ERP Risk Advisors

INTEGRIGY

Upgrade +1
Improving Your Security
During Your Upgrade to R12

Jeffrey T. Hare, CPA CISA CIA
Industry Analyst, Author, Consultant
ERP Risk Advisors

Stephen Kost
Chief Technology Officer
Integrigy Corporation

September 13, 2011

Speakers

Jeff Hare

ERP Risk Advisors

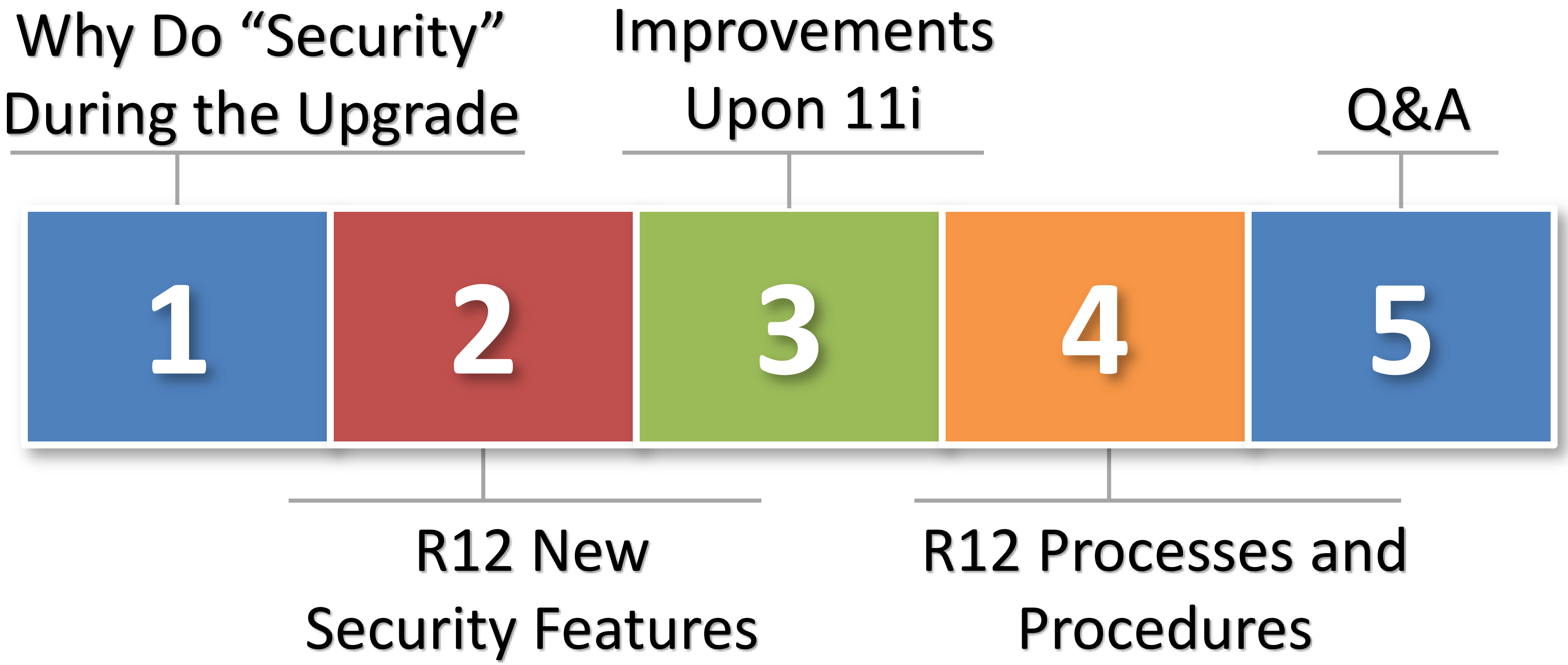
- Founder of ERP Risk Advisors / ERP Seminars and Oracle User Best Practices Board
- 14 years working with Oracle EBS as client and consultant
- Experience includes Big 4 audit, 6 years in CFO/Controller roles – both as auditor and auditee
- Author – *Oracle E-Business Suite Controls: Application Security Best Practices*

