom packages, procedures, functions ▪ Privilege escalation when using DEFINER versus INVOKER rights ▪ Access to privileged database packages such as DBMS_SYS_SQL ▪ Unauthorized access to resources using UTL_FILE, UTL_HTTP, UTL_SMTP, … ▪ Hard-coding of credentials and keys especially in wrapped code ▪ Weak cryptographic functions especially in older code

Code Review	`sqlstr := 'SELECT code FROM states WHERE state-name = ''' || name || ''';`
	`EXECUTE IMMEDIATE sqlstr INTO code;`
	`-`
	`sqlstr := 'SELECT code FROM states WHERE state-name = ''' || name || ''';`
	`rows_processed := DBMS_SQL.EXECUTE(cursor_name);`
	`-`
	`sqlstr := 'SELECT code FROM states WHERE state-name = ''' || name || ''';`
	`OPEN cursor_states FOR sqlstr;`

Java – Concurrent Program, Servlet, OA Framework, …

Oracle EBS Issues	▪ SQL injection through user input such as HTTP request parameters, concurrent request parameters, etc. ▪ Cross-site scripting (XSS) in servlets and OA Framework ▪ Java deserialization attacks ▪ XML entity attacks ▪ Inappropriate file access

Code Review	`PreparedStatement pstmt =`
	`conn.prepareStatement("insert into EMP (ENAME) values ('" + name + "')");`
	`pstmt.execute();`
	`-`
	`String name = request.getParameter( "name" );`
	`pw.println( "<h1> Hello " + name + "</h1>");`
	`-`
	`Object object = ois.defaultReadObject();`

Custom Web Pages (JSP)

Oracle EBS Issues	▪ Missing authorization as authorization is done per page ▪ Sub-pages and include pages make code reviews difficult ▪ SQL injection through user input such as HTTP request parameters ▪ Cross-site scripting (XSS) in servlets and OA Framework ▪ Java deserialization attacks ▪ XML entity attacks ▪ Inappropriate file access

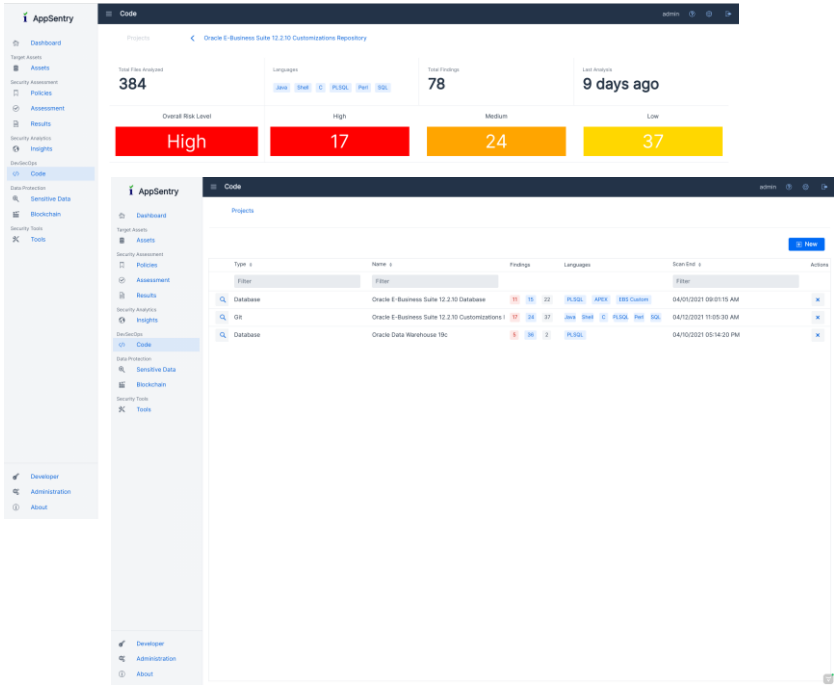
Code Review	`Missing check session or function – multiple ways to do this`
	`-`
	`PreparedStatement pstmt = request.getParameter("sql");`
	`pstmt.execute();`
	`-`
	`String renderMenu = request.getParameter("RENDER_MENU_PARAM");`
	`<p>%=renderMenu%</p>`

AppSentry Code

AppSentry Code brings DevSecOps to the Oracle E-Business Suite, PeopleSoft, and Oracle Database with source code analysis (SAST) and change tracking.

