ERP RISK ADVISORS.
Practical thought leadership in managing ERP risk.

INTEGRIGY

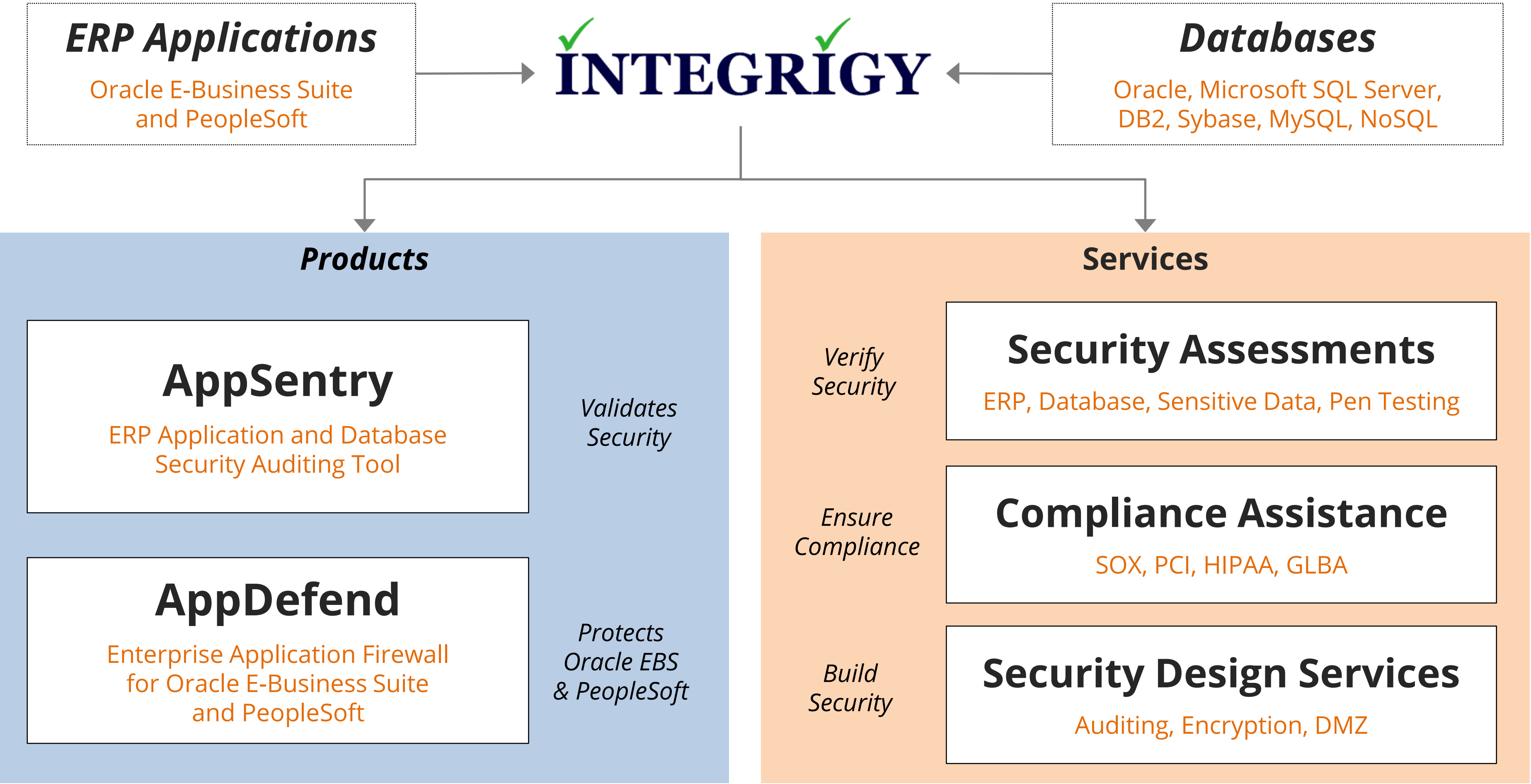
Effective Oracle E-Business Suite Change Management from DBA to Auditor

April 2, 2020

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Jeffrey Hare, CPA CISA CIA
Founder and CEO
ERP Risk Advisors

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 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

About ERP Risk Advisors

- Founded in 1998, 20+ years experience in providing Oracle Application Risk Advisory Services.
- Our mission: To provide companies with the best Compliance, Security, Risk Management, and Controls that reduces overall risks (and potential for fraud) in their ERP System.
- U.S. based – global clientele
- Partner with leading software providers and provide level 1 and 2 support for installed solutions
- Introduced our first product, ERP Armor, in 2019.

ERP ARMOR.
Design. Build. Test.

- Expanding to **ERPAaaS**, **ERP Armor: Rules** and **ERP Armor: Roles** in 2020.
- Prolific training experience, EBS and ERP Cloud through MISTI

Notable Clients

amazon

LinkedIn

amc

WESTERN UNION

FIRST AMERICAS
The First American Corporation

FRUIT OF THE LOOM

THE NOBLEST MOTIVE IS THE PUBLIC GOOD
COUNTY OF SAN DIEGO
MDCCCLI

GP STRATEGIES

Clayton homes

Agenda

1 Change Management Overview

2 Application Changes in Oracle EBS

3 Database Changes in Oracle EBS

4 Auditing Oracle EBS Changes

5 Q & A

Agenda

1 **Change Management Overview**

2 Application Changes in Oracle EBS

3 Database Changes in Oracle EBS

4 Auditing Oracle EBS Changes

5 Q & A

Change Management Definition

The Institute of Internal Auditors (IIA)
Global Technology Audit Guide (GTAG)
IT Change Management – 3rd Edition – February 2020

“Change management” is defined broadly as “the technology changes that affect an organization’s systems, programs, or applications.”

