INTEGRIGY

Guide to Auditing and Logging in the Oracle E-Business Suite

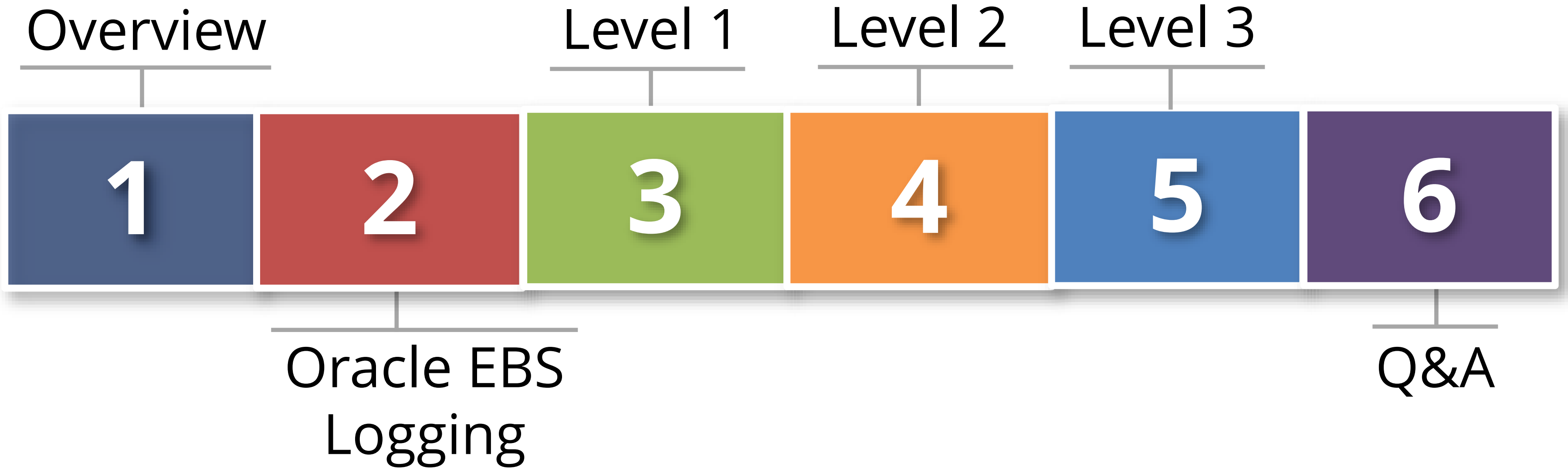
February 13, 2014

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Mike Miller
Chief Security Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