AppSentry Code Features

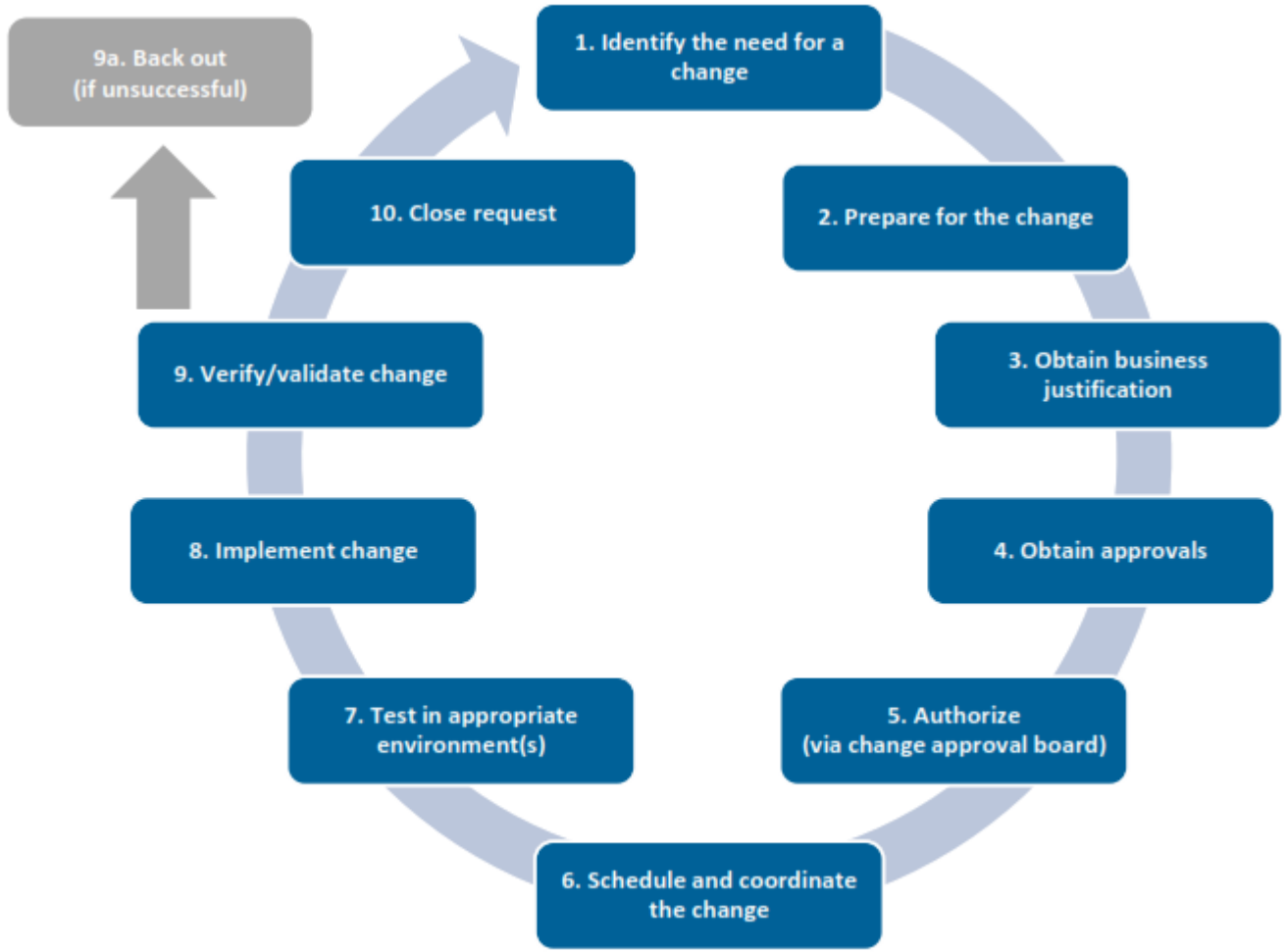
- Application and database DevSecOps processes integrating directly with your existing change management and object migration tools
- Oracle Database, Oracle E-Business Suite, and PeopleSoft specific code analysis and vulnerability discovery
- Secrets scanning with Oracle Database, EBS, PeopleSoft, OCI, AWS, and Azure patterns



