
# Identifying Security Vulnerabilities in Oracle E-Business Suite Customizations

April 21, 2022

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**

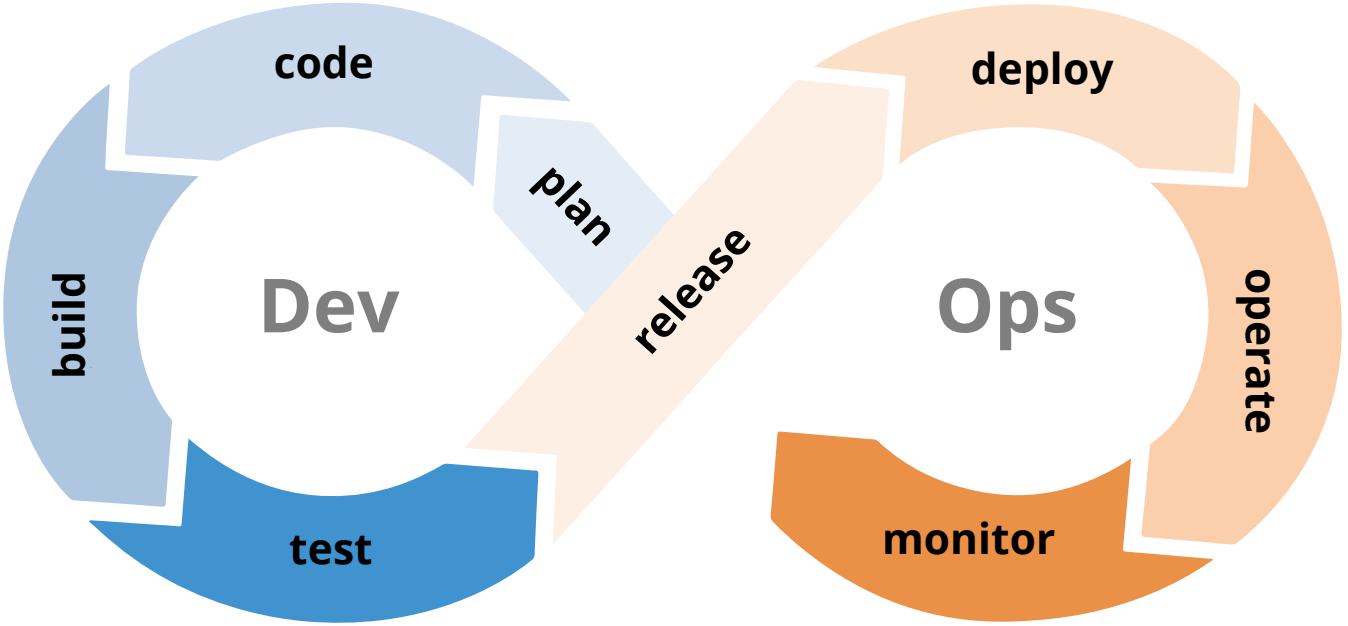
Auditing, Encryption, DMZ

**Integrigy Research Team**

ERP Application and Database Security Research

ORACLE Gold Partner

# What are “DevOps” and “DevSecOps”?




| | |
|---|---|
| **DevOps** | **Development – Operations**<br>▪ Software Development and IT Operations philosophies, practices, and tools to accelerate development, provide continuous delivery, and improve software quality |
| **DevSecOps** | **Development – Security – Operations**<br>▪ 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** | 2.2 |
| **Cross-Site Scripting (XSS)** | 0.6 |
| **XML Issues** (e.g., XML entity attacks) | 0.3 |
| **APPS Password Issues** | 1.7 |
| **Authorization/Authentication Issues** | 2.8 |
| **Other Issues** | 1.2 |

Source – Integrigy Customization Assessments 2018 – 2021

# Oracle E-Business Suite DevSecOps Challenges

| | |
|---|---|
| **Highly Complex Application Environment** | ▪ Web, application, and database development<br>▪ 886 security vulnerabilities have been patched in Oracle code between 2005 and 2021 – if Oracle can't do it perfectly, can you? |
| **Customization vs Development** | ▪ Development is focused on customizations<br>▪ Each customization is a small development project<br>▪ Pinpoint development objects created in a multiple technologies and languages |
| **Open Development Environment** | ▪ Development is done at multiple layers of the technology stack – web, application, database<br>▪ Some development is done inside the application<br>▪ Easy to have poor version control and weak change management |

# DevSecOps Reality – ERP Staffing Ratios

| **Developers** (Dev) | : | **Operations** (Ops) | : | **IT Security** (Sec) |
|---|---|---|---|---|
| **25** | : | **10** | : | **1** |