Stephen Kost

Integrigy Corporation

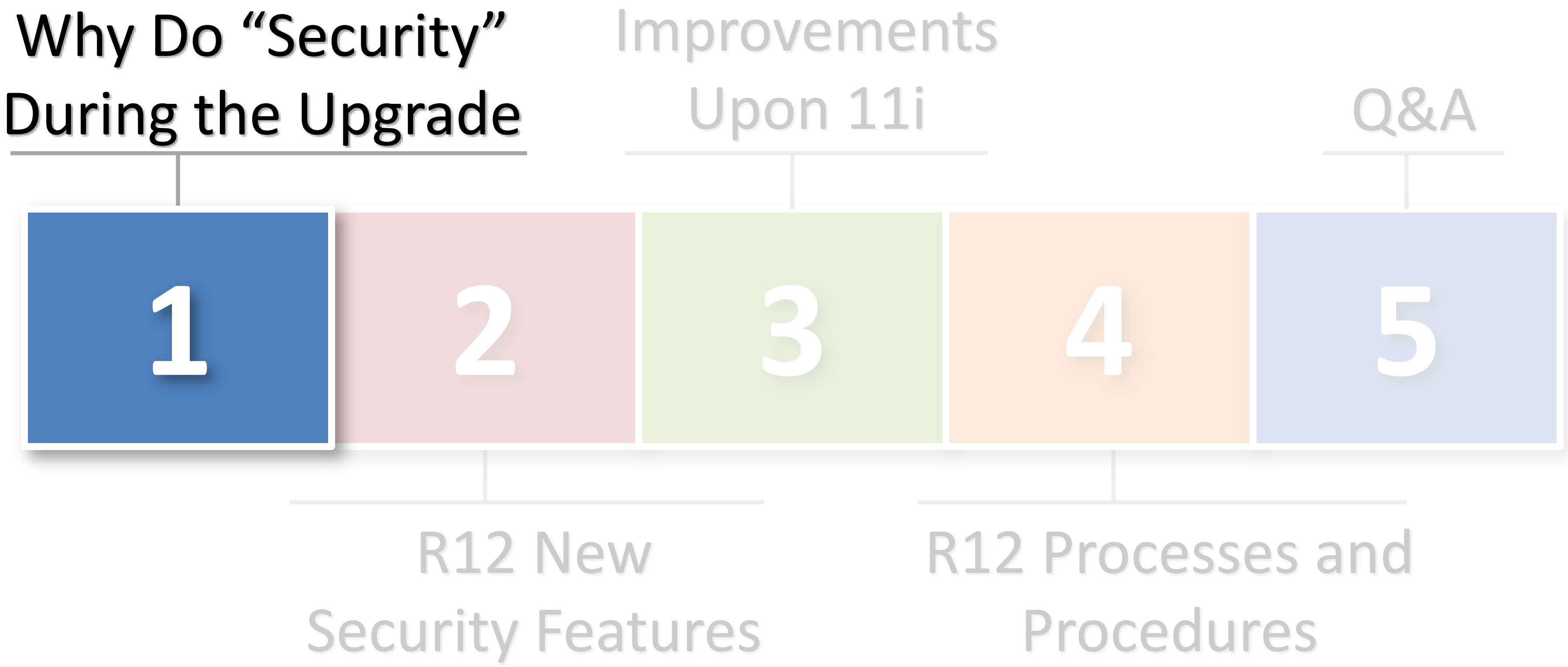
- CTO and Founder
- 16 years working with Oracle and 12 years focused on Oracle security
- DBA, Apps DBA, technical architect, IT security, …
- Integrigy Consulting – Oracle EBS security assessments and services
- Integrigy AppSentry – Oracle EBS Security Assessment and Audit Tool

Agenda



1. Why Do "Security" During the Upgrade
2. R12 New Security Features
3. Improvements Upon 11i
4. R12 Processes and Procedures
5. Q&A

Agenda



1 Why Do “Security” During the Upgrade

2 R12 New Security Features

3 Improvements Upon 11i

4 R12 Processes and Procedures

5 Q&A

Why do “Security” during the upgrade?