AppSentry Code Scope

- Oracle E-Business Suite – concurrent manager (shell, PL/SQL, SQL*Plus, Java, C, Perl), web (Java, JSP, OA Framework), Forms, Reports, web services
- PeopleSoft – PeopleCode
- Oracle Database – PL/SQL, SQL, Java, APEX

Effective Oracle EBS Change Management Process



Source: The Institute of Internal Auditors.

Effective Change Management Process

Process Maturity	Change Management Metric
Low	▪ Number of changes to Oracle EBS authorized over a specific period ▪ Number of changes implemented to Oracle EBS over a specific period ▪ Change success rate (percentage of changes that did not cause issues or unplanned work) ▪ Number of emergency changes to Oracle EBS (including patches)
Medium	▪ Average duration from security patch release date until security patch is applied to Oracle EBS application and database ▪ Number of unauthorized changes that circumvent the documented change process (partial)
High	▪ Number of unauthorized changes that circumvent the documented change process (full population) ▪ Percentage of DBA, developer, and business analyst time spent on unplanned work

Oracle EBS Effective Change Management Controls

Type	Details	Observations/Suggestions
Preventative	Access controls are built to restrict access to only those that are authorized to make changes Segregation of Duties between development, test, and production	Use Integrigy AppSentry to test regularly
Detective	Monitoring / advanced audit trail is enabled for all activities you would expect to go through the change management process	Most organizations don't have this type of monitoring enabled
Corrective	Review of audit logs are done on a periodic basis (how often is based on access controls and risks). Testing for unapproved changes are done; root cause analysis is performed where unapproved changes are identified; corrective actions are taken	Most organizations don't have this type of quality assurance over their change management process

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

This is a partial list for demonstration purposes only

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

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**

Oracle 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 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.)**