Source – Integrigy ERP Security Staffing reviews by hours

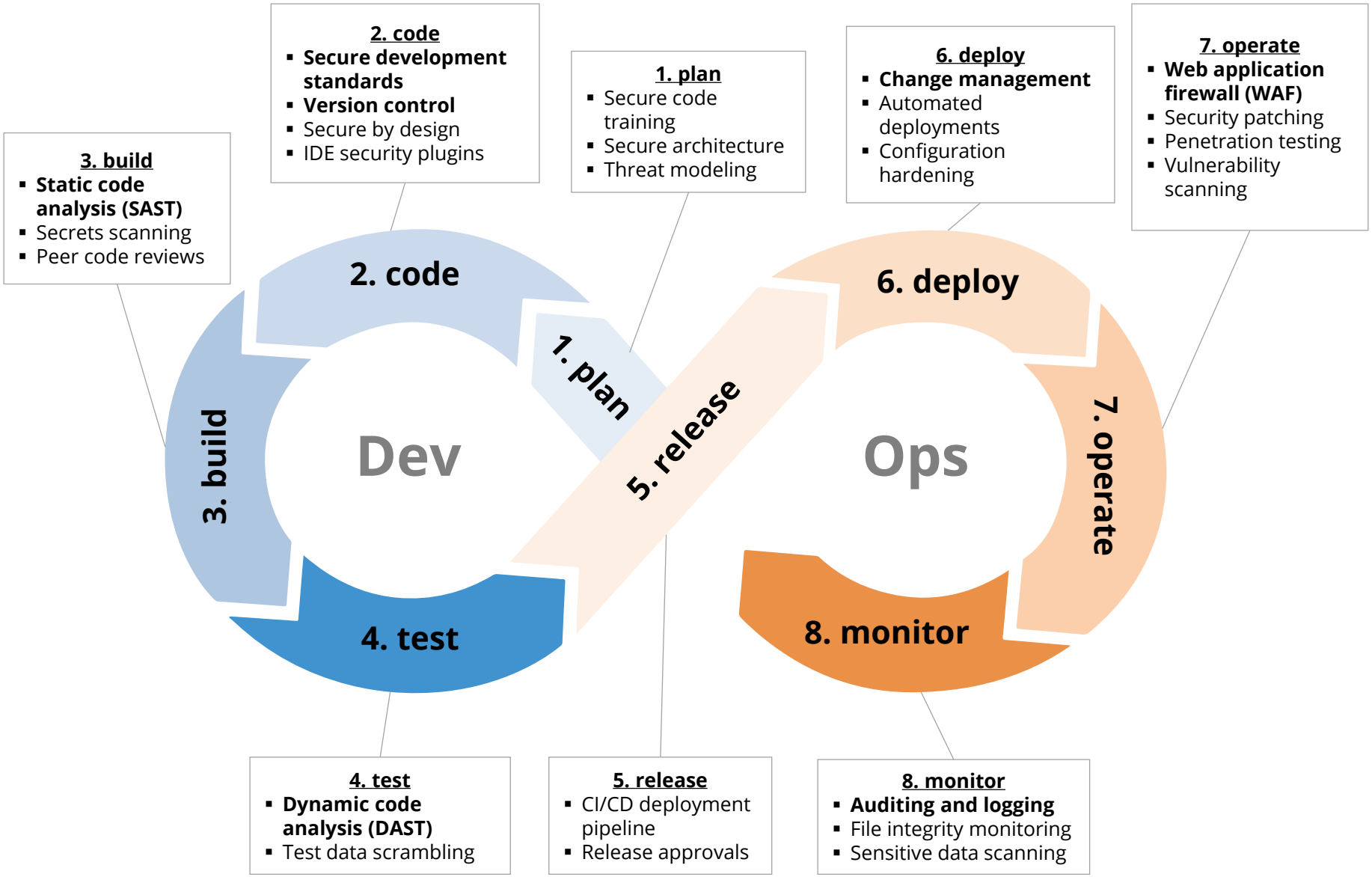
# DevSecOps Principles

| | |
|---|---|
| **Shift Left** | ▪ "Shifting left" is moving security to earlier stages of the development cycle<br>▪ Ensure security standards and best practices are met when code is first developed |
| **Automation** | ▪ Automated code analysis, security testing, and compliance verification<br>▪ 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<br>▪ Security vulnerabilities are fixed immediately early in the development cycle |