1 Functional, Technical, & Stress Testing

- Functional application testing
- Performance and stress testing

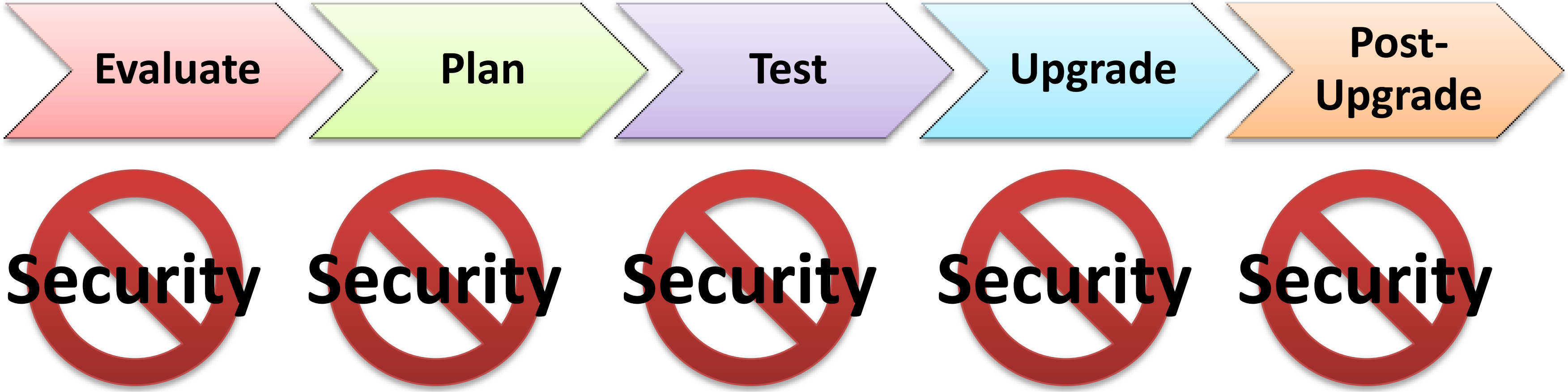
2 Technology Stack Upgrades

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

3 Modifications to Customizations

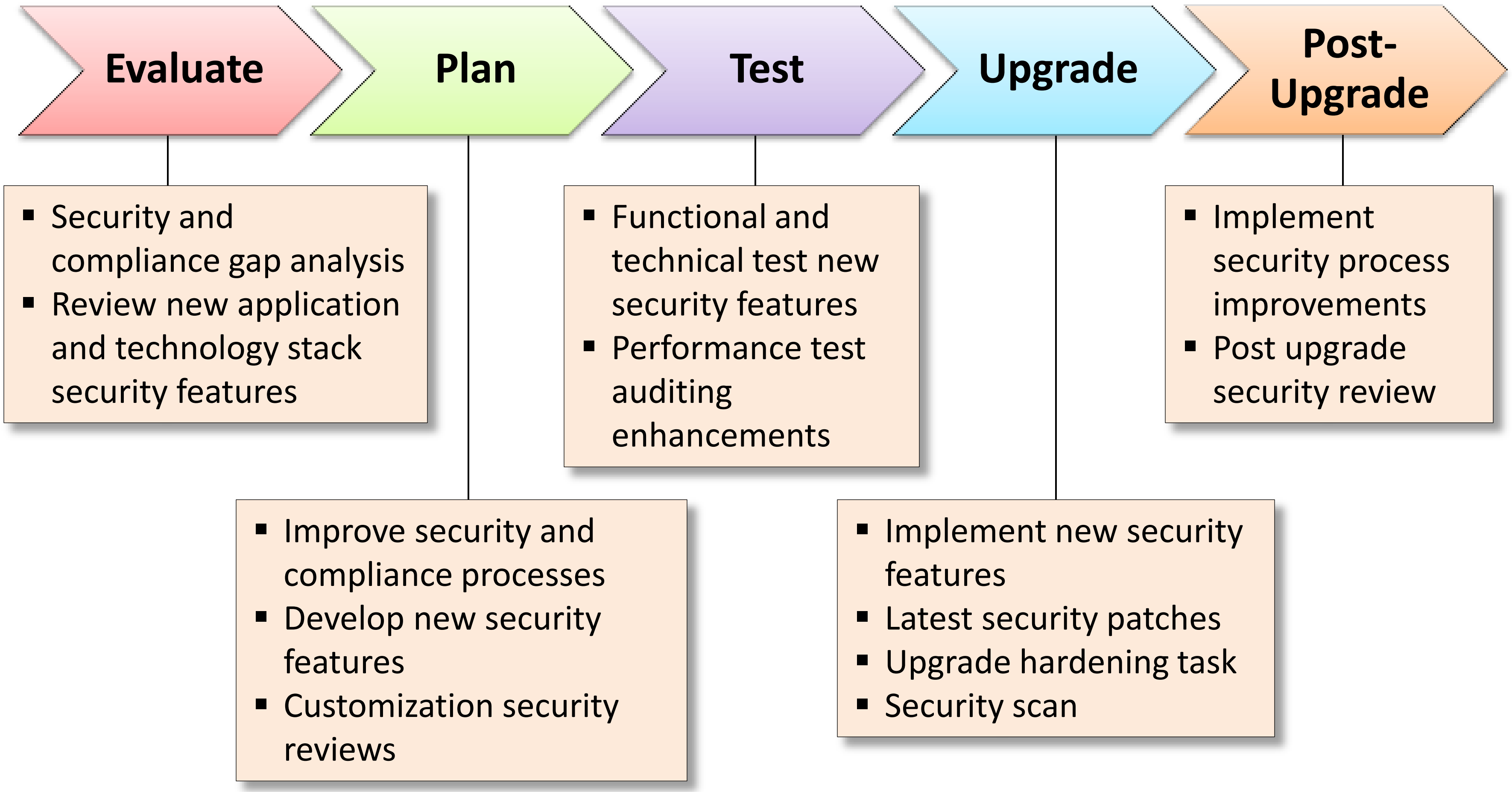
- Some or many customizations must be upgraded
- Ideal time to review development standards

