# Upgrade Security in Your Oracle R12 Upgrade

**Stephen Kost**
**Chief Technology Officer**
**Integrigy Corporation**

**Phil Reimann**
**Director of Business Development**
**Integrigy Corporation**

**January 13, 2011**

INTEGRIGY

# Integrigy Overview

**Integrigy Corporation is a leader in application security for enterprise mission-critical applications. AppSentry, our application and database security assessment tool, assists companies in securing their largest and most important applications through detailed security audits and actionable recommendations. Integrigy Consulting offers comprehensive security assessment services for leading databases and ERP applications, enabling companies to leverage our in-depth knowledge of this significant threat to business operations.**

**Corporate Details**

- Founded December 2001
- Privately Held
- Based in Chicago, Illinois

INTEGRIGY

# Background

## Speaker

### Stephen Kost

- CTO and Founder
- 16 years working with Oracle
- 12 years focused on Oracle security
- DBA, Apps DBA, technical architect, IT security, …

## Company

### Integrigy Corporation

- Integrigy bridges the gap between databases and security
- Security Design and Assessment of Oracle Databases
- Security Design and Assessment of the Oracle E-Business suite
- AppSentry - Security Assessment Software Tool

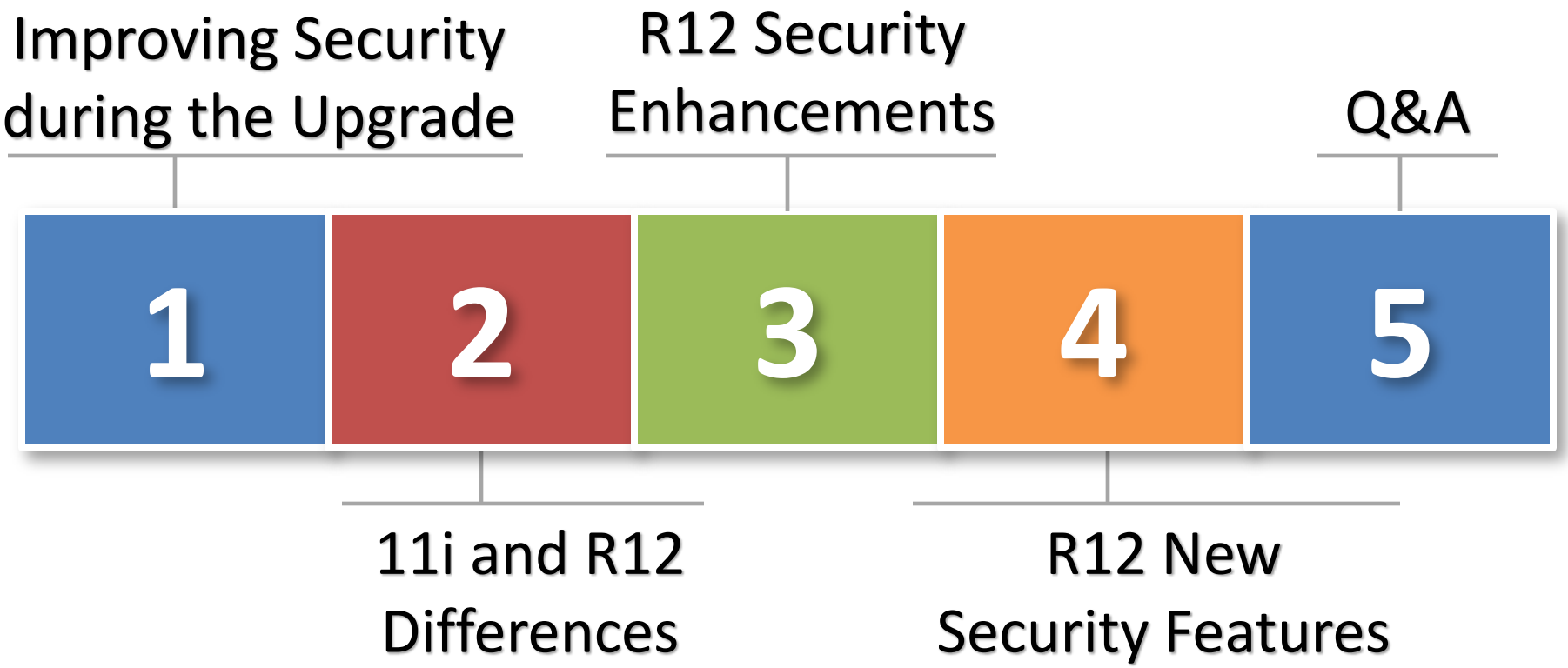
INTEGRIGY

# Integrigy Security Alerts

| Security Alert | Versions | Security Vulnerabilities |
|---|---|---|
| **Critical Patch Update July 2008** | **Oracle 11g**<br>**11.5.8 – 12.0.x** | ▪ 2 Issues in Oracle RDBMS Authentication<br>▪ 2 Oracle E-Business Suite vulnerabilities |