Agenda



1 Overview

2 Oracle EBS Logging

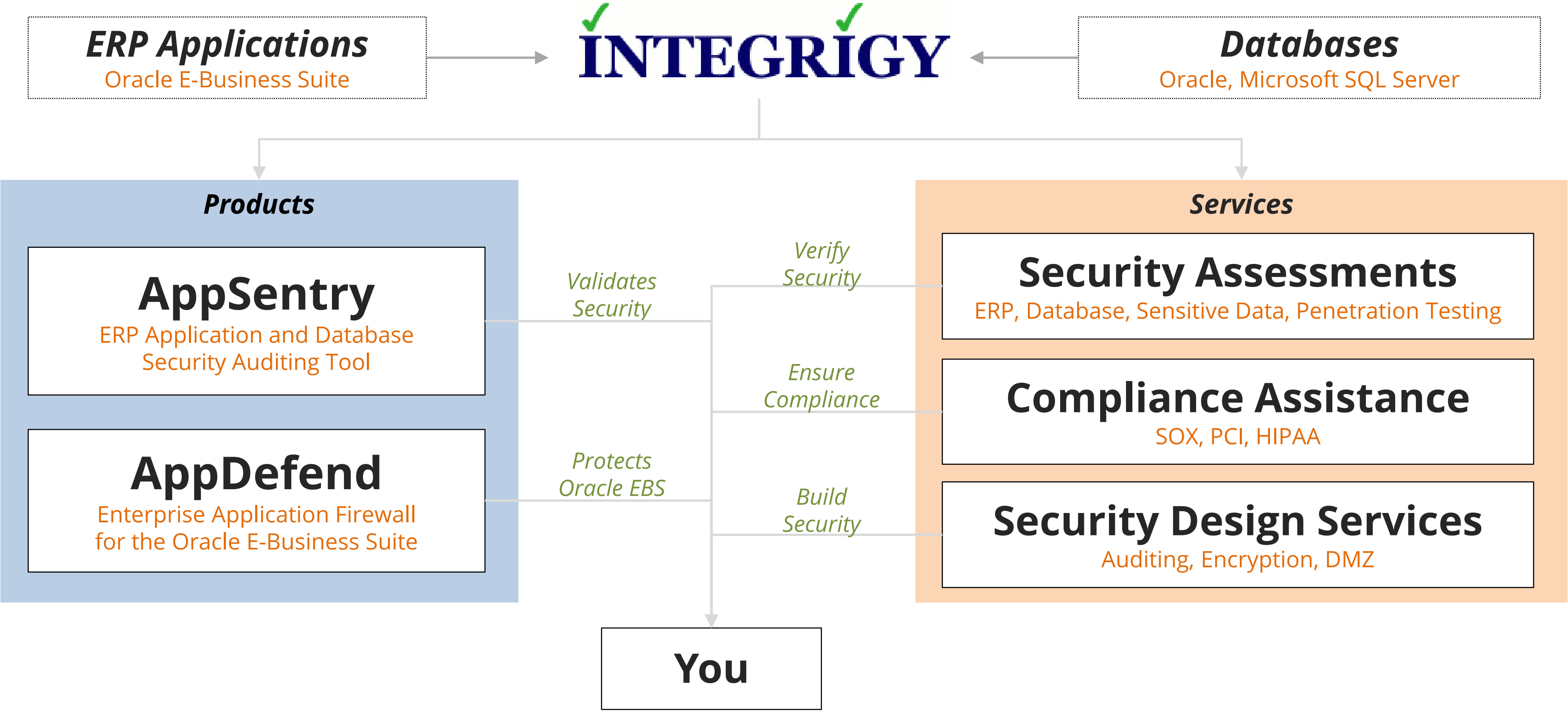
3 Level 1

4 Level 2

5 Level 3

6 Q&A

About Integrigy



ERP Applications
Oracle E-Business Suite

INTEGRIGY

Databases
Oracle, Microsoft SQL Server

Products

AppSentry
ERP Application and Database Security Auditing Tool

AppDefend
Enterprise Application Firewall for the Oracle E-Business Suite

Validates Security

Protects Oracle EBS

Verify Security

Ensure Compliance

Build Security

Services

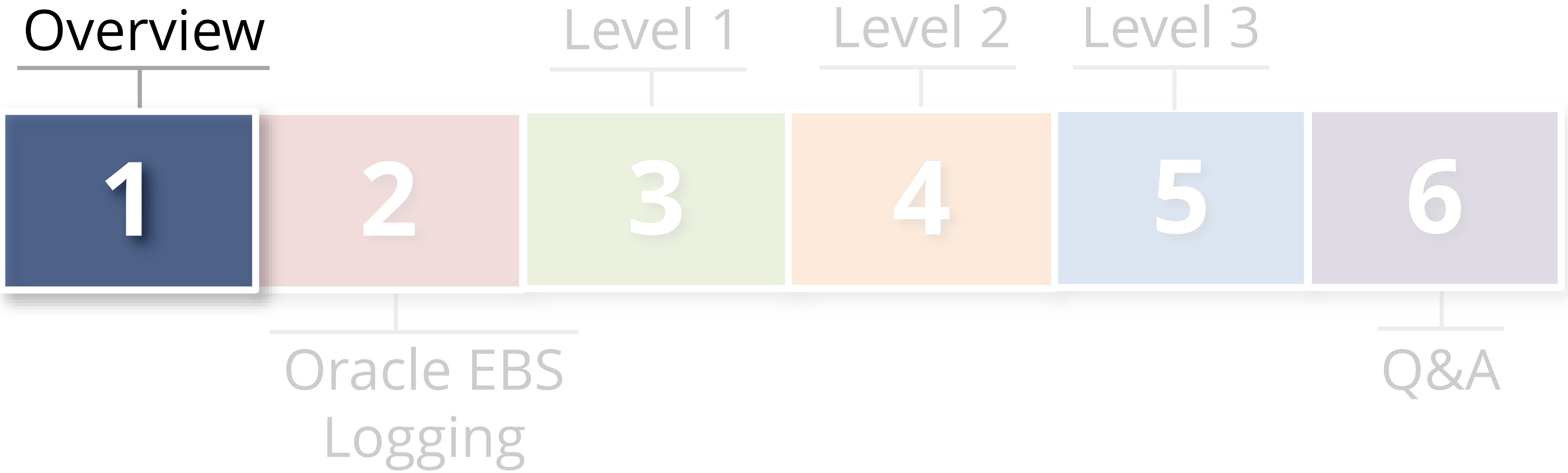
Security Assessments
ERP, Database, Sensitive Data, Penetration Testing

Compliance Assistance
SOX, PCI, HIPAA

Security Design Services
Auditing, Encryption, DMZ

You

Agenda



1 Overview

2 Oracle EBS Logging

3 Level 1

4 Level 2

5 Level 3

6 Q&A

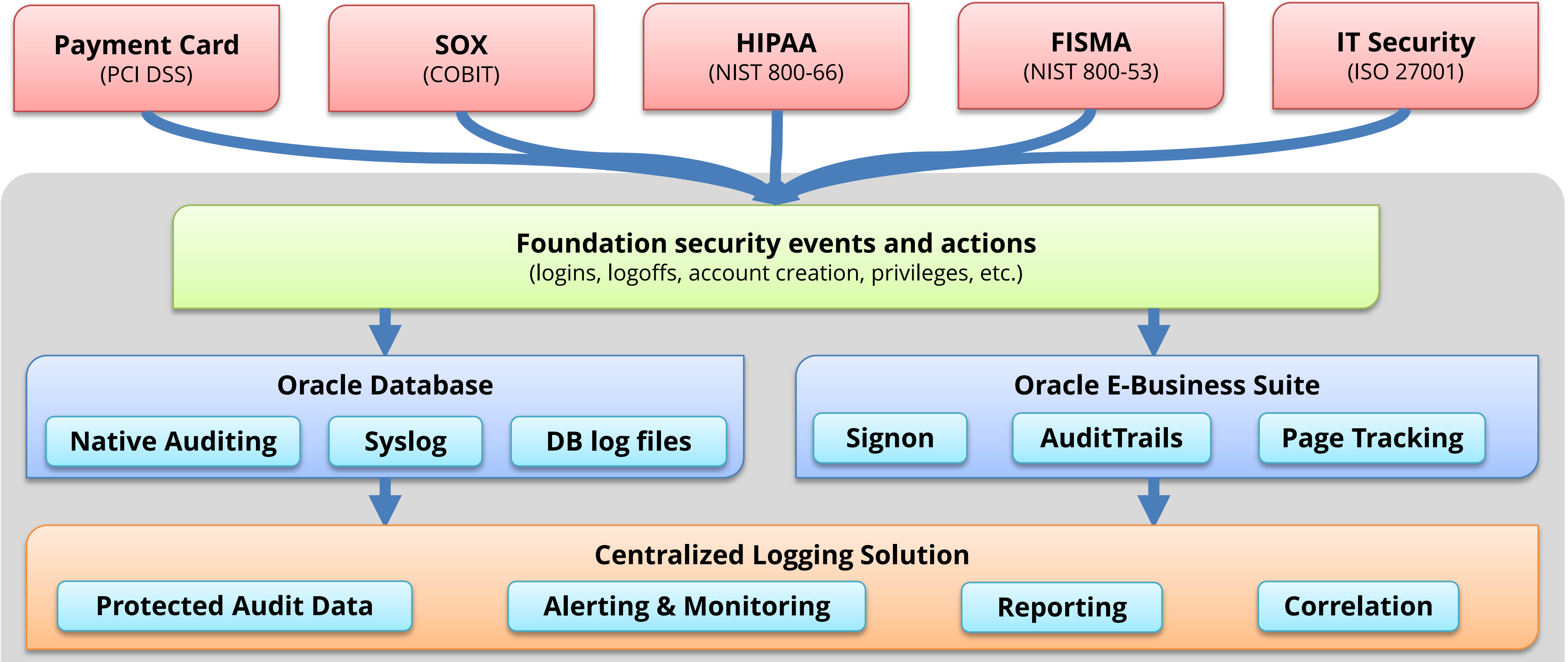
Auditing and Logging the Oracle E-Business Suite

- **Log so can audit, monitor and alert**
  - Related but separate disciplines

- **Requirements are difficult**
  - Technical, Compliance, Audit, and Security

- **The Oracle database and Oracle E-Business Suite offer rich log and audit functionality**
  - **Most organizations do not fully take advantage**

Integrigy Framework for Auditing and Logging



Payment Card (PCI DSS)

SOX (COBIT)

HIPAA (NIST 800-66)

FISMA (NIST 800-53)

IT Security (ISO 27001)

Foundation security events and actions
(logins, logoffs, account creation, privileges, etc.)