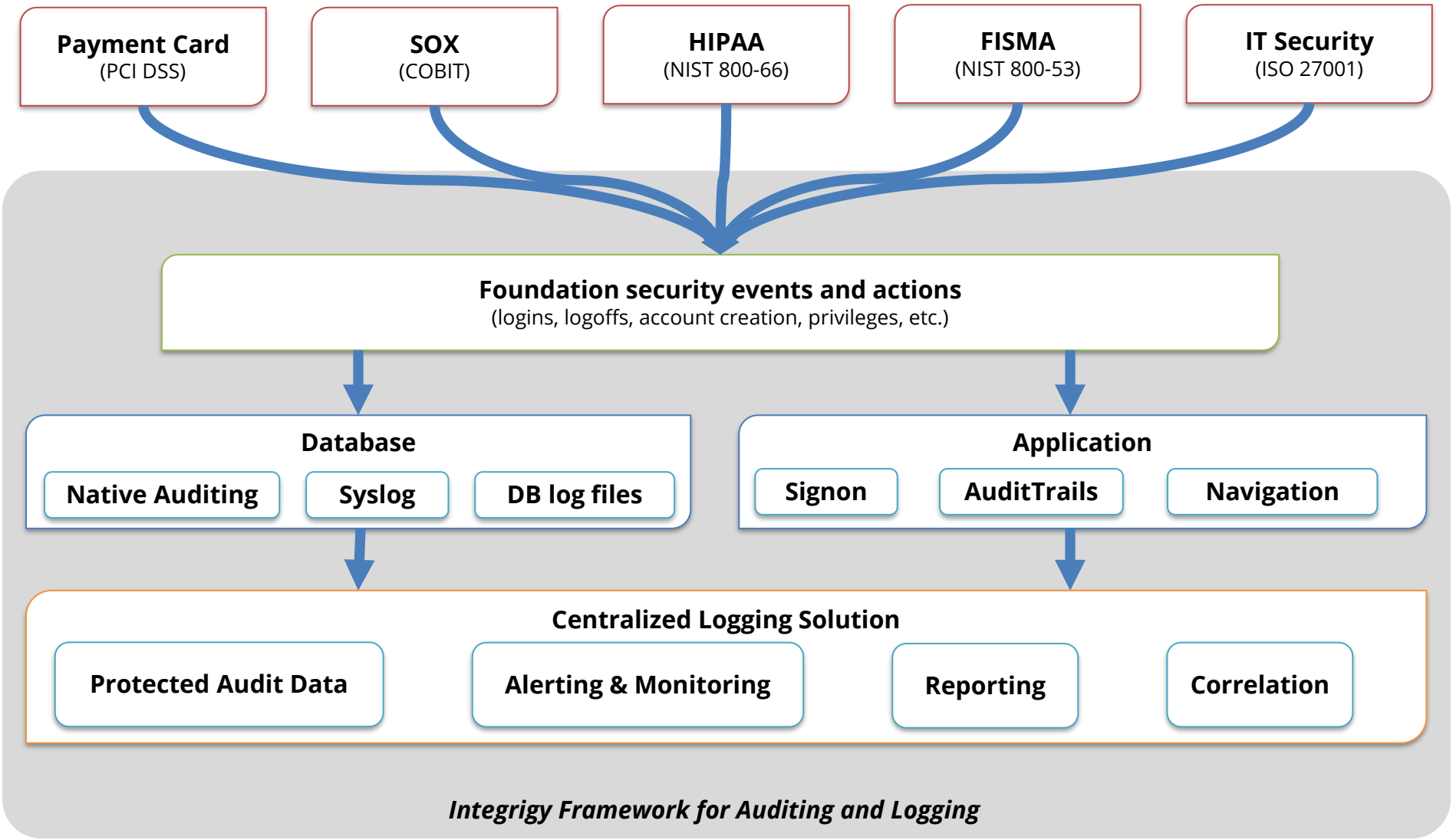
Change Management Challenges

- 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

Agenda

1. Integrigy Security Framework for Oracle E-Business Suite
2. Access Management
3. Sensitive Data Protection
4. DevSecOps
5. **Anomaly and Event Management**

Integrigy Framework for Database Auditing



Integrigy Framework for Auditing and Logging

Foundation Security Events and Actions

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.

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

Foundation Security Events Mapping

Security Events and Actions	PCI DSS 10.2	SOX (COBIT)	HIPAA (NIST 800-66)	IT Security (ISO 27001)	FISMA (NIST 800-53)
E1 - Login	10.2.5	A12.3	164.312(c)(2)	A 10.10.1	AU-2
E2 - Logoff	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E3 - Unsuccessful login	10.2.4	DS5.5	164.312(c)(2)	A 10.10.1 A.11.5.1	AC-7
E4 - Modify authentication mechanisms	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E5 – Create user account	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E6 - Modify user account	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E7 - Create role	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E8 - Modify role	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E9 - Grant/revoke user privileges	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E10 - Grant/revoke role privileges	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E11 - Privileged commands	10.2.2	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E12 - Modify audit and logging	10.2.6	DS5.5	164.312(c)(2)	A 10.10.1	AU-2 AU-9
E13 - Objects Create/Modify/Delete	10.2.7	DS5.5	164.312(c)(2)	A 10.10.1	AU-2 AU-14
E14 - Modify configuration settings	10.2.2	DS5.5	164.312(c)(2)	A 10.10.1	AU-2

Event Management Database Layered Design (Sample)

All Databases

Common Events

Database Events
- Database logins
- Database logoffs
- Failed database logins
- Database configuration changes