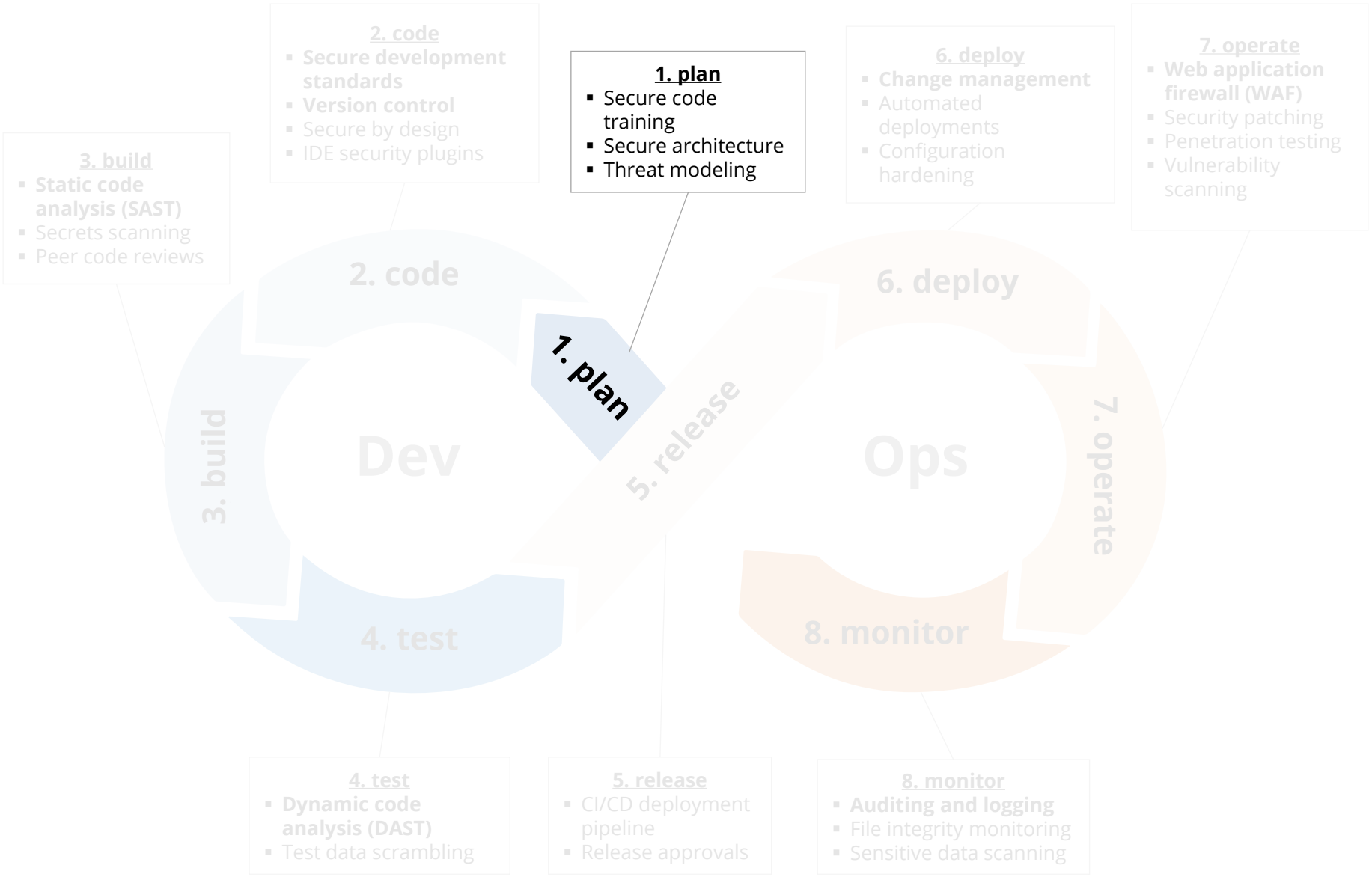
# DevSecOps Benefits

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

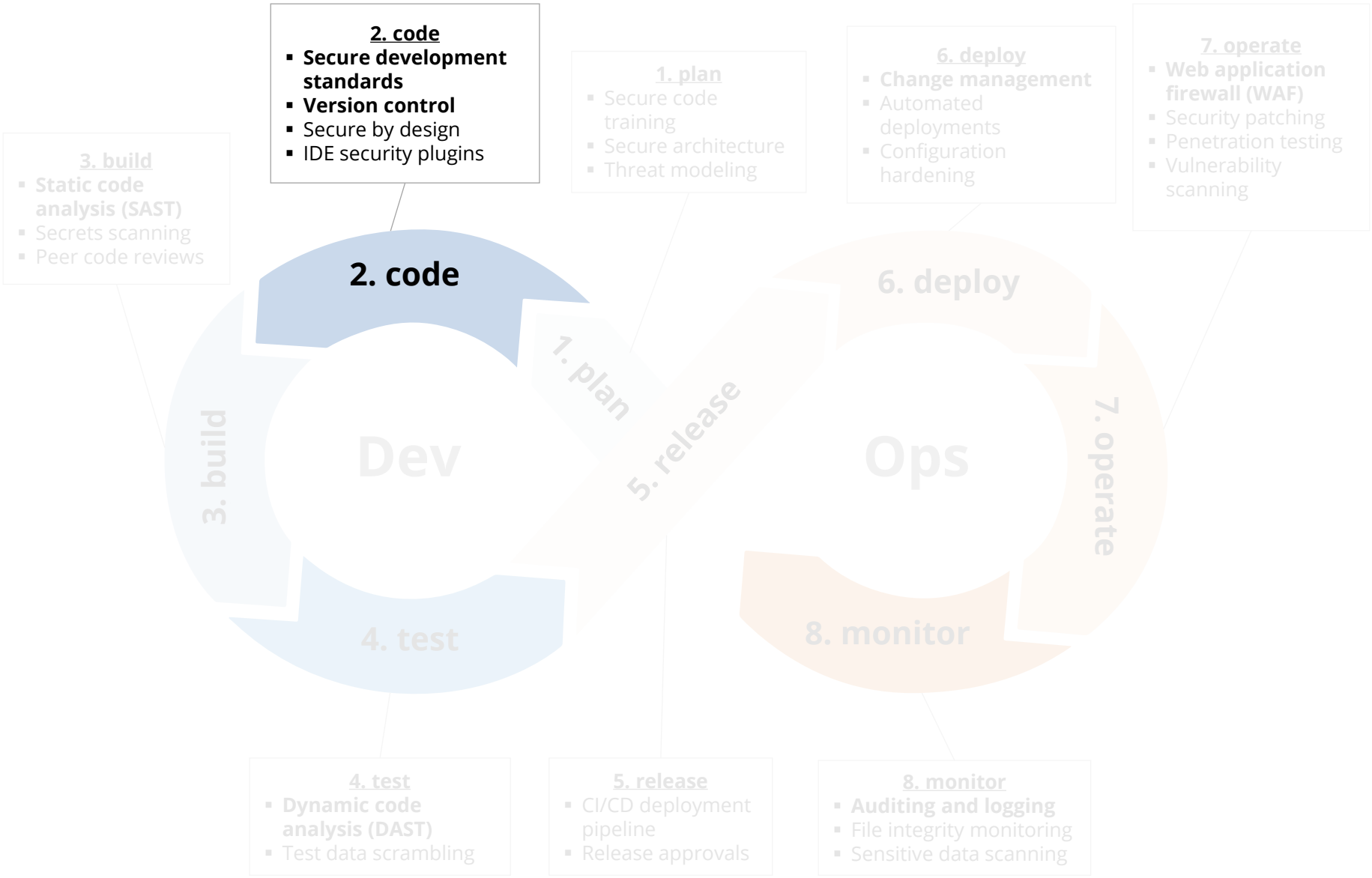
# Oracle E-Business Suite DevSecOps



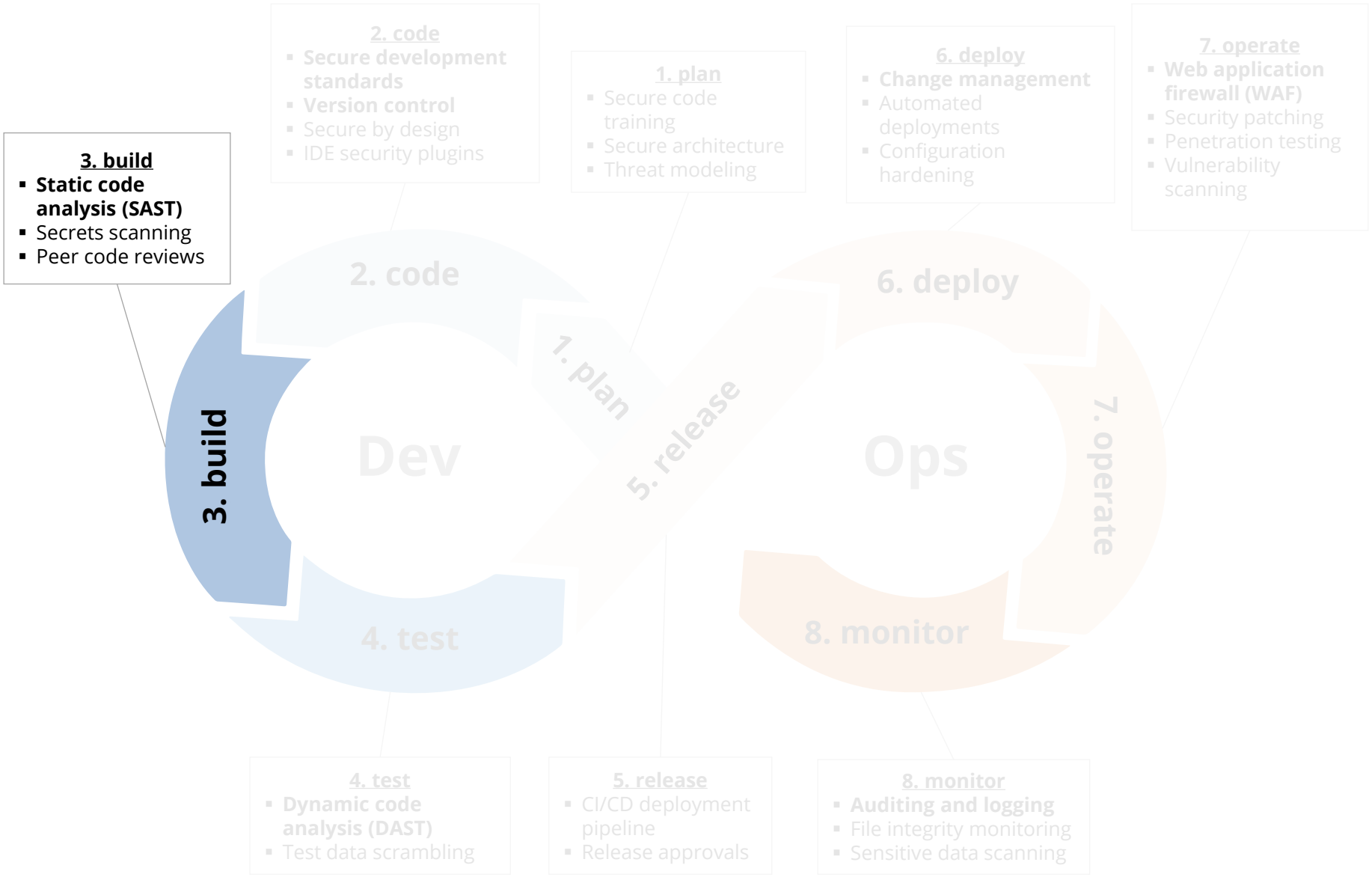
# Oracle E-Business Suite DevSecOps



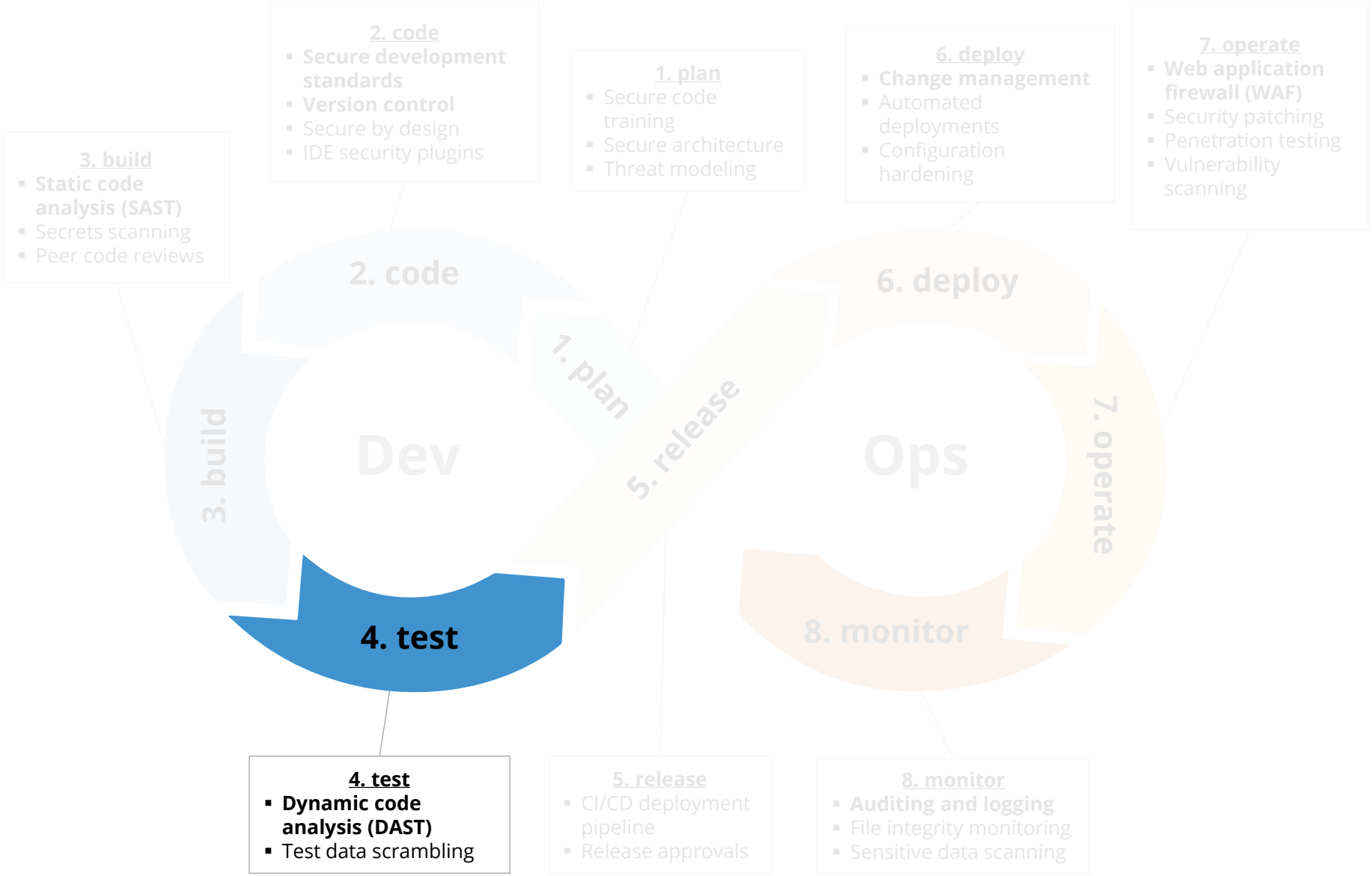
# Oracle E-Business Suite DevSecOps



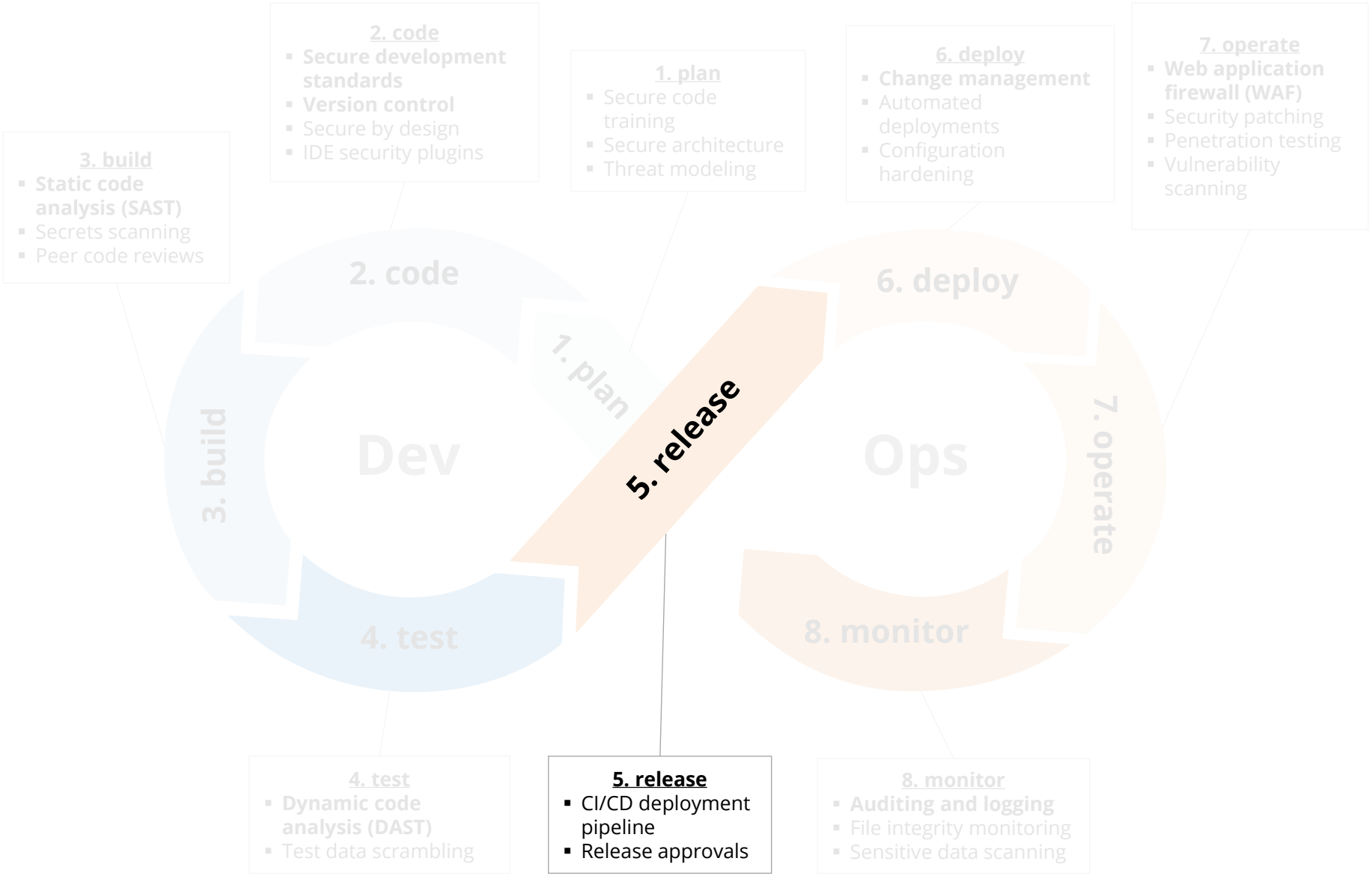
# Oracle E-Business Suite DevSecOps



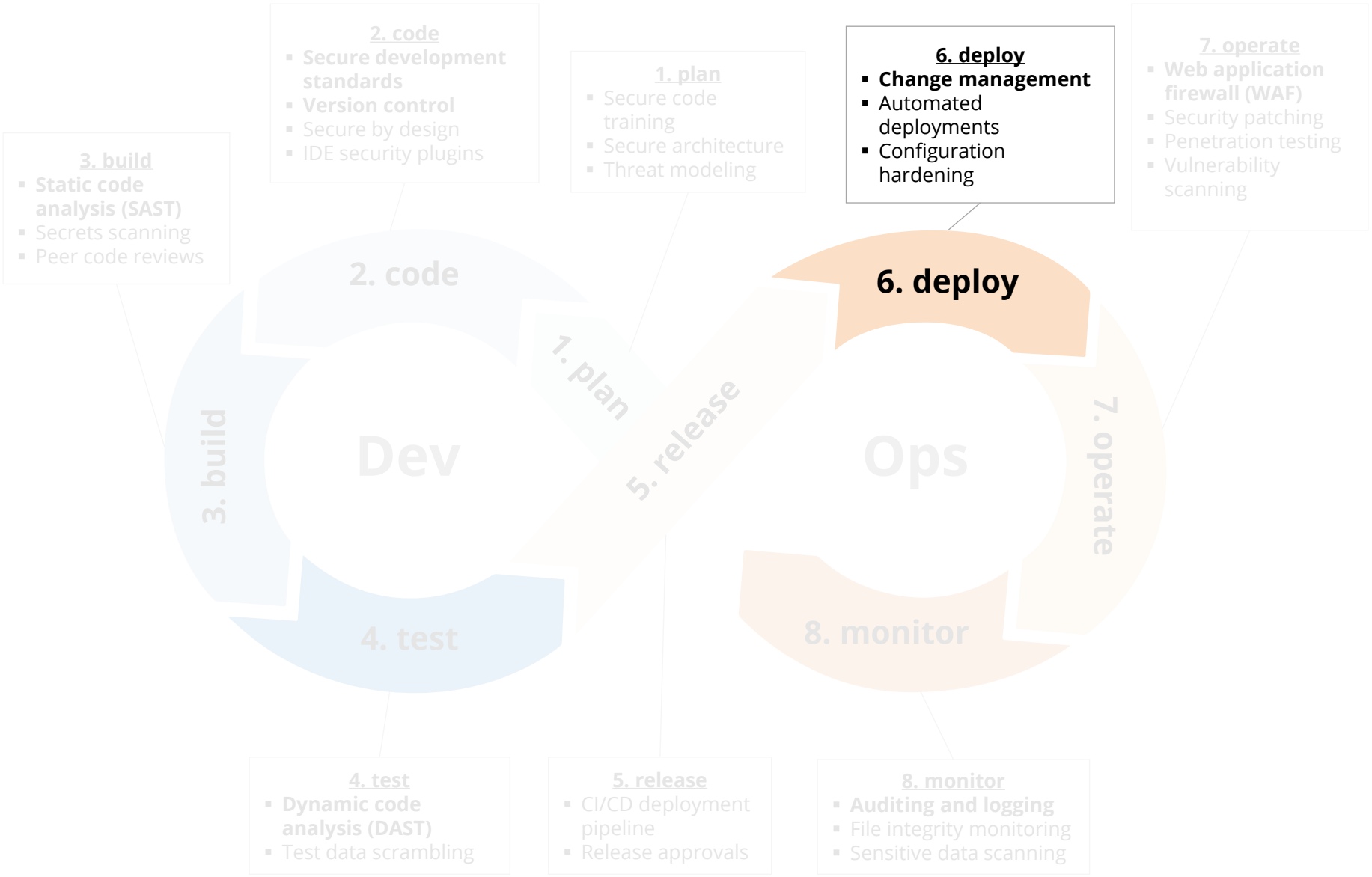