Oracle Database

- Native Auditing
- Syslog
- DB log files

Oracle E-Business Suite

- Signon
- AuditTrails
- Page Tracking

Centralized Logging Solution

- Protected Audit Data
- Alerting & Monitoring
- Reporting
- Correlation

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**

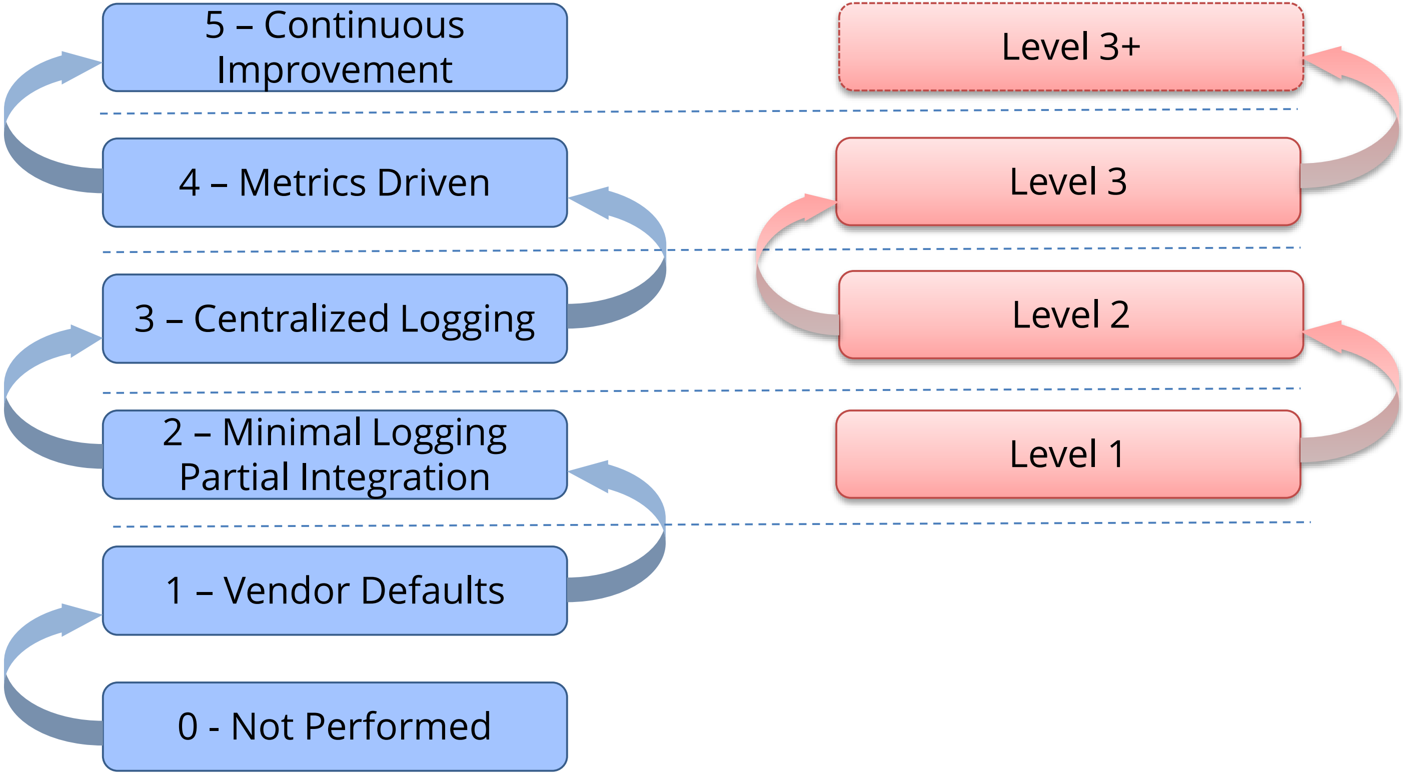
Foundation Security Events Mapping

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

Integrigy Framework Maturity Model

Level 1	Enable **baseline auditing and logging** for application/database and implement security monitoring and auditing alerts
Level 2	Send audit and log data to a **centralized logging** solution outside the Oracle Database and E-Business Suite
Level 3	Extend logging to include **functional logging** and more complex alerting and monitoring

Logging Maturity Model



5 – Continuous Improvement

4 – Metrics Driven

3 – Centralized Logging

2 – Minimal Logging Partial Integration

1 – Vendor Defaults

0 - Not Performed

Level 3+

Level 3

Level 2

Level 1

Common Maturity Model (CMM)