Security Events
- Create/Update/Delete User
- Grants and Revokes
- Security profile changes
- SQL Errors (defined list)

Anomalous and Intrusion Detection
- Defined anomalous events
- Known security vulnerabilities

DAM Events and Activity
- User logins and activity
- Security changes
- Infrastructure alerts

Compliance DBs

Compliance Events

SOX
- Database object changes
- Privileged account access by global list of accounts

PCI
- Requirement 10.2
- Access to card data in global list of tables
- Privileged account access by global list of accounts

GLBA
- Privileged account access by global list of accounts

HIPAA
- Privileged account access by global list of accounts
- Access to HIPAA data based on global list of tables

Per Database

Per Database Events (defined during database on-boarding)

Access to SHR/Confidential Data
- Tables and columns containing SHR/Confidential Data
- Select, Insert, Update, and/or Delete based on requirements

Privileged Account Access
- Definition of accounts per application or database
- Exceptions to monitoring based on location or type of access

Event Management Database Layered Design (Sample)

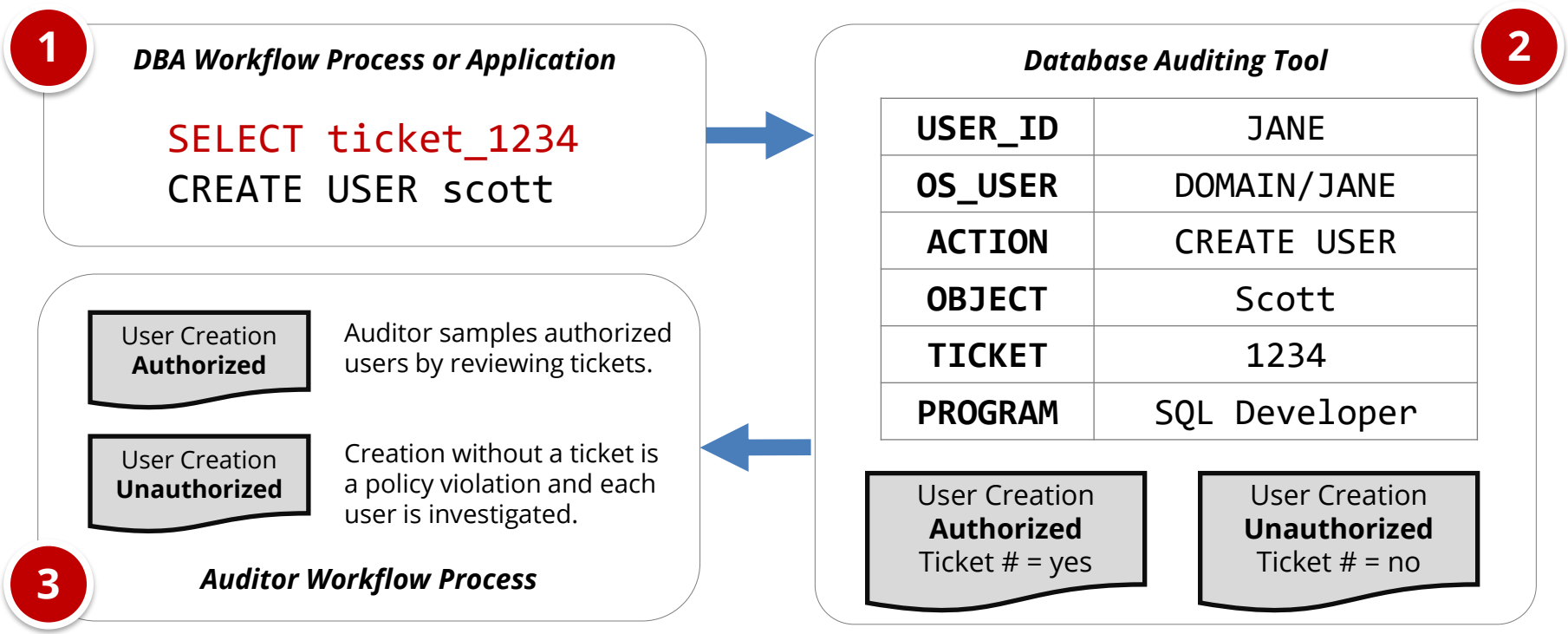
Common Events

Security Events	Database Events	SOX Events and Reports	Guardium Events and Activity
▪ All database sessions ▪ All failed database logins ▪ All application sessions ▪ All failed application logins	▪ SQL errors ▪ SQL errors by EBS end-user	▪ Database user changes ▪ Database user password changes ▪ System privileges and roles changes	▪ User logins and activity ▪ Security changes ▪ DAM infrastructure alerts

	EBS End-User	EBS Batch	PPM	APPS DBA	All Other