| **Critical Patch Update April 2008** | **12.0.x**<br>**11.5.7 – 11.5.10** | ▪ 8 vulnerabilities, SQL injection, XSS, information disclosure, etc. |
| **Critical Patch Update July 2007** | **12.0.x**<br>**11.5.1 – 11.5.10** | ▪ 11 vulnerabilities, SQL injection, XSS, information disclosure, etc. |
| **Critical Patch Update October 2005** | **11.5.1 – 11.5.10**<br>**11.0.x** | ▪ Default configuration issues |
| **Critical Patch Update July 2005** | **11.5.1 – 11.5.10**<br>**11.0.x** | ▪ SQL injection vulnerabilities<br>▪ Information disclosure |
| **Critical Patch Update April 2005** | **11.5.1 – 11.5.10**<br>**11.0.x** | ▪ SQL injection vulnerabilities<br>▪ Information disclosure |
| **Critical Patch Update Jan 2005** | **11.5.1 – 11.5.10**<br>**11.0.x** | ▪ SQL injection vulnerabilities |
| **Oracle Security Alert #68** | **Oracle 8i, 9i, 10g** | ▪ Buffer overflows<br>▪ Listener information leakage |
| **Oracle Security Alert #67** | **11.5.1 – 11.5.8**<br>**11.0.x** | ▪ 10 SQL injection vulnerabilities |
| **Oracle Security Alert #56** | **11.5.1 – 11.5.8**<br>**11.0.x** | ▪ Buffer overflow in FNDWRR.exe |
| **Oracle Security Alert #55** | **11.5.1 – 11.5.8** | ▪ Multiple vulnerabilities in AOL/J Setup Test<br>▪ Obtain sensitive information (valid session) |
| **Oracle Security Alert #53** | **10.7, 11.0.x**<br>**11.5.1 – 11.5.8** | ▪ No authentication in FNDFS program<br>▪ Retrieve any file from O/S |

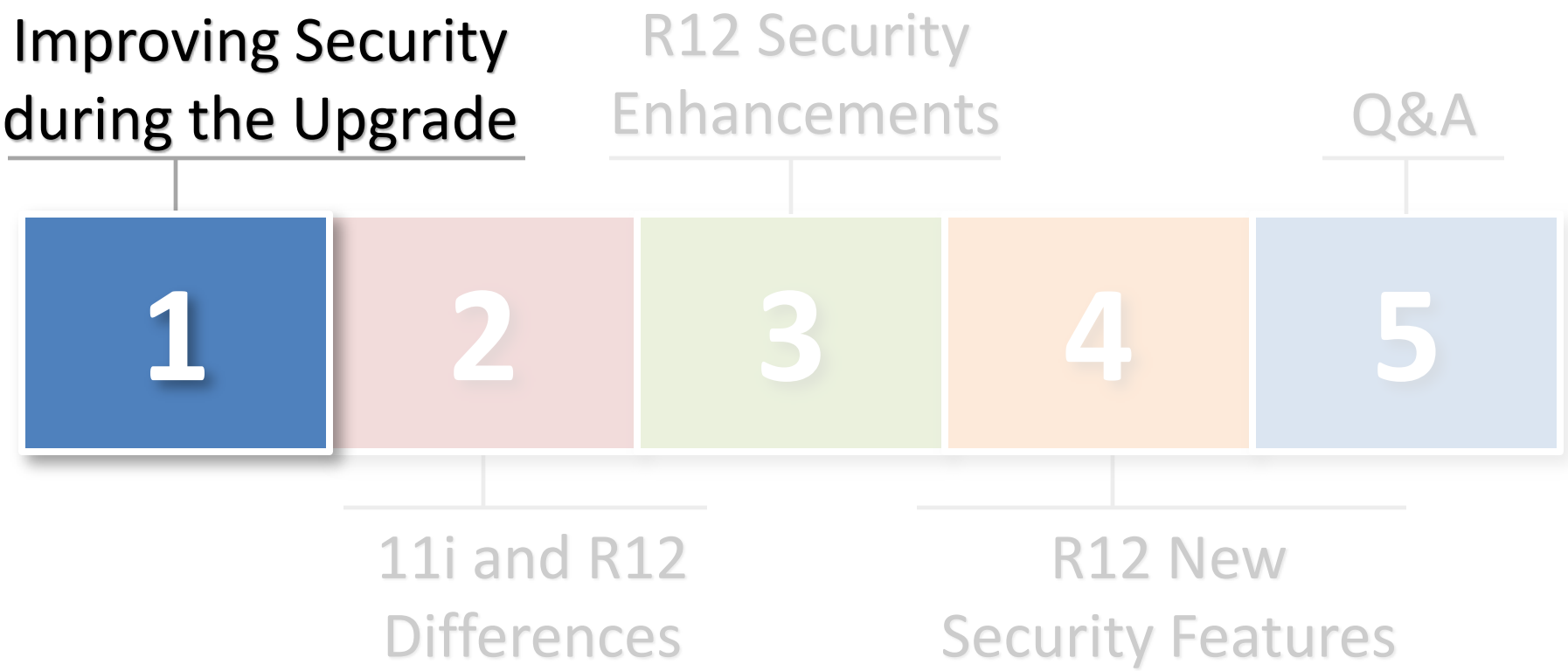
INTEGRIGY

# Agenda




INTEGRIGY

# Agenda




INTEGRIGY

# Why do “Security” during the upgrade?

## 1 Technology Stack Upgrades

- New version = new security features
- Reset of security patching – should be current at go-live