Traditional R12 Upgrade Project



Security "Aware" R12 Upgrade Project

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



Evaluate

- Security and compliance gap analysis
- Review new application and technology stack security features

Plan

- Improve security and compliance processes
- Develop new security features
- Customization security reviews

Test

- Functional and technical test new security features
- Performance test auditing enhancements

Upgrade

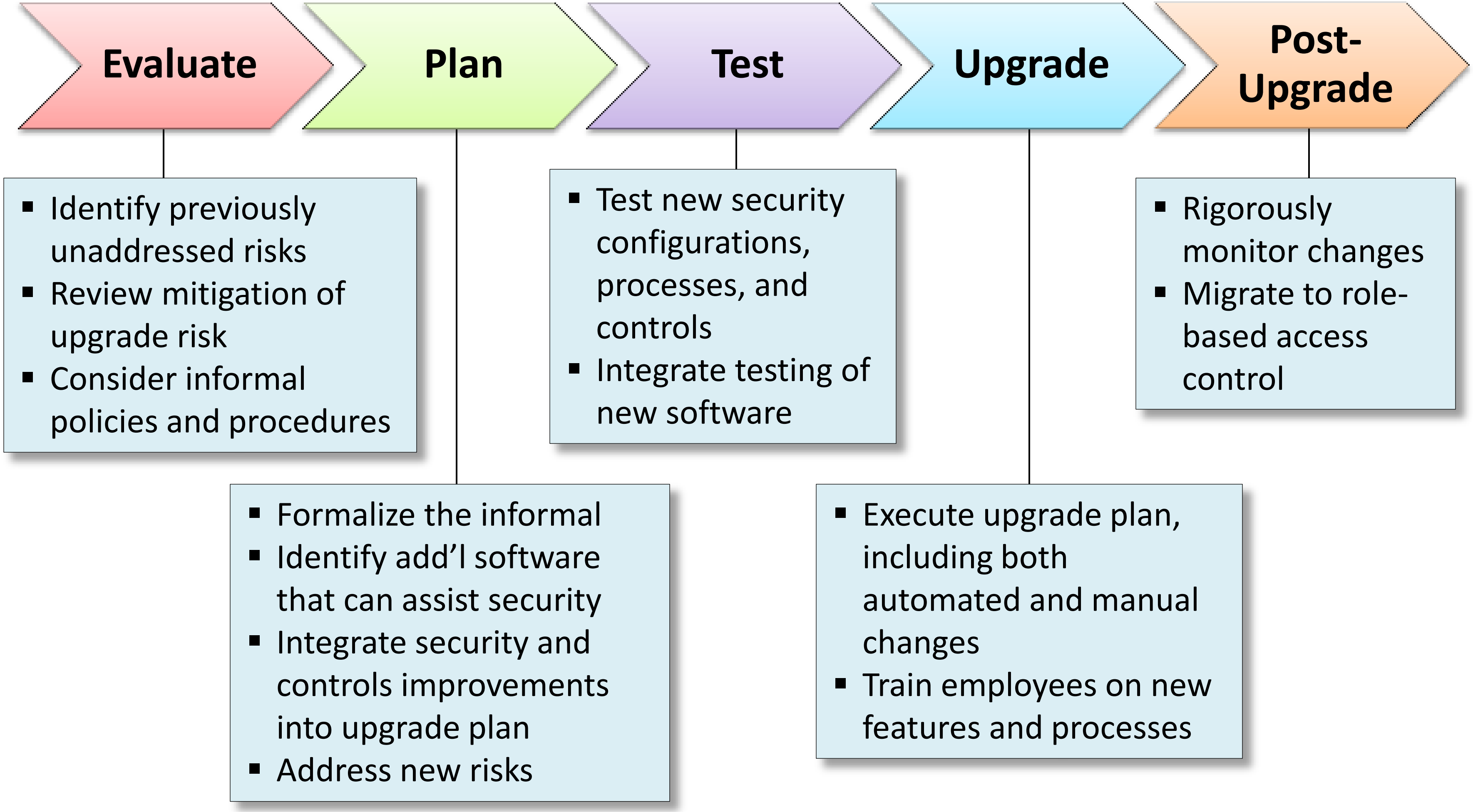
- Implement new security features
- Latest security patches
- Upgrade hardening task
- Security scan