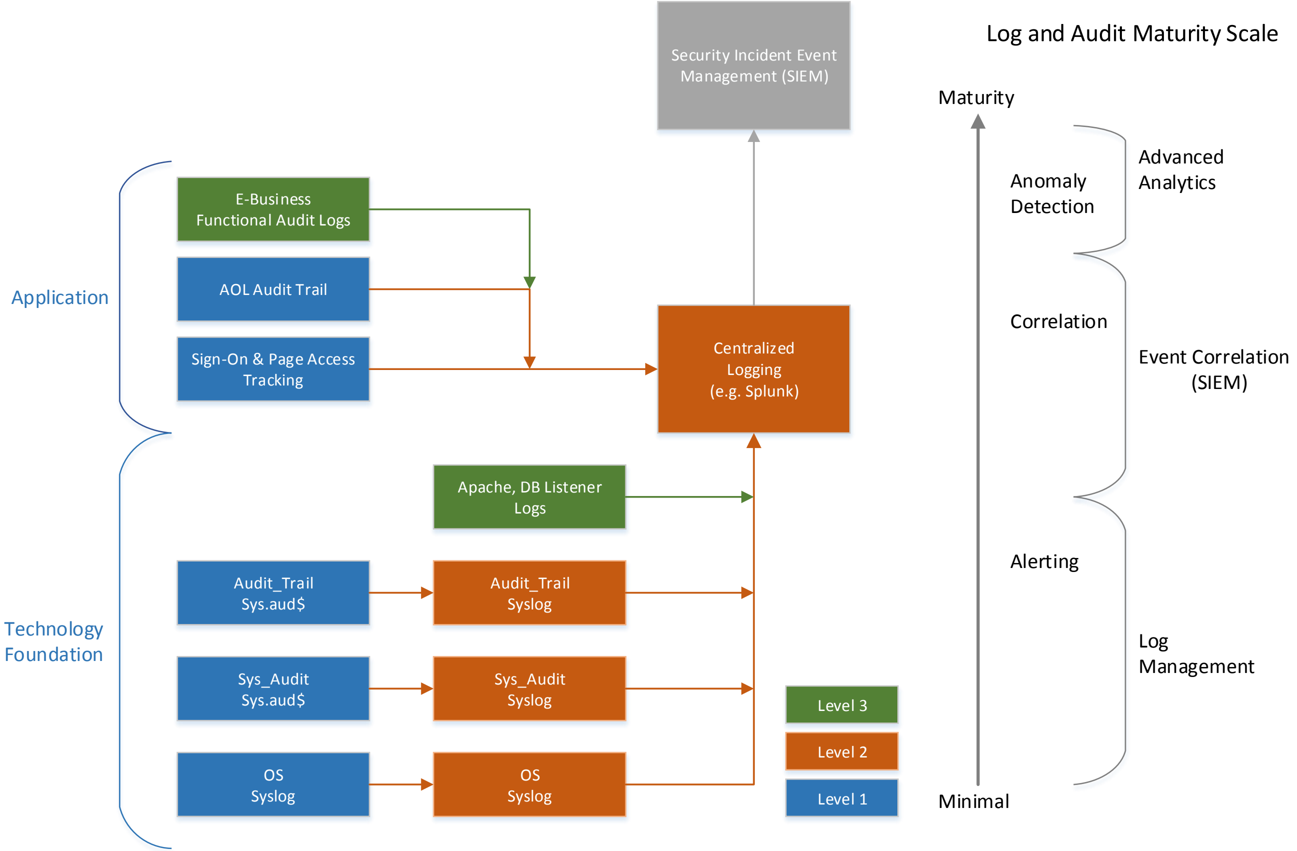
Integrigy Framework

Centralized Logging

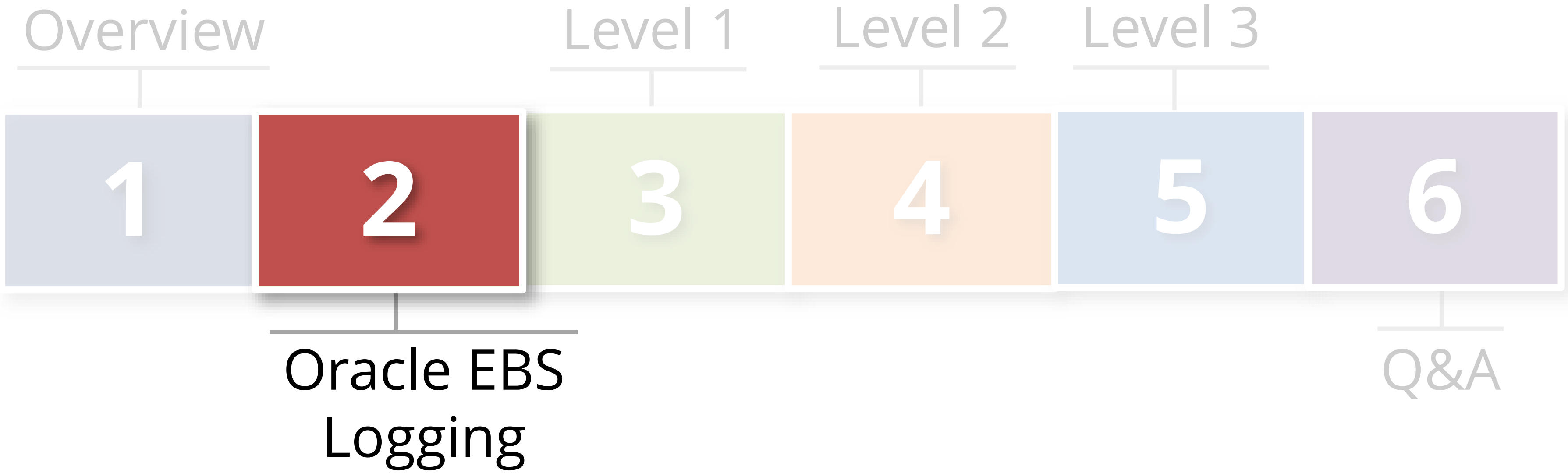
- **Integrate EBS with centralized logging solution**
  - People and processes use multiple applications and technologies
  - E-Business Suite is a cornerstone

- **Use Commercial or open source solutions**
  - Purpose built functionality for correlation, monitoring and unified alerting
  - Protection of log and audit data