## 2 Functional, Technical, & Stress Testing

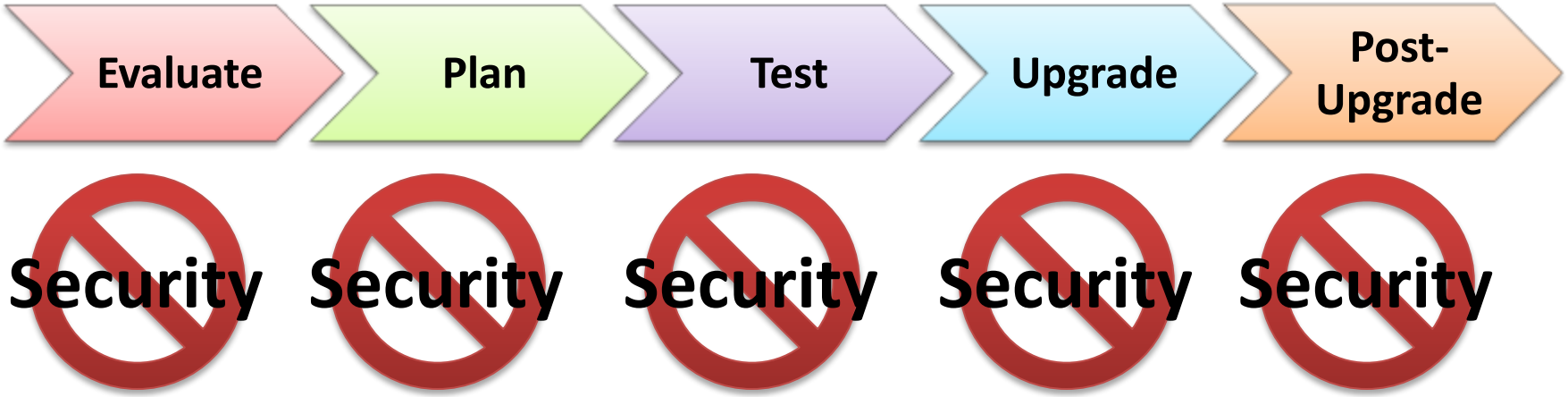
- Functional application testing
- Performance and stress testing

## 3 Modifications to Customizations

- Some or many customizations must be upgraded
- Ideal time to review development standards