Post-Upgrade

- Implement security process improvements
- Post upgrade security review

Security “Aware” R12 Upgrade Project

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



Evaluate

- Identify previously unaddressed risks
- Review mitigation of upgrade risk
- Consider informal policies and procedures

Plan

- Formalize the informal
- Identify add’l software that can assist security
- Integrate security and controls improvements into upgrade plan
- Address new risks

Test

- Test new security configurations, processes, and controls
- Integrate testing of new software

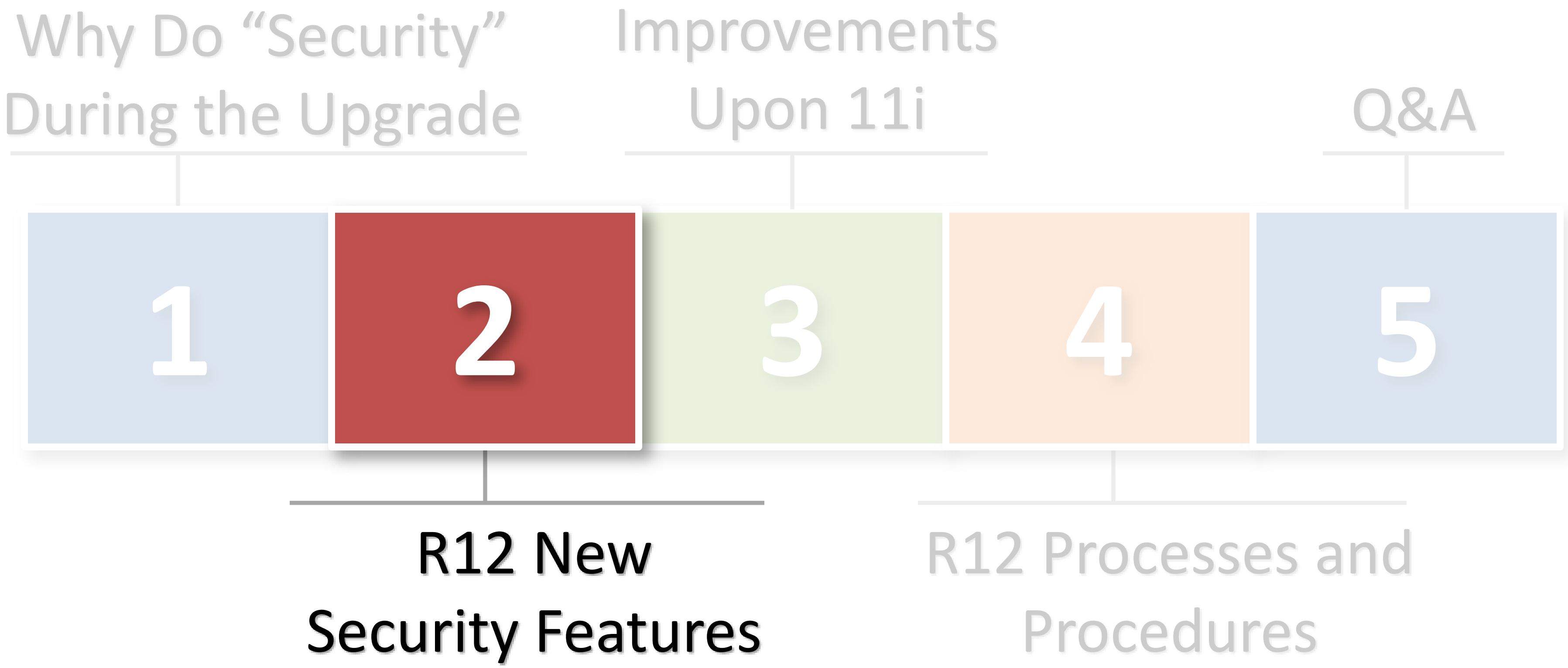
Upgrade

- Execute upgrade plan, including both automated and manual changes
- Train employees on new features and processes