# Oracle E-Business Suite DevSecOps



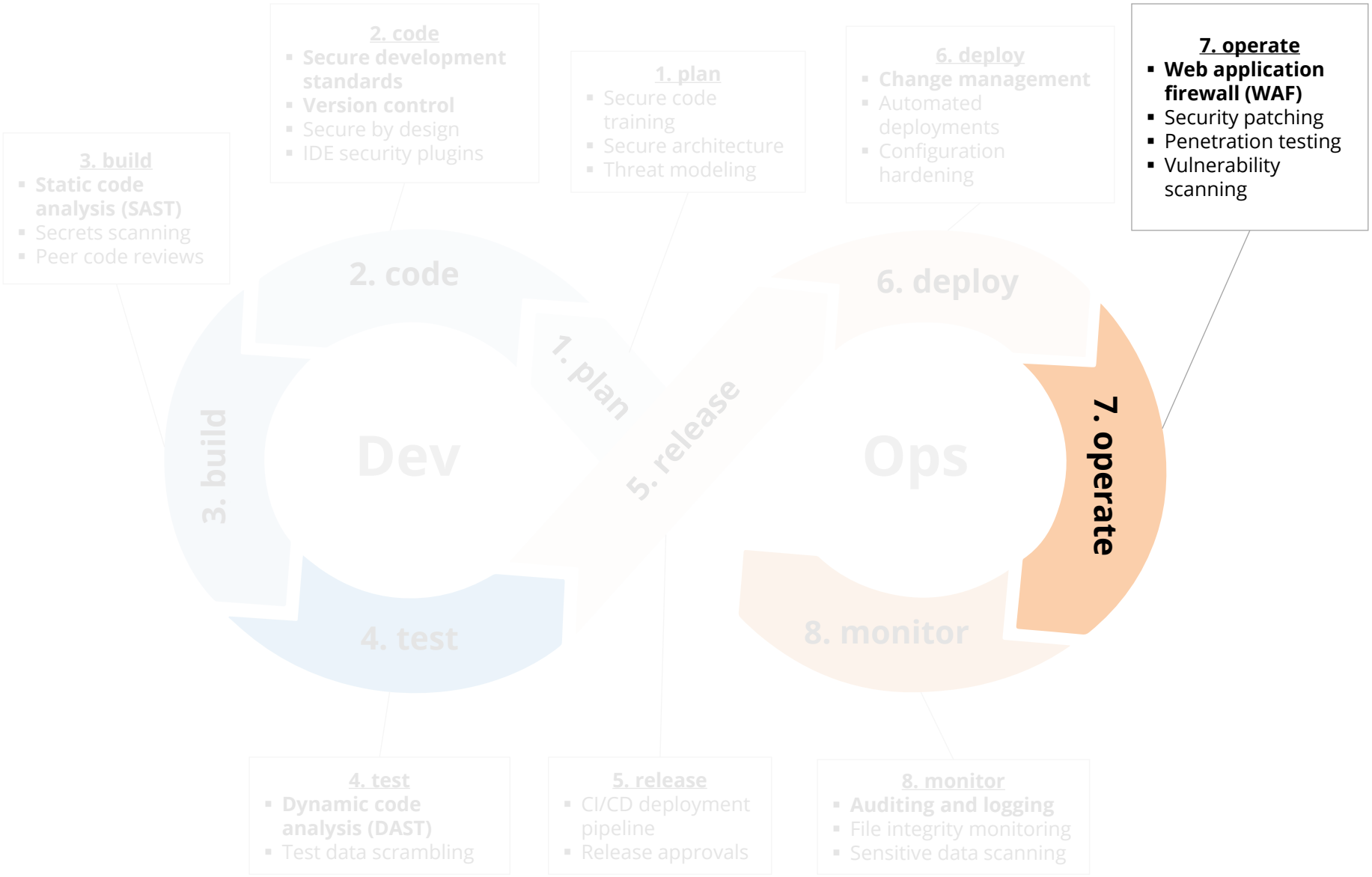
# Oracle E-Business Suite DevSecOps



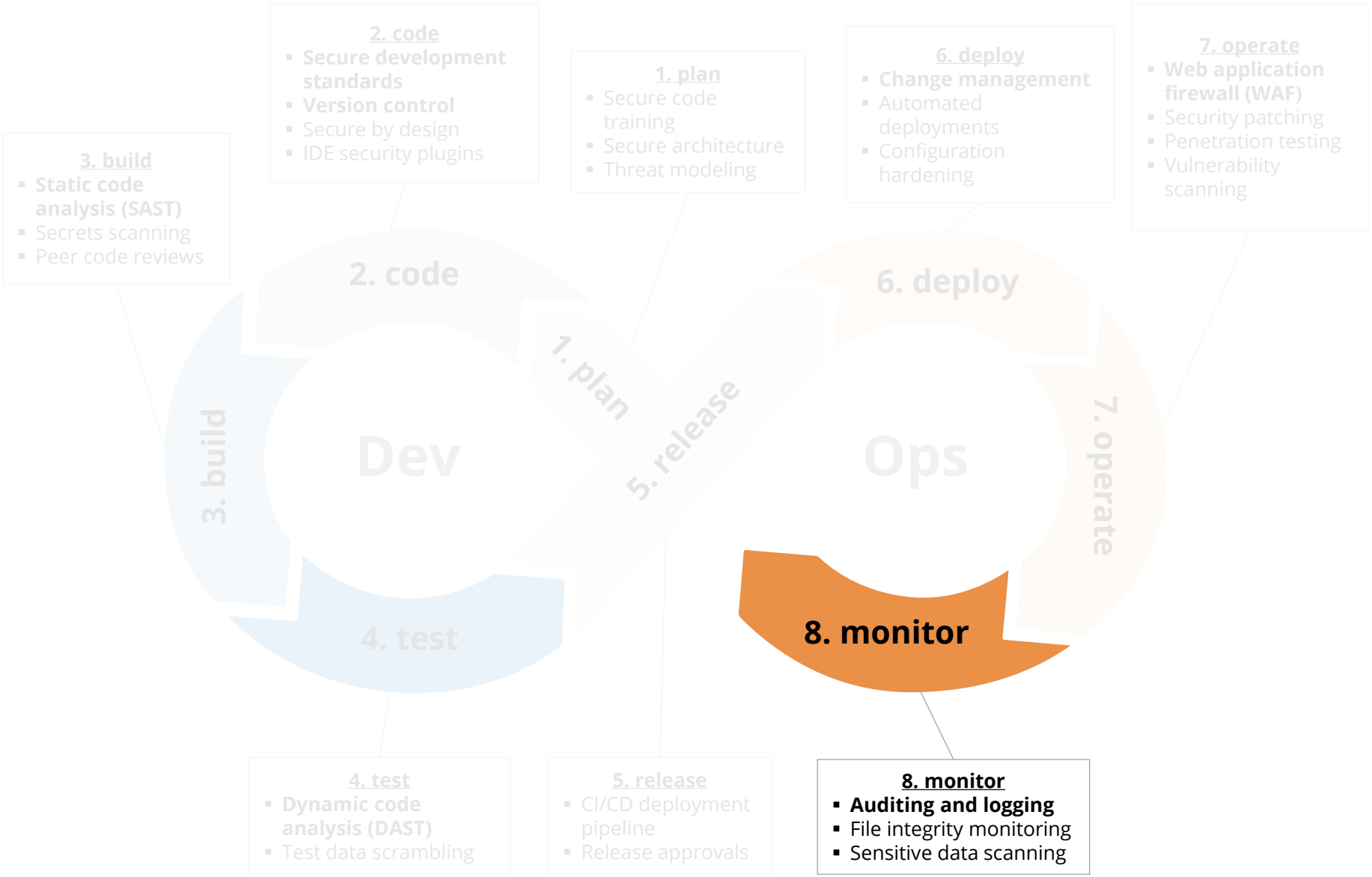
# Oracle E-Business Suite DevSecOps



# Oracle E-Business Suite DevSecOps



# 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)**

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

- **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 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 | PL/SQL | Database | | SQL injection, authorization |
| | FRM2 - Custom Forms | PL/SQL | File (.fm*) | | SQL injection, authorization |
| | FRM3 - Custom Libraries (custom.pll) | PL/SQL | 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<br>File (.xml) | | |
| | WEB5 - Modplsql | PL/SQL | Database | | SQL injection |
| | WEB6 - Application Express (APEX) | SQL | Database<br>File (.sql) | | SQL injection |
| | WEB7 - ADF applications | Java | File (.java) | Yes | SQL injection |
| **Database** | DB1 - Packages, Procedures, and Functions | PL/SQL | Database<br>File (.sql) | Yes | SQL injection, authorization |
| | DB2 - Tables/Views | SQL | Database<br>File (.sql) | | |
| | DB3 - Triggers | SQL | Database<br>File (.sql) | | authorization |
| | DB4 - Materialized Views | SQL | Database<br>File (.sql) | | |
| **Web Services** | WS1 - SOA Gateway | Multiple | Database | Yes | SQL injection, authorization |
| | WS2 - XML Gateway | | Database | | |

# 2. Code

| | |
|---|---|
| **Version Control** | ▪ A version control system such as Git should be used for all custom code that resides on the operating system<br>▪ The DEV environment is not a version control system<br>▪ 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<br>▪ 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<br>▪ JDeveloper supports PMD plugin for Java and PL/SQL security checks |