INTEGRIGY

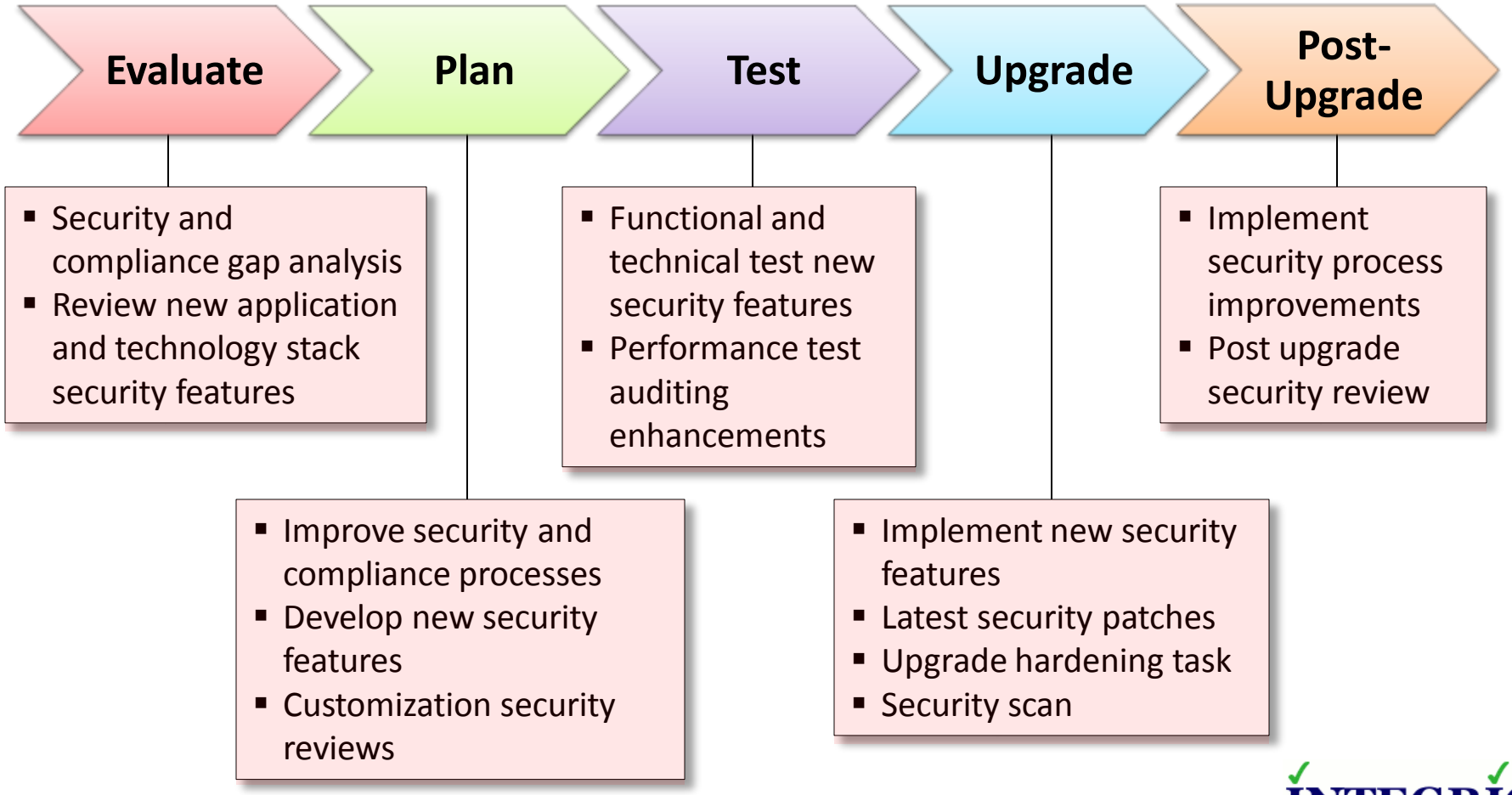
# Traditional R12 Upgrade Project




INTEGRIGY

# Security “Aware” R12 Upgrade Project

**Goal: High security value, low project effort, major testing required, low project risk**




INTEGRIGY

# Example Upgrade Security Enhancements

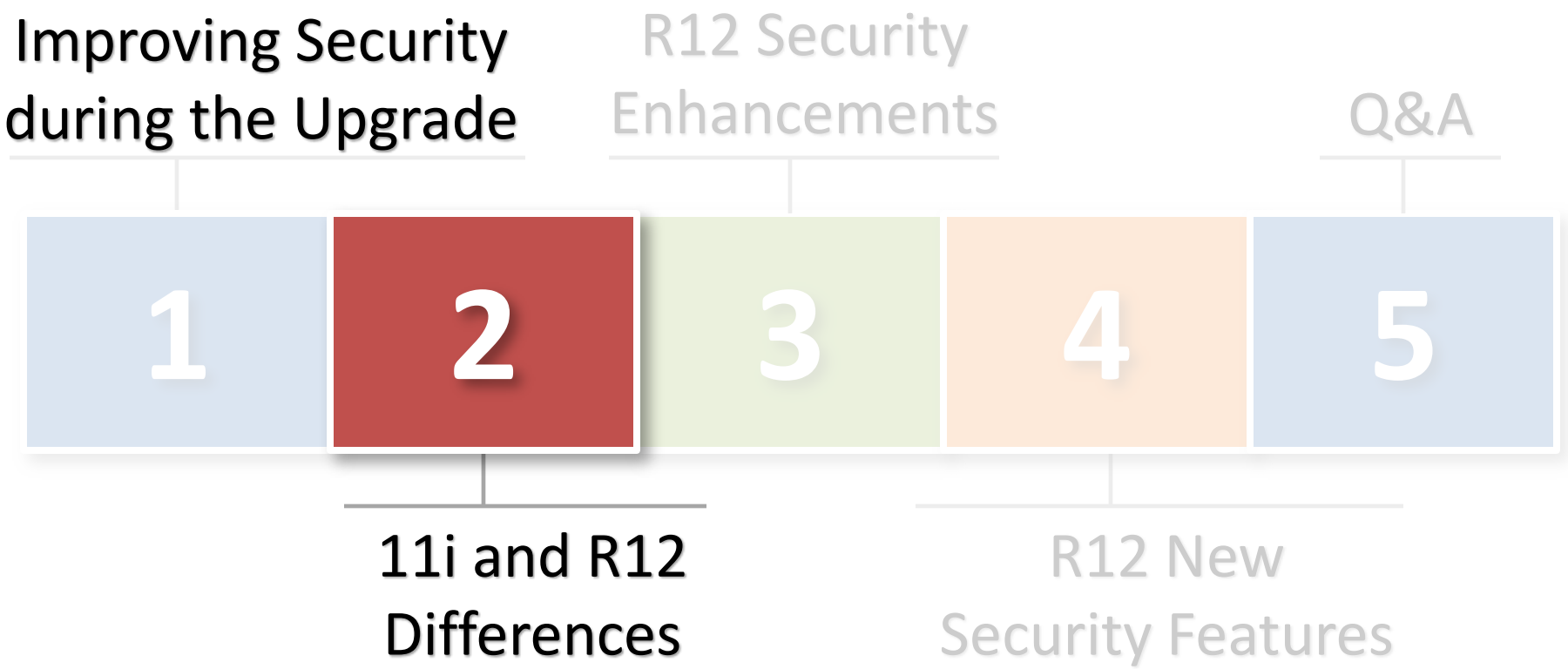
| Security Enhancement | Security Value | Project Effort | Testing Required | Project Risk |
|---|---|---|---|---|
| **Restricted Database Access** | High | Medium | High | Medium |
| **Auditing** | High | Low | Medium | Low |
| **Encryption** | High | Low | High | Medium |
| **Security Patches** | High | Low | Medium | Low |
| **Security Hardening** | Medium | Low | Medium | Low |
| **Database Access Controls** | Medium | Medium | Medium | Low |
| **Data Scrambling** | Medium | Low | Low | Low |
| **Single Sign-on** | Low | High | High | High |