Post-Upgrade

- Rigorously monitor changes
- Migrate to role-based access control

Agenda



1 Why Do “Security” During the Upgrade

2 R12 New Security Features

3 Improvements Upon 11i

4 R12 Processes and Procedures

5 Q&A

R12 New Features

- **MOAC – reduce number of responsibilities**
  - Restrictions on localizations
- **SLA – ability to enter journal through subledgers**
- **Definition Access Sets – better secure various components throughout the GL**
- **Data Access Sets – better security within the chart of accounts (Inquiry, Balancing Segment Values)**

Role Based Access Control (RBAC)

- RBAC is an ANSI standard for access control
- Allows for responsibilities to be assigned through roles
- Simplifies assigned of common responsibilities
- Role Inheritance and Role Categories
- See Metalink Note ID 290525.1

User Management (UMX)

- **New user registration**
  - Self request access with approvals and workflow
- **Enhanced Login Assistance**
  - Forgot Username
  - Forgot Password
- **Process to create users with strong, one-time passwords**
- **New security wizards**

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**

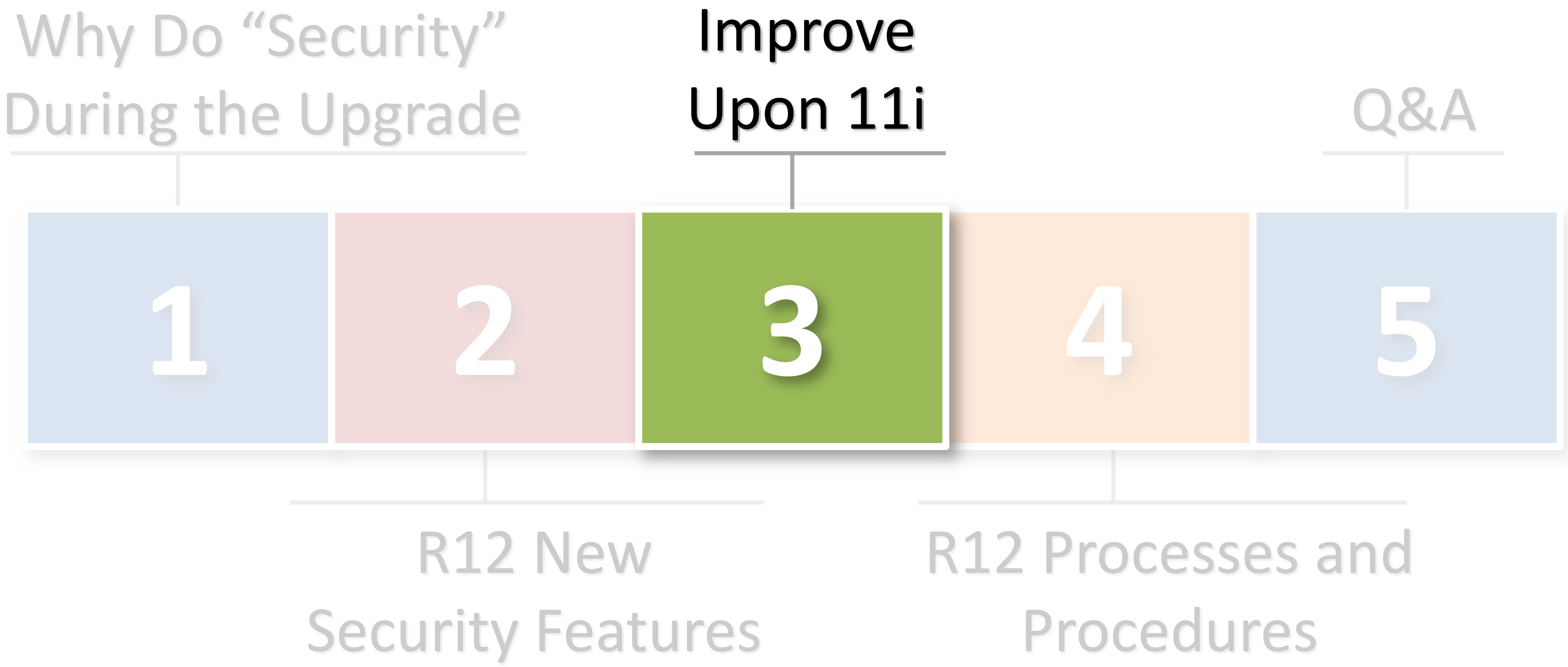
Protecting Database Accounts

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

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

Agenda



1

Why Do “Security” During the Upgrade

2

R12 New Security Features

3

Improve Upon 11i

4

R12 Processes and Procedures

5

Q&A

Upgrade +1 Concept

- **Consider new software:**
  - SOD software
  - Trigger or log-based technologies to develop detailed audit trails (before/after values)
  - External security analysis
  - Allow for monitoring of SQL forms, configurations related to key controls, development objects – better QA over your Change Management process