# 3. Build

| | |
|---|---|
| **SAST (Static Code Analysis)** | ▪ All source code and custom database code (PL/SQL, APEX, etc.) must be periodically scanned for security vulnerabilities<br>▪ Problem with Oracle EBS customizations is that there are at least nine languages that may be used<br>▪ Use tools like PMD (Java, PL/SQL), FindSecBugs, SonarCube, Checkmarx to scan source code repository<br>▪ **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<br>▪ Use a tool such as **AppSentry Code** to scan source code and database for secrets – scan all deployment packages using both regex and entropy<br>▪ Wrapped PL/SQL code may contain DBMS_CRYPTO encryption keys |

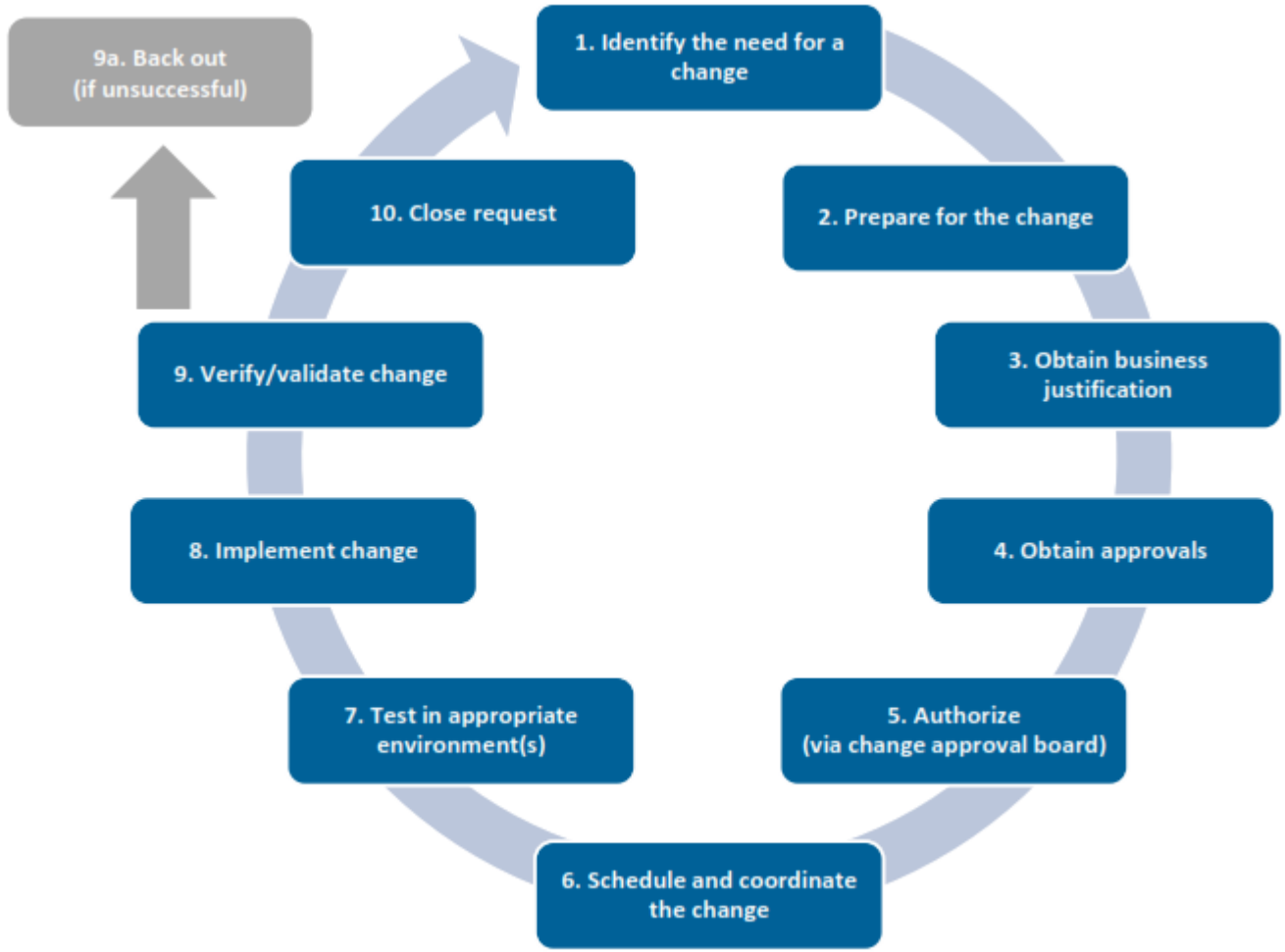
# 6. Deploy

| | |
|---|---|
| **Change Management** | ▪ ALL changes to Oracle EBS production must go through the change management process<br>▪ The organization must clearly define what is an Oracle EBS change<br>▪ Only authorized users may be allowed to make changes or migrate code into production<br>▪ Developers should only have read access to production<br>▪ 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<br>▪ Use the “Secure Configuration Guide for Oracle E-Business Suite” as a starting point<br>▪ Use **AppSentry** to validate the configuration of Oracle EBS, WebLogic, and Oracle Database |

# 7. Operate

| | |
|---|---|
| **Web Application Firewall (WAF)** | ▪ Implement a WAF to protect Oracle EBS from web vulnerabilities such as SQL injection, XSS, Java deserialization<br>▪ General purpose WAFs do not adequately protect Oracle EBS<br>▪ **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<br>▪ 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.<br>▪ Use both periodic automated scanning and in-depth annual manual penetration testing for comprehensive testing<br>▪ **AppSentry** can automate vulnerability assessment and assist with penetration testing |

# 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<br>▪ Number of changes implemented to Oracle EBS over a specific period<br>▪ Change success rate (percentage of changes that did not cause issues or unplanned work)<br>▪ 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<br>▪ Number of unauthorized changes that circumvent the documented change process (partial) |
| **High** | ▪ Number of unauthorized changes that circumvent the documented change process (full population)<br>▪ 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<br><br>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).<br><br>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

# 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**