INTEGRIGY

# R12 Upgrade Impacted Security Processes

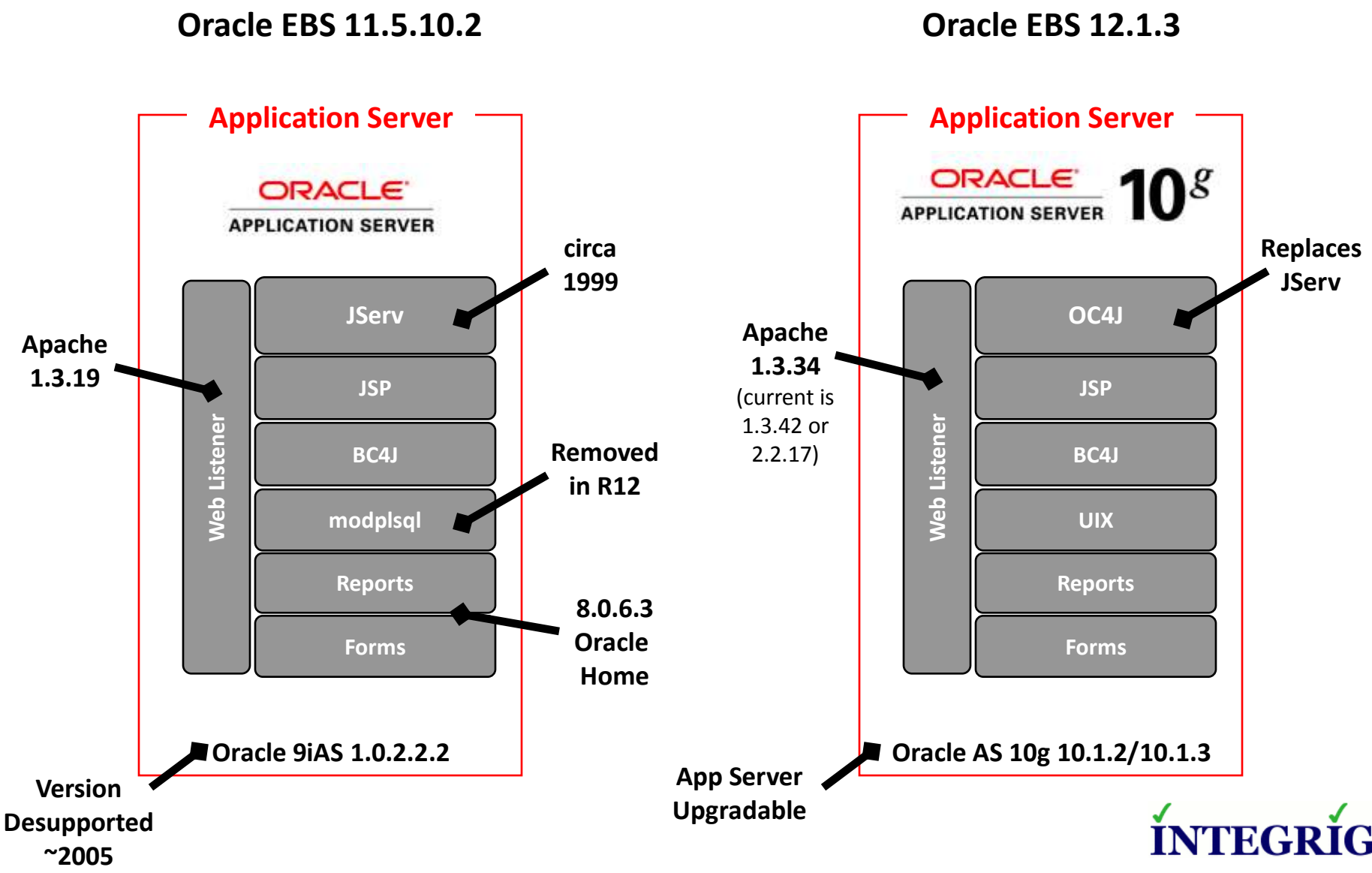
| Operational Processes | Oracle Applications Technical Components | | | |
|---|---|---|---|---|
| | Oracle Applications | Database | Application Server | Operating System |
| 1. Account Security | 1.1 User Management | 1.3 Database Security | 1.4 Network and Web | 1.5 OS Security |
| | 1.2 Segregation of Duties | | | |
| 2. Data Security | 2.1 Data Management and Privacy | 2.2 Database Access and Privileges | 2.3 Web Access | 2.4 File Permissions |
| 3. Auditing | 3.1 Application Auditing | 3.2 Database Auditing | 3.3 Web Logging | 3.4 OS Auditing |
| 4. Monitoring and Troubleshooting | 4.1 Application | 4.2 Database | 4.3 Web and Forms | 4.4 Operating System |
| 5. Change Management | 5.1 Object Migrations | 5.3 Change Control | 5.5 Change Control | 5.6 Change Control |
| | 5.2 Application Configuration | 5.4 Database Configuration | | |
| 6. Patching | 6.1 Application Patches | 6.2 Database Patches | 6.3 Application Server Patches | 6.4 OS Patches |
| 7. Development | 7.1 Application | 7.2 Database | 7.3 Web | 7.5 Shell and File Transfer |
| | | | 7.4 Web Services and SOA | |

# Agenda




INTEGRIGY

# 11i/R12 Architecture Differences




INTEGRIGY

# 11i/R12 Architecture Differences

- **Oracle Database Upgrade**
  - 9.2/10.2 replaced with 11.2
  - 11.2 has TDE tablespace encryption
- **Oracle Jinitiator -> Sun JRE**
  - Improved support and standardization
- **mod_plsql retired**
  - Significant security vulnerabilities historically
  - Allowed direct execution of PL/SQL packages in database
- **Forms Server -> Forms Listener Servlet**
  - All network traffic through Apache server – no standalone port
- **Oracle Reports -> XML Publisher**
  - Improved security model and features

# Critical Patch Updates

- **R12 Critical Patch Updates are cumulative**
  - 11i introduced cumulative patches with January 2010 CPU

| Database Version Upgrade Patch | Included CPU |
|---|---|
| 10.2.0.4 | April 2008 |
| 11.1.0.6 | October 2007 |
| 11.1.0.7 | January 2009 |
| 11.2.0.1 | January 2010 |
| 11.2.0.2 | January 2011 |

| EBS Version | Included CPU |
|---|---|
| 12.0.6 | October 2008 |
| 12.1.1 | April 2009 |
| 12.1.2 | October 2009 |
| 12.1.3 | January 2011 |

# R12 Application Users Added

- **New application accounts from 12.0.0 onward**
  - INDUSTRY DATA
  - ORACLE12.0.0
  - ORACLE12.1.0
  - ORACLE12.2.0
  - ORACLE12.3.0
  - ORACLE12.4.0
  - ORACLE12.5.0
  - ORACLE12.6.0
  - ORACLE12.7.0
  - ORACLE12.8.0
  - ORACLE12.9.0
- **All are active accounts with invalid passwords**

# Database Accounts Added

- **A new database account is added for each new product module**
  - Partial list of new module database accounts:

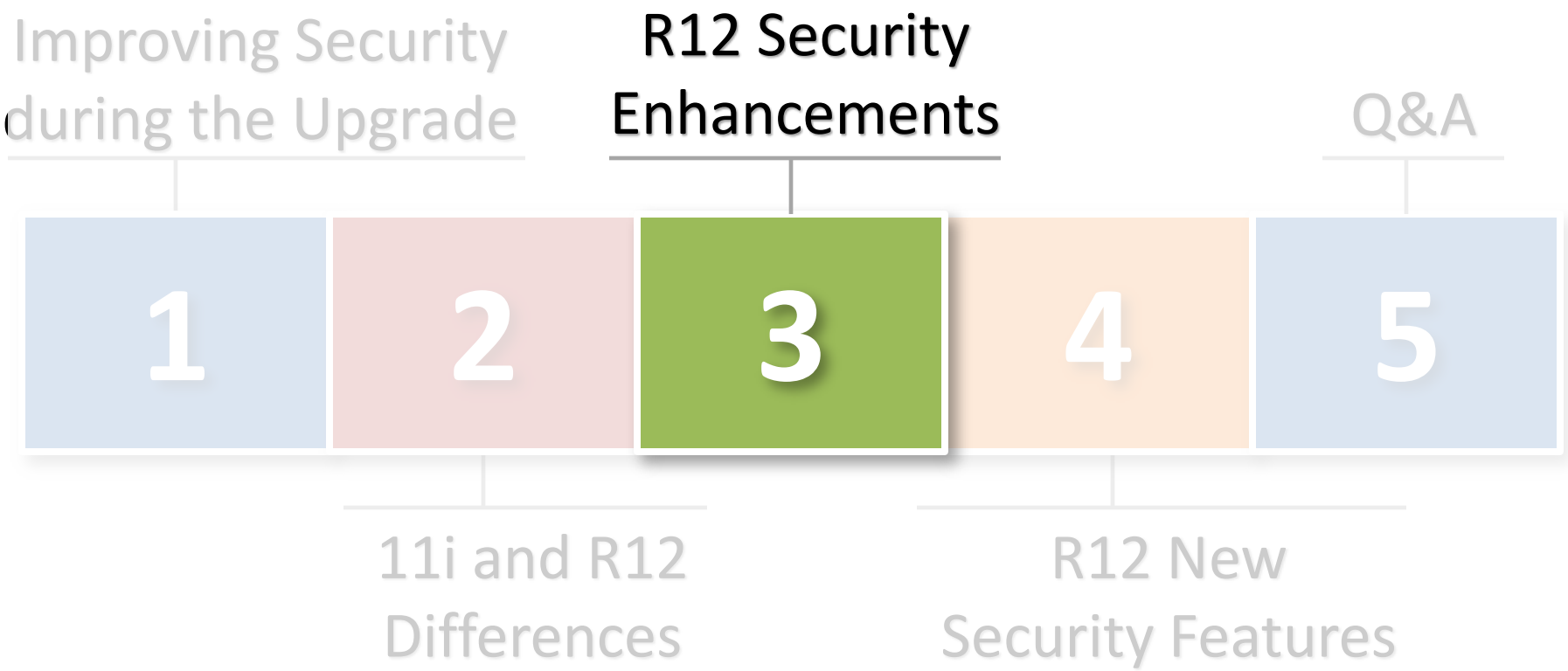
**CA, DDR, DNA, DPP, FTP, GMO,**

**IBW, INL, IPM, ITA, JMF, MTH,**

**PFT, QPR, RRS,**

INTEGRIGY

# Agenda




INTEGRIGY

# Protecting Database Accounts

- **Oracle 11g case sensitive passwords (12.1 only)**
  - SEC_CASE_SENSITIVE_LOGON = TRUE
  - APPLSYSPUB must always be uppercase
- **Use AFPASSWD rather than FNDCPASS**
  - **Lock Products Schema Accounts**
    > AFPASSWD –L TRUE
  - Improved separation of duties
  - Fewer errors changing password with password confirmation entry
  - *See R12 SAG – Configuration*
- **Change the APPLSYSPUB password**
  - Finally works in R12 and supported by Oracle
  - Also make sure the password is changed in AutoConfig