E-Business Suite Auditing and Logging



Agenda



1 Overview

2 Oracle EBS Logging

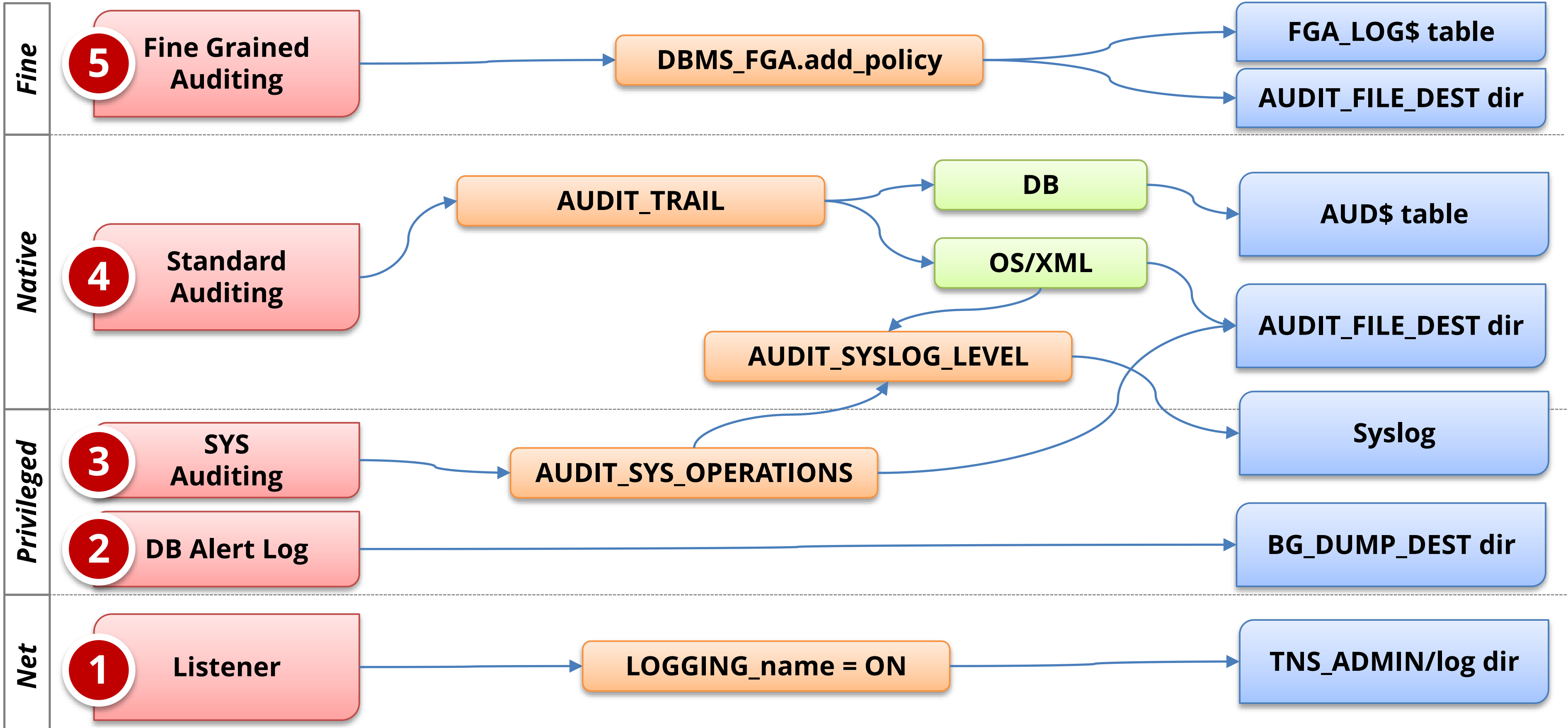
3 Level 1

4 Level 2

5 Level 3

6 Q&A

Oracle Database Auditing and Logging



Fine

5 Fine Grained Auditing

DBMS_FGA.add_policy

FGA_LOG$ table

AUDIT_FILE_DEST dir

Native

4 Standard Auditing

AUDIT_TRAIL

DB

OS/XML

AUD$ table

AUDIT_FILE_DEST dir

AUDIT_SYSLOG_LEVEL

Syslog

Privileged

3 SYS Auditing

AUDIT_SYS_OPERATIONS

2 DB Alert Log

BG_DUMP_DEST dir

Net

1 Listener

LOGGING_name = ON

TNS_ADMIN/log dir

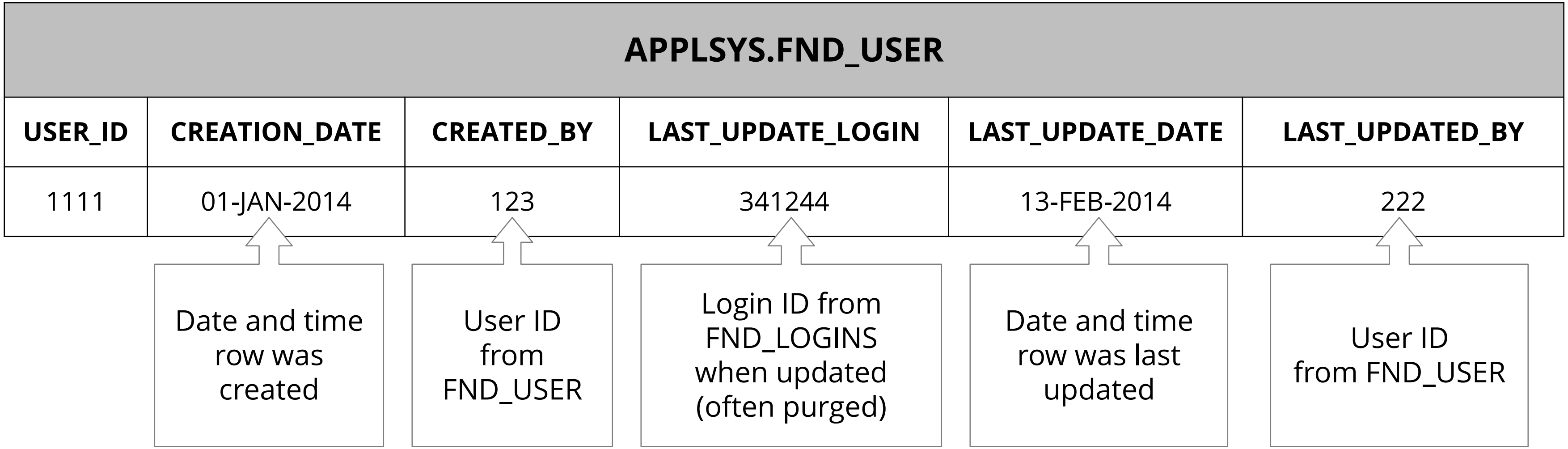
Type of auditing and logging

Audit and logging parameters

Location of audit data

Oracle EBS Who Columns

Almost all Oracle EBS tables have “Who Columns” which capture **creation and last update information**. Changes between creation and last update are not. Access in Forms using About this Record.



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

Date and time row was created

User ID from FND_USER

Login ID from FND_LOGINS when updated (often purged)

Date and time row was last updated

User ID from FND_USER

Oracle EBS Sign-On Audit

Standard EBS functionality to log **Professional Forms** use and navigation. Enabled by the system profile option **Sign-on: Audit Level** and the default is None.

Profile Option	Report	Table
User	Signon Audit Users	FND_LOGINS
Responsibility	Signon Audit Responsibilities	FND_LOGIN_RESPONSIBILITIES
Form	Signon Audit Forms	FND_LOGIN_RESP_FORMS

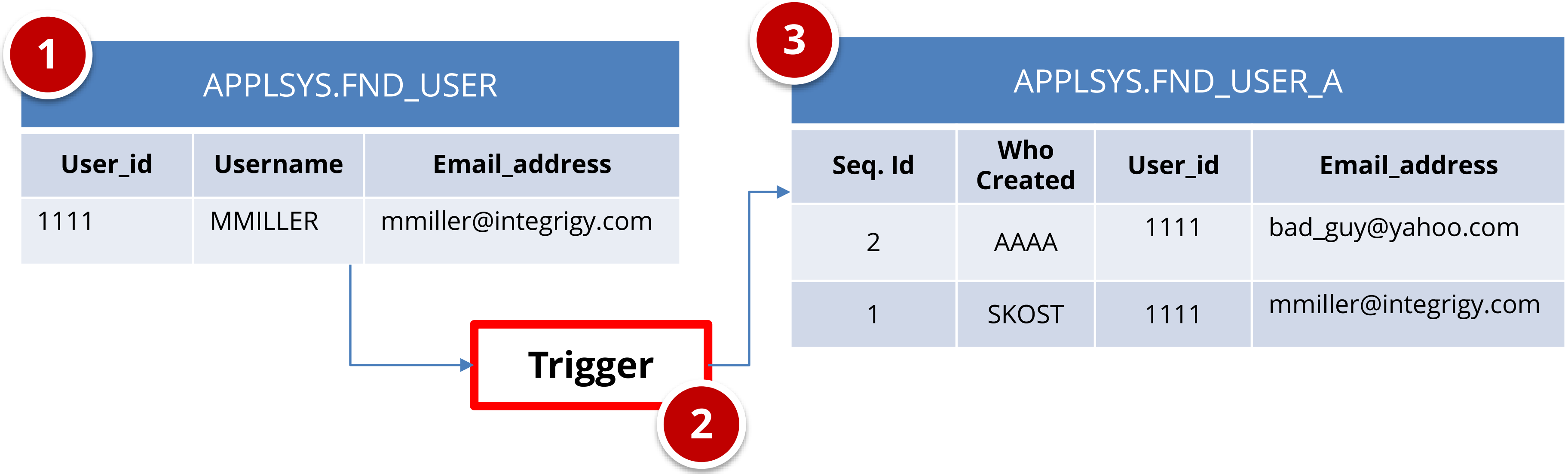
Oracle EBS Page Access Tracking

EBS functionality to log **Web and HTML** use and navigation. Configured through Oracle Application Manager and stores audit data in JTF_PF_* tables. Concurrent programs to stage data daily.