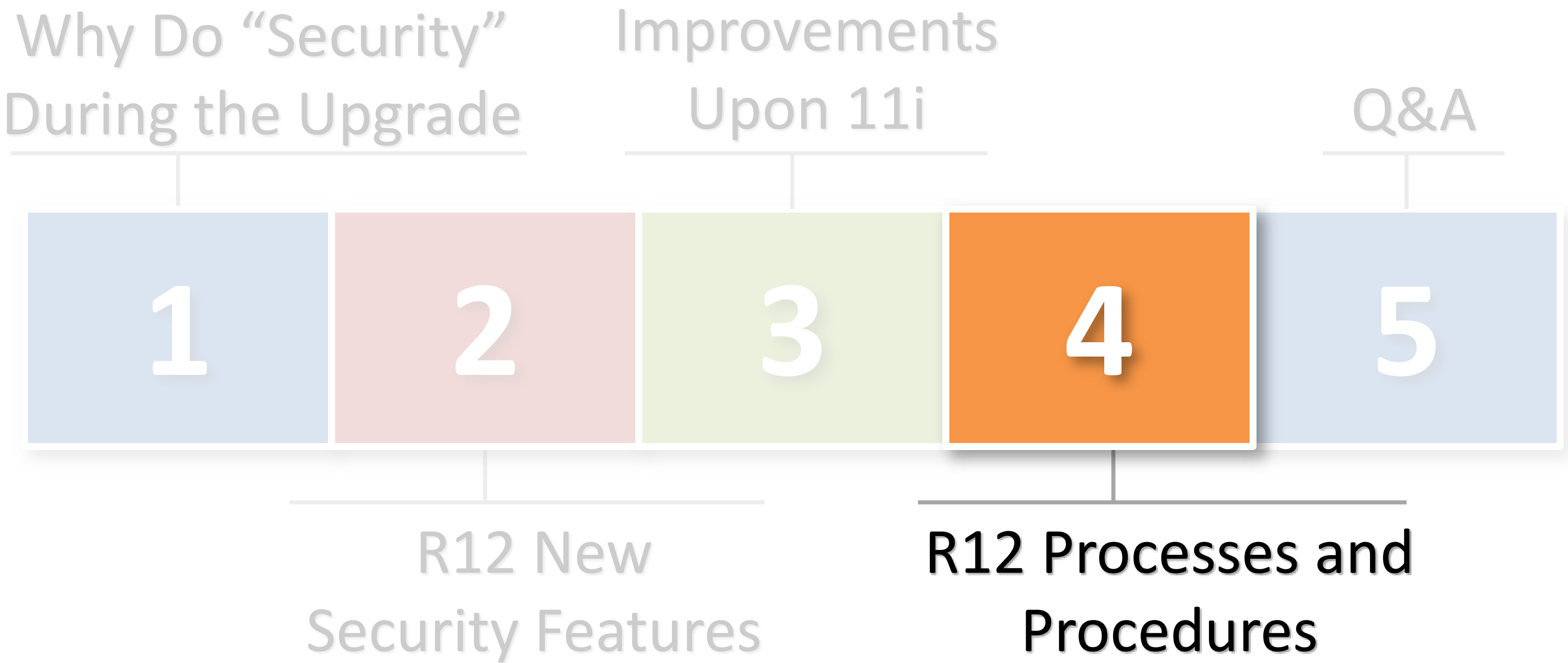
Fix What Was Broken

- Privileged user access
- Excessive access to configurations by end users
- Access to transactions by IT personnel
- Usage of generic or vendor supplier user accounts
- Not monitoring activity through SQL forms

Application Security Design

- Move toward use more customized responsibilities, if not all custom responsibilities
- Move toward use of all custom top-level menus and more custom sub-menus – such as those related to setups – reduce upgrade risks
- Take into consideration sensitive data
- Better definition of Request Groups

Agenda



1 Why Do “Security” During the Upgrade

2 R12 New Security Features

3 Improvements Upon 11i

4 R12 Processes and Procedures

5 Q&A

Change Management

- **Formalize processes related to:**
  - Configuration Change Management
  - Patch Change Management
  - Application Security Change Management
  - Database Security Change Management
- **Implement a more robust Quality Assurance process related to Change Management**
  - Reduce unapproved changes
  - Protect integrity of system