INTEGRIGY

# Web Server Traffic Encryption (SSL)

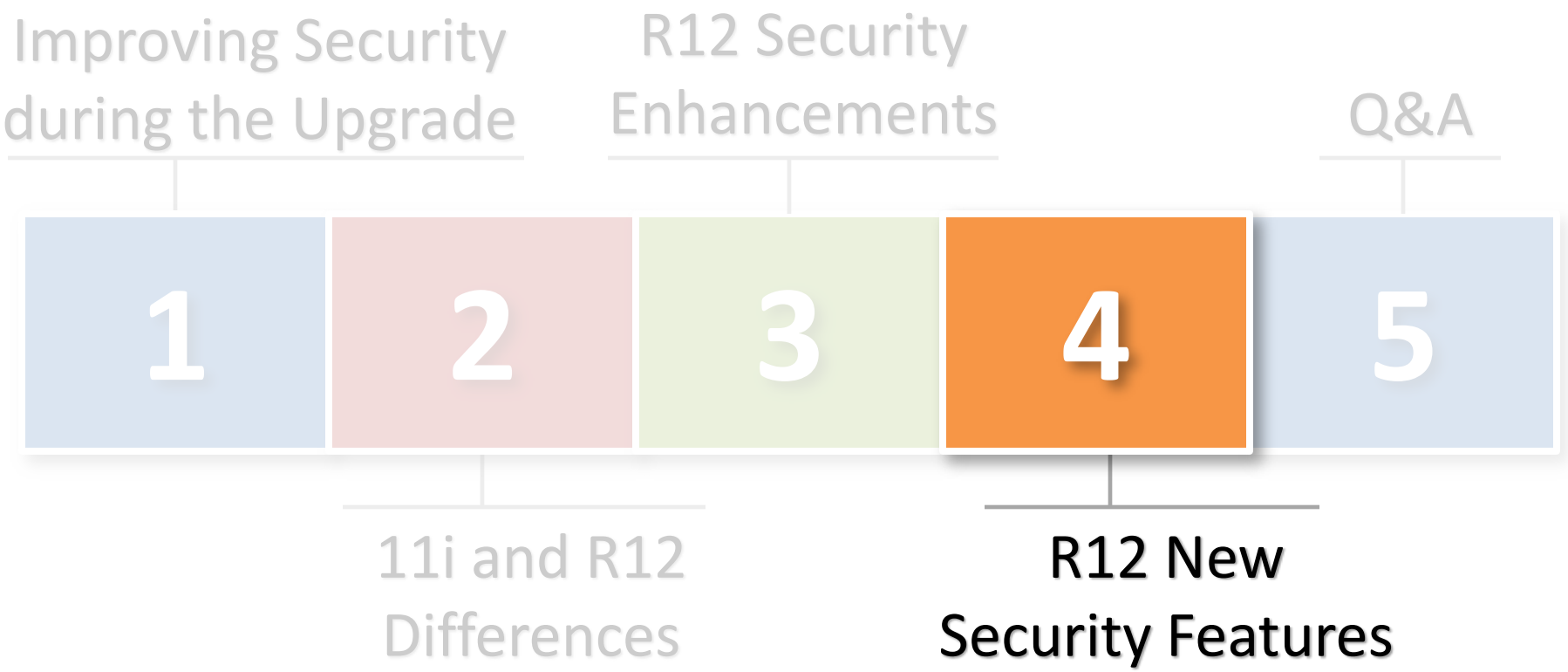
- **Improved SSL support**
  - Changed from mod_ssl -> mod_ossl
  - Uses Oracle Wallet for storing certificates
  - Only strong ciphers enabled and SSLv2 disabled
- **Provides AutoConfig support for securing the major communication routes with SSL.**
- **See Metalink Note ID 376700.1**

# Advanced Configuration Wizards

- **New "Advanced Configuration Wizards" for complex setups of advanced configurations**
  - Available through OAM
  - DNS load balancing
  - HTTP load balancing
  - SSL setup on web server
  - SSL Accelerator setup

INTEGRIGY

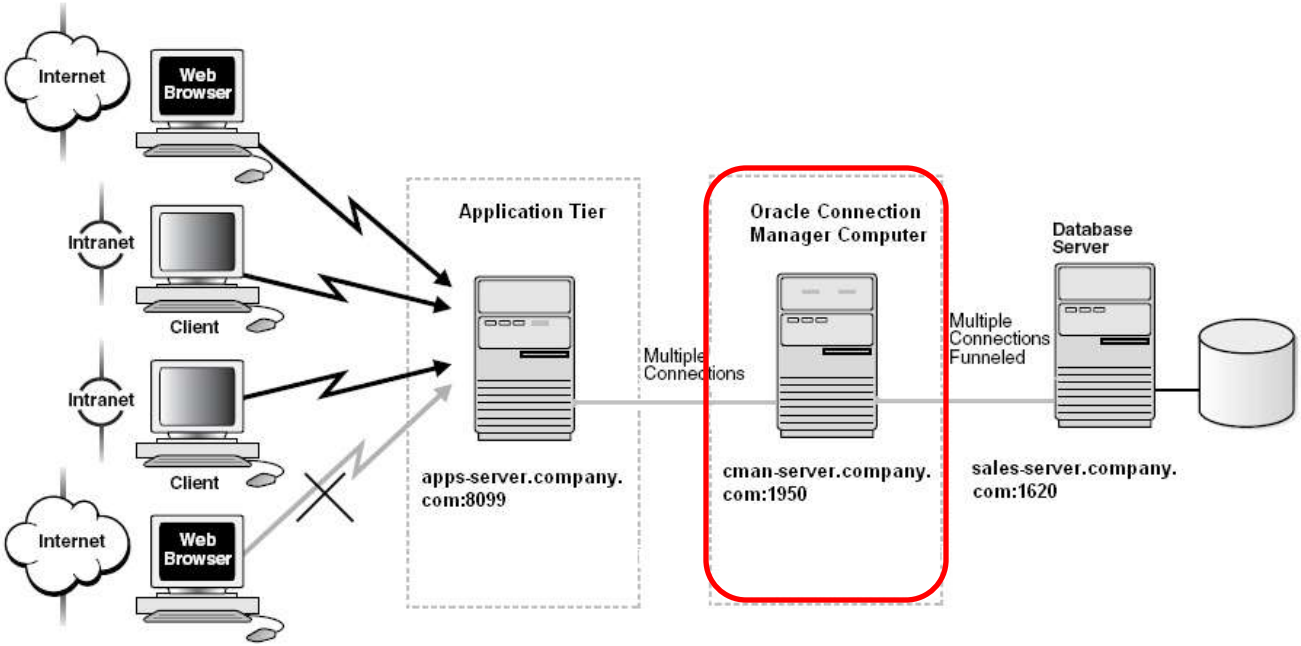
# Agenda




INTEGRIGY

# Oracle Connection Manager

- **Oracle Connection Manager Supported**
  - Advanced security to restrict database connections
  - Replaces Managed SQL*Net Access
  - See Metalink Note ID 558959.1