On-line Views & Reports	Tables
Session Date Form User Application	JTF.JTF_PF_SES_ACTIVITY JTF.JTF_PF_ANON_ACTIVITY JTF.JTF_PF_APP_SUMM JTF.JTF_PF_HOST_SUMM JTF.JTF_PF_PAGE_SUMM JTF.JTF_PF_SESSION_SUMM JTF.JTF_PF_USER_SUMM

Oracle EBS AuditTrail

AuditTrail functionality stores row changes to EBS tables in **shadow tables** using database triggers. Only tracks insert, update, and deletes to Oracle EBS tables.



APPLSYS.FND_USER

User_id	Username	Email_address
1111	MMILLER	mmiller@integrigy.com

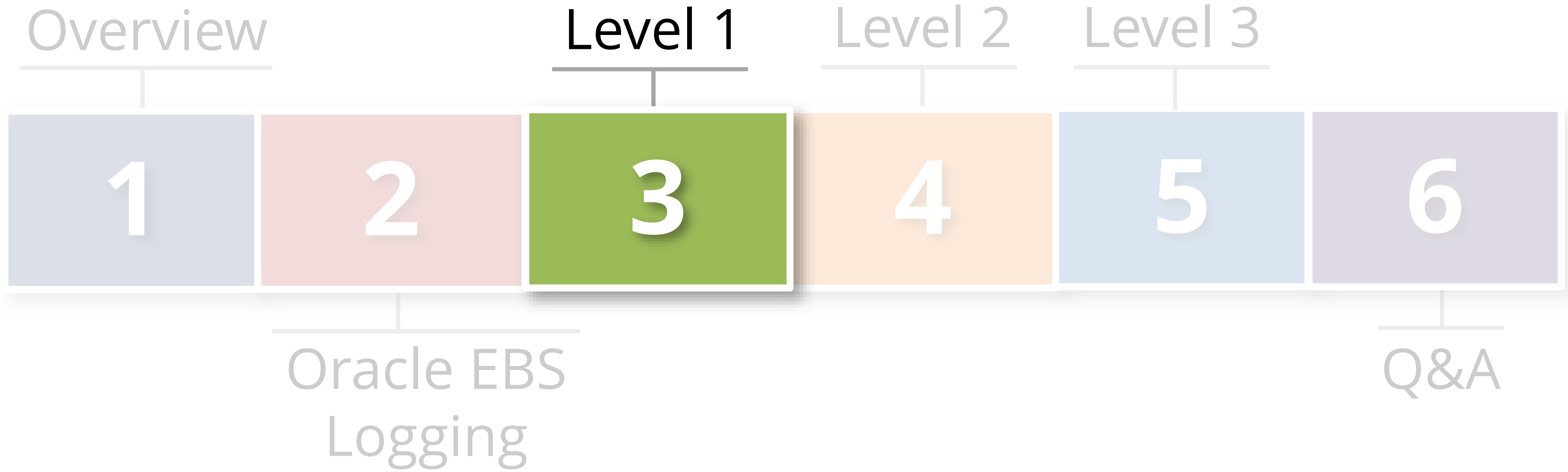
APPLSYS.FND_USER_A

Seq. Id	Who Created	User_id	Email_address
2	AAAA	1111	bad_guy@yahoo.com
1	SKOST	1111	mmiller@integrigy.com

Oracle EBS Other Logging

Unsuccessful Logins	**Report** ▪ Signon Audit Unsuccessful Logins **Tables** ▪ APPLSYS.FND_UNSUCCESSFUL_LOGINS ▪ ICX.ICX_FAILURES
Concurrent Requests	**Report** ▪ Signon Audit Concurrent Requests **Tables** ▪ APPLSYS.FND_CONCURRENT_REQUESTS

Agenda



1 Overview

2 Oracle EBS Logging

3 Level 1

4 Level 2

5 Level 3

6 Q&A

Integrigy Framework – Level 1

Objectives

- Enhance or start **baseline auditing and logging**
- Enhance or implement base security monitoring and auditing alerts
- Using standard database and EBS functionality

Tasks

1. **Database logging**
   - Enable AUDIT_SYS_OPERATIONS
   - Enable Standard auditing
2. **E-Business Suite logging**
   - Set Sign-on audit to log at the ‘Form’ level
   - Enable Page Access Tracking
   - Enable Audit Trail
3. **Create simple alerts**

Level 1 – Database Logging

- **Enable Standard Audit**
  - Log to sys.aud$
  - Define events

- **Purge per organizational policy**

Object	Oracle Audit Statement	Resulting Audited SQL Statements
Session	session	Database logons and failed logons
Users	user	create user alter user drop user
Roles	role	create role alter role drop role
Database Links **Public Database Links**	database link public database link	create database link drop database link create public database link drop public database link
System	alter system	alter system
Database	alter database	alter database
Grants (system privileges and roles)	system grant	grant revoke
Profiles	profile	create profile alter profile drop profile
SYSDBA and SYSOPER	sysdba sysoper	All SQL executed with sysdba and sysoper privileges

Note: table is not complete – see whitepaper for full table

Level 1 – Oracle EBS Logging

Signon-On Audit	▪ System Profile Option **Sign-on: Audit Level** ▪ Set to **Form**
Page Access Tracking	▪ Set Information Capture Level to **Session Info, Cookies and All Parameters** ▪ **Tracked Applications**: System Administration, Oracle Application Manager, Application Object Library, and Common Modules-AK

Level 1 – Oracle EBS Logging

- **Enable Audit Trail for key tables**
  - Low velocity changes
  - High security impact