Improve Controls

- **Identify additional risks such as:**
  - Operational risks specific to your organization
  - Fraud risks
  - Data security
- **Automate controls:**
  - Seeded workflows – build/changes processes to accommodate; Personalizations; Alerts
- **Document compliance with published Best Practices**

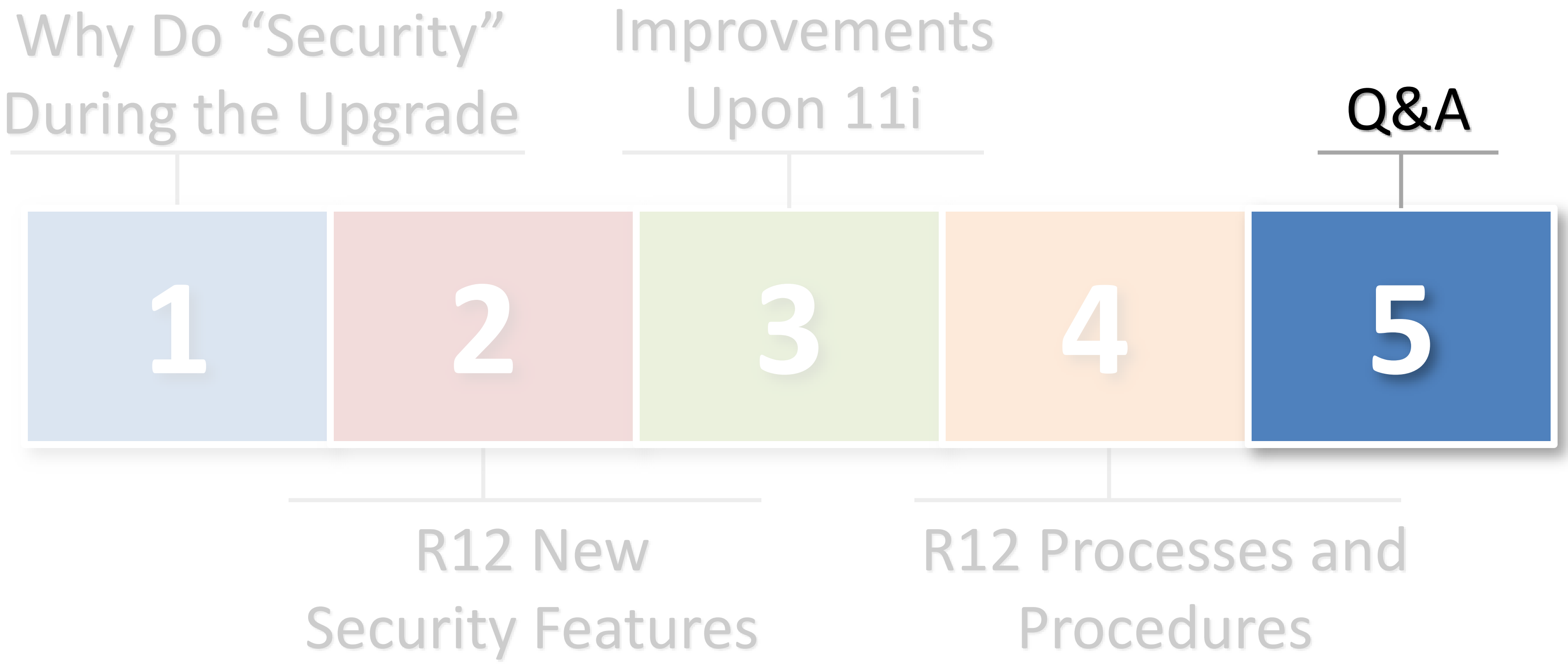
R12 Upgrade Controls Recommendations

- Process and Controls Change Committee
- Automate controls, where possible
- Evaluate ‘key’ controls to reduce audit scope, cost
- Implement technology and processes to better monitor / automate controls
- Document formal risk assessment process for application security risks
- Develop process to assess and document results of risk assessment – all risks

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”

Agenda



Why Do “Security” During the Upgrade

Improvements Upon 11i

Q&A

1

2

3

4

5

R12 New Security Features

R12 Processes and Procedures

Speaker Contact Information

Jeffrey T. Hare
Industry Analyst, Author
ERP Risk Advisors

e-mail: jhare@erpra.net
website: www.erpra.net
blog: jeffreythare.blogspot.com
twitter: @jeffreythare

Stephen Kost
Chief Technology Officer
Integrigy Corporation

e-mail: info@integrigy.com
blog: integrigy.com/oracle-security-blog
website: www.integrigy.com
twitter: @integrigy