INTEGRIGY

# RBAC and User Management

- **Role Based Access Control (RBAC)**
  - RBAC is an ANSI standard for access control
  - Allows for responsibilities to be assigned through roles
  - Role Inheritance and Role Categories
  - See Metalink Note ID 290525.1
- **Oracle User Management (UMX)**
  - New user registration
  - Enhanced Forget Username/Password Functionality
  - New security wizards

INTEGRIGY

# Proxy User

- **Proxy User allows a user to specify a proxy who can act on their behalf.**
  - For example, an executive can designate an assistant as a proxy, allowing that assistant to
  - Create, edit or approve transactions on behalf of that executive
- **Generally, avoid use due to auditing issues**
- **Can be used to solve the concurrent request scheduling problem**

# PCI PA-DSS

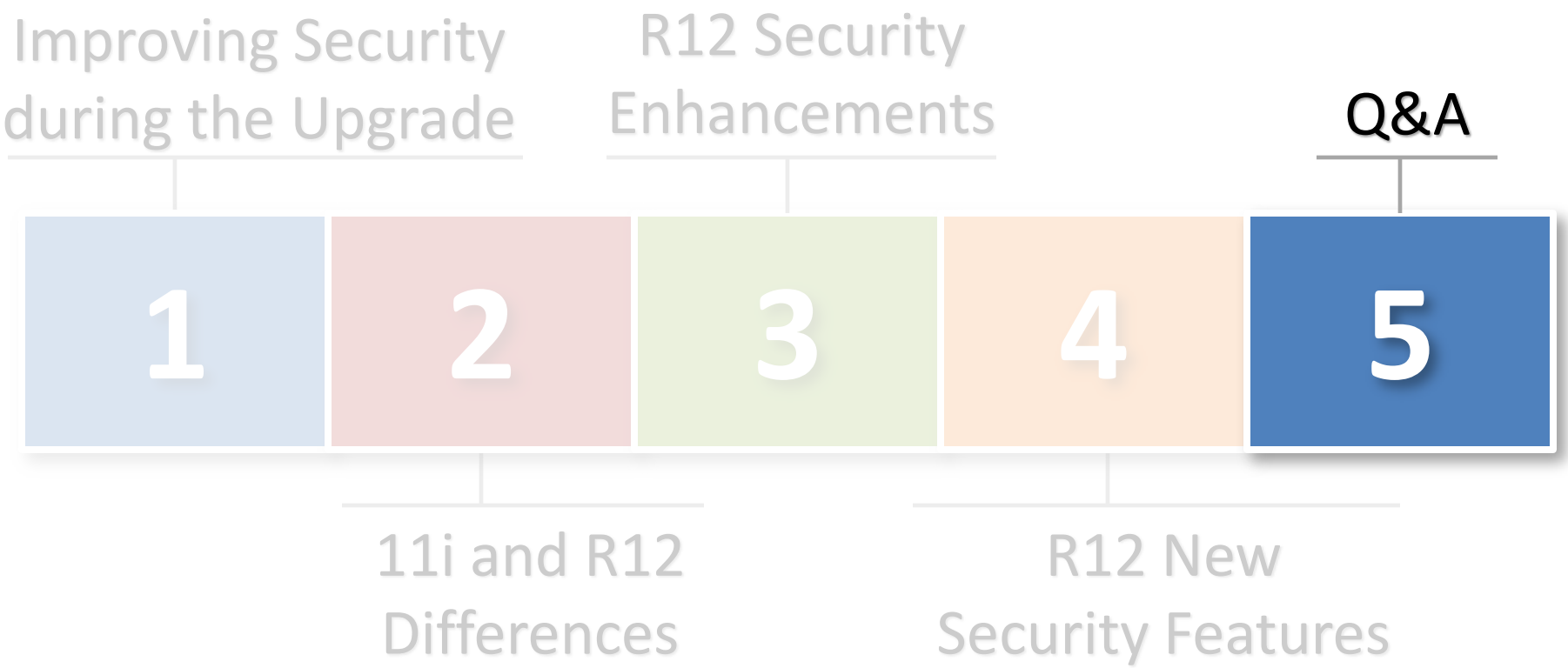
- **Oracle PA-DSS Consolidated Patch for Release 12.1**
  - Reduces complexity of PCI DSS compliance
  - Fixes multiple functional weaknesses when processing and viewing credit card data
  - Does not eliminate significant manual configuration for PCI DSS
  - Only 12.1 is PA-DSS compliant
  - See Metalink Note ID 984283.1
- **11i and 12.0 will not be PA-DSS compliant**
  - See Metalink Note ID 1101213.1

# R12 Upgrade Security Recommendations

- **Include security tasks throughout the upgrade project**
  - Implement high value, low effort security improvements and enhancements
  - Leverage the “free” testing cycles
- **Adhere to the Oracle Best Practices for Oracle EBS security**
  - See Metalink Note ID 403537.1
  - Written by Integrigy
  - Oracle has not updated since 2007
- **Validate the security configuration post-upgrade**
  - Perform a post-upgrade security scan or review
  - Validate compliance against security best practices
  - Oracle E-Business Suite is complex and “the devil is in the details”

INTEGRIGY

# Agenda




INTEGRIGY

# Integrigy Contact Information

**Stephen Kost**
**Chief Technology Officer**
**Integrigy Corporation**

**e-mail: info@integrigy.com**
**blog: integrigy.com/oracle-security-blog**

**For information on -**

- Oracle Database Security
- Oracle E-Business Suite Security
- Oracle Critical Patch Updates
- Oracle Security Blog

**www.integrigy.com**



INTEGRIGY