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

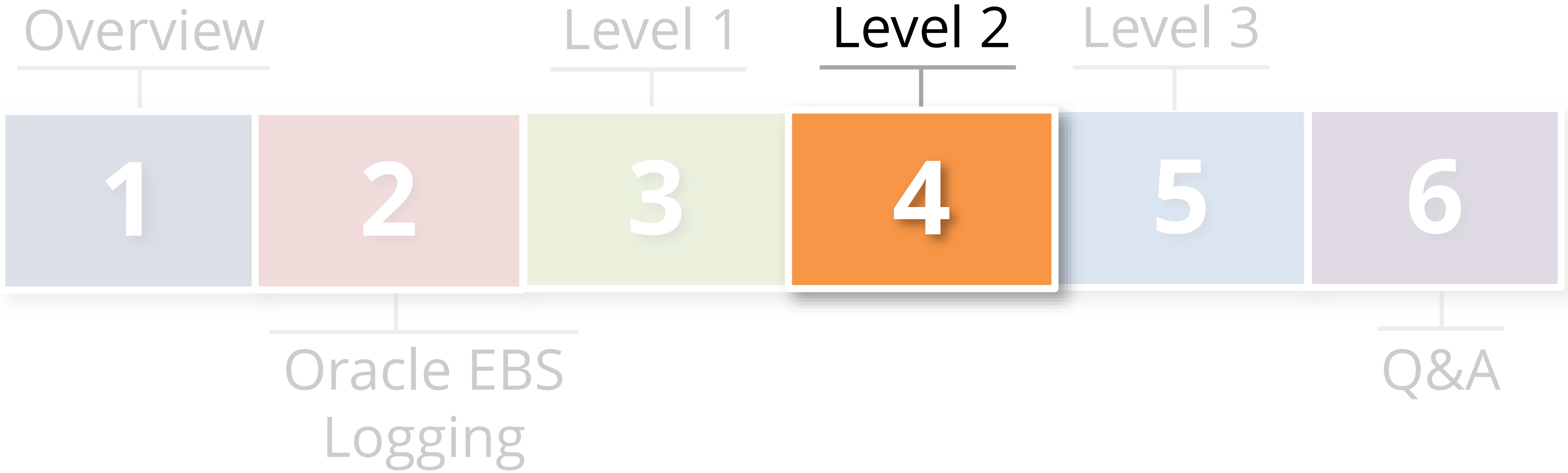
Level 1 – Recommended Alerts

Framework	What to Monitor For
E1	Direct database logins (successful or unsuccessful) to EBS schema database accounts
E1, E11	User SYSADMIN successful logins
E1, E11	Generic seeded application account logins
E1, E11	Unlocking of generic seeded application accounts
E1 **E2**	Login/Logoff

Framework	What to Monitor For
E3	User SYSADMIN - unsuccessful login attempts
E4	Modify authentication configurations to database
E4	Modify authentication configurations to Oracle E-Business Suite
E6	New database accounts created
E9, E10, E12, E13, E14	Updates to AOL tables under AuditTrail

Framework	What to Monitor For
E12	Turning Sign-On Audit off
E12	Turning off AuditTrail
E12	Turning Page Access Tracking off
E12	Turning Audit Trail off
E12	Turning audit sys operations off

Agenda



1 Overview

2 Oracle EBS Logging

3 Level 1

4 Level 2

5 Level 3

6 Q&A

Integrigy Framework – Level 2

Objectives

- Integrate Oracle Database and Oracle EBS with **centralized logging** for protection and alerting
- Use Oracle Database Syslog auditing functionality
- EBS logon and navigation activity retrieved

Tasks

1. **Implement centralized logging solution**
   - Use commercial or open source solutions
2. **Redirect database logs to centralized logging**
   - Use native Oracle Database Syslog auditing
3. **Use logging solution to retrieve EBS audit data**
4. **Transition level alerts and monitoring to logging solution**

Redirect Database Audit Log

- Configure database audit log to write to file in operating system rather than sys.aud$ table
  - Use Syslog for the log file format
- Feed Syslog formatted database logs to centralized logging solution

Pass End-User Navigation Activity

Table	Description
APPLSYS.FND_USERS	This is the base table defining all users and their associated email address and links to HR records
APPLSYS.FND_LOGINS	Sign-On Audit table
APPLSYS.FND_LOGIN_RESPONSIBILITIES	Sign-On Audit table
APPLSYS.FND_LOGIN_RESP_FORMS	Sign-On Audit table
APPLSYS.FND_UNSUCCESSFUL_LOGINS	Unsuccessful logins via the Personal Home Page (Self Service/Web Interface) are stored in both the FND_UNSUCCESSFUL_LOGINS and ICX_FAILURES tables.
ICX.ICX_FAILURES	The ICX_FAILURES table contains more information than the FND_UNSUCCESSFUL_LOGINS. Failed logins to the Professional Interface (Forms) are only logged to the FND_UNSUCCESSFUL_LOGINS tables.
JTF.JTF_PF_SES_ACTIVITY	Page Access Tracking Table
JTF.JTF_PF_ANON_ACTIVITY	Page Access Tracking Table
JTF.JTF_PF_REPOSITORY	Page Access Tracking Table
JTF.JTF_PF_LOGICAL_FLOWS	Page Access Tracking Table
APPLSYS.WF_USER_ROLE_ASSIGNMENTS	Need for E-Business end-user entitlements and role assignments
APPLSYS.FND_USER_RESP_GROUPS	Need for E-Business end-user entitlements and role assignments

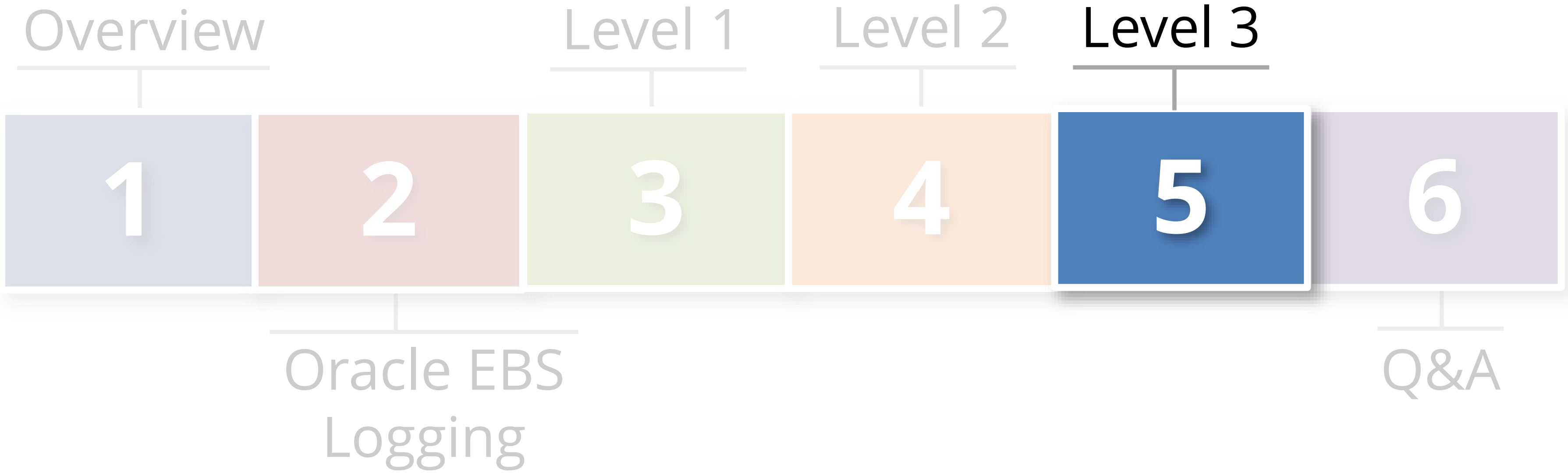
Framework:
E1, E2 & E3

Level 2 – Recommended Alerts

Framework	What to Monitor
E1	Successful or unsuccessful login attempts to E-Business without network or system login
E1	Successful or unsuccessful logins of named database user without network or system login
E3	Horizontal unsuccessful application attempts – more than 5 users more than 5 times within the hour
E3	Horizontal unsuccessful direct database attempts – more than 5 users more than 5 times within the hour