Overview	All end-user application SQL is ignored, except specific statements/objects for select users.	All concurrent requests SQL is ignored.	PPM will tag all DDL/DML with PPM ticket number.	All APPS DDL/DML performed by DBAs for manual changes, patching, and maintenance.	All DDL/DML for all other database users, including standard Oracle DB, Oracle EBS, and individual database accounts.
Capture/Filter	DB User: APPS Source: App Servers App User: Set and (not GUEST or SYSADMIN) App: FRMWEB, …	DB User: APPS Source: CM Servers App: STANDARD, …	DB User: APPS Source: PPM Server <u>Additional Capture</u> PPM Package # Package Deployer	DB User: APPS Source: Not filtered prior <u>Operating System ID</u> UNIX user chain	DB User: All other ▪ Oracle – SYS, SYSTEM, … ▪ Oracle EBS – APPLSYS, APPLSYSUB, 300+ module ▪ Other – SSO, … <u>Operating System ID</u> UNIX user chain
Alerts/Reporting	SYSADMIN Logins SYSADMIN Activity Summary SYSADMIN Activity Detail GUEST Errors/SQL Injection GUEST Large Queries	None	All-PPM-No Ticket All-PPM-With Ticket	DBA APPS Logins DBA APPS Usage Summary DBA APPS Usage Detail DBA-Changes Window DBA-Changes Ad-hoc Unauth APPS Use Summary Unauth APPS Use Details	All-DB Logins All-DB Usage Summary All-DB Usage Detail Unath APPLSYSPUB Use Non-App/Non-DBA DDL/DML

Change Ticket Tracking – Create User Example

Auditing tools are able to capture ticket numbers and other information for a database session based on special SQL executed by database users or applications.



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

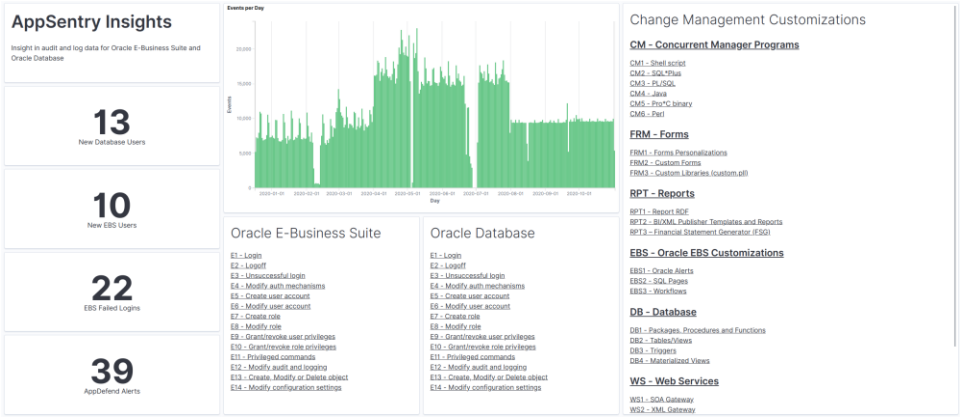
- One-step configuration – a database account
- Pre-configured dashboards, reports, and alerts optimized for Oracle EBS and Oracle Database
- Automatic discovery of Oracle EBS audit and log data locations
- Validation of organizational policy and best practice audit and log configuration

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)



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**