Framework	What to Monitor
E9	End-users granted System Administration Responsibility
E9	Addition or removal of privileges granted to user SYSADMIN
N/A	Monitor for database attacks

Agenda



1 Overview

2 Oracle EBS Logging

3 Level 1

4 Level 2

5 Level 3

6 Q&A

Integrigy Framework – Level 3

Objectives

- Extend logging to include **functional logging** and more complex alerting and monitoring
- Automate routine compliance activities
- Enhance and extend for continuous monitoring

Tasks

1. **Pass database logs and application server logs**
   - Use correlation to identify multi-layer incidents
2. **Extend to include EBS functional setups**
   - Focus on automating compliance activities
3. **Enhance and extend alerting, monitoring, and reporting for continuous monitoring**
   - Integrate people, processes, and technology

Additional Logs for Connection Activity

- **Apache logs**
  - Access, error, security, mod_rewrite

- **Database listener**
  - $TNS_ADMIN/listener.ora

- **Who is connecting from where and when**
  - Need for correlation

Oracle EBS Functional Activity

- **Extend Page Access Tracking**
  - Responsibilities
  - Applications
  - Key users

- **When and where are key users going within the Oracle E-Business Suite**

- **Complementary effort to Governance Risk and Compliance (GRC) implementation**

Governance Risk and Compliance (GRC)

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

This is a partial list for demonstration purposes only

Level 3 is Continuous

- **Continuous process**
  - Baseline expected activity
  - Define correlations
  - Build alerts and reports
  - Look for anomalies

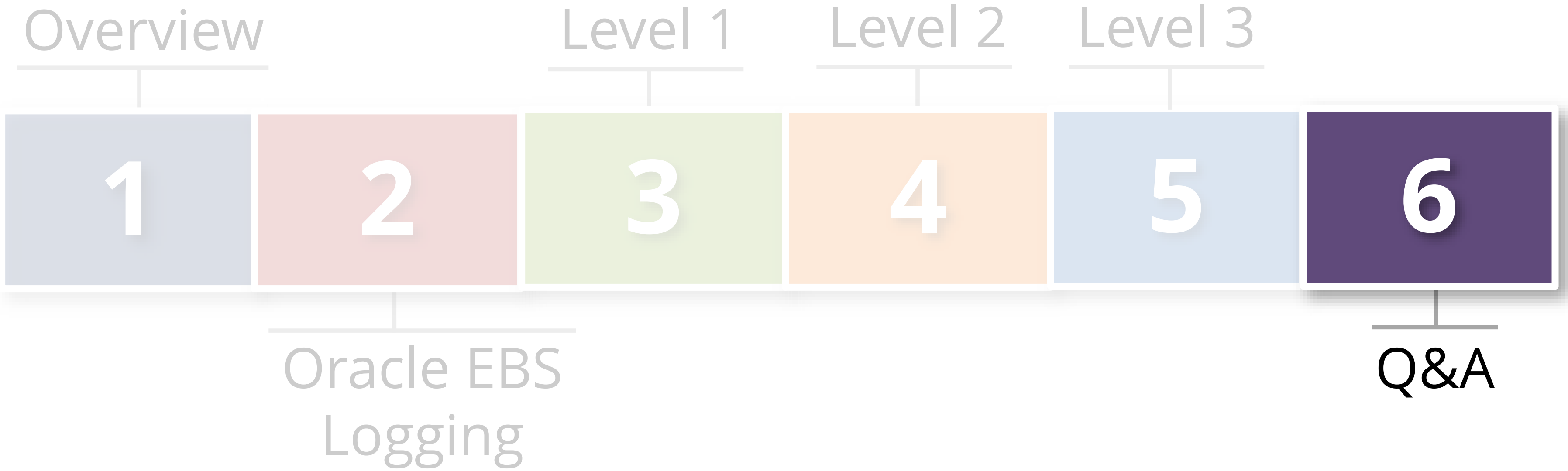
- **Continuous audit and operations monitoring**
  - Automated compliance

Level 3 – Recommended Alerts

Framework	What to Monitor
E1	Key functional setup and configuration activity
E1	SYSADMIN usage pattern
E6, E11	E-Business Suite Proxy user grants
E5, E11	Database account creation and privilege changes

Framework	What to Monitor
E13, E14	Reconcile creation and updates to Forms, Menus, Responsibilities, System Profiles and Concurrent Programs
E6	FND User email account changes
E14	Tables listed in APPLSYS.FND_AUDIT_TABLES

Agenda



1 Overview

2 Oracle EBS Logging

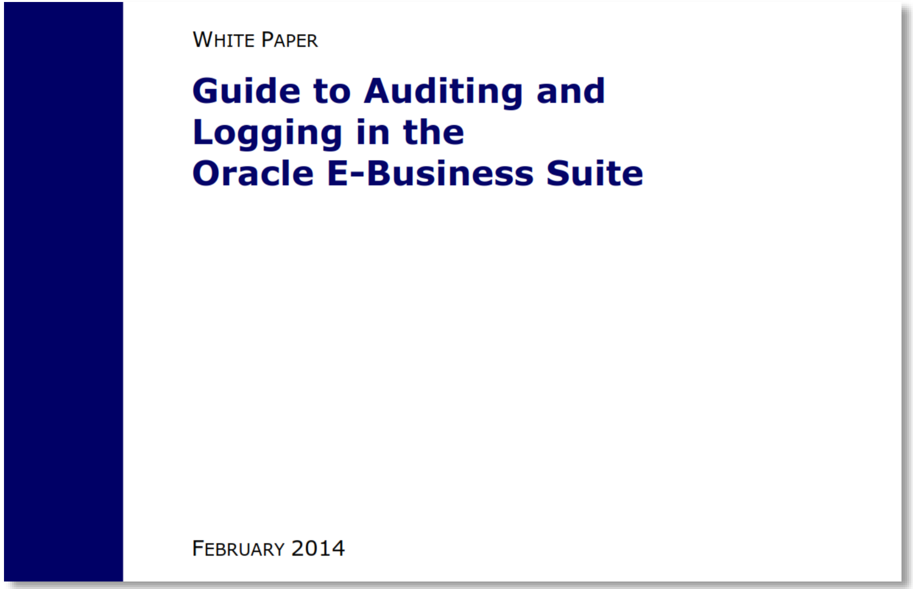
3 Level 1

4 Level 2

5 Level 3

6 Q&A

Integrigy Oracle EBS Whitepapers



WHITE PAPER

Guide to Auditing and Logging in the Oracle E-Business Suite

FEBRUARY 2014

This presentation is based on our recently updated Auditing and Logging whitepaper available for download at –

www.integrigy.com/security-resources

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**