Change management controls are an integral part of an organization’s IT general controls (ITGCs), and in most organizations, the question isn’t whether a change management process exists; it’s whether the process is as effective and efficient as possible and is followed for all changes. Generally, effective change management can assist an organization in addressing risk, reducing unplanned work, limiting unintended results, and ultimately improving the quality of service for internal and external customers.

Change Management Definition

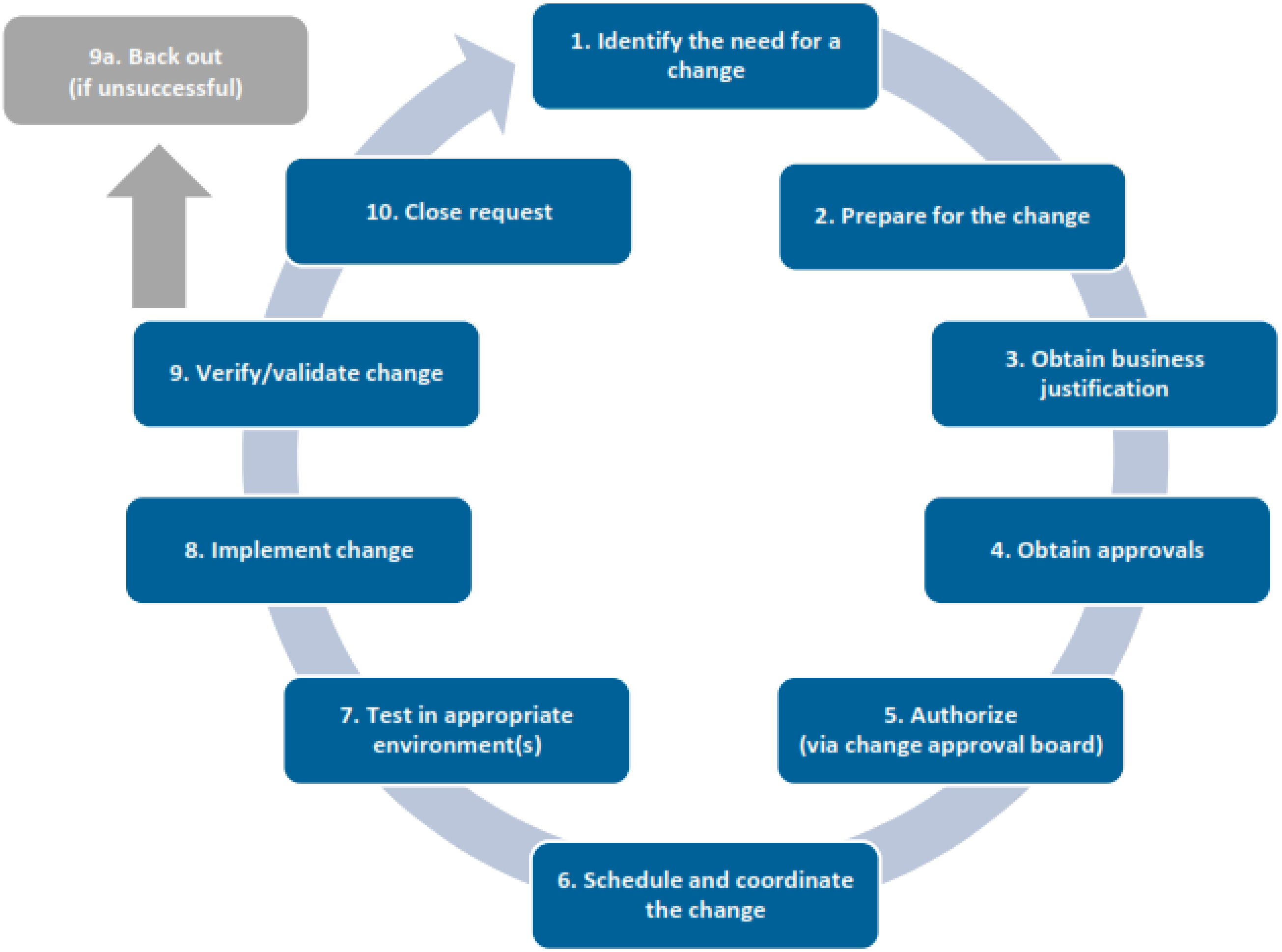
IT Governance Institute (ITGI) and ISACA
Control Objectives for Information and Related Technology (COBIT)
COBIT AI6 – Manage Changes

All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner. Changes are logged, assessed and authorized prior to implementation and reviewed against planned outcomes following the implementation. This process assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.

Effective Oracle EBS Change Management

- What is being changed, why it is being changed, and when it is being changed?
- Is change is properly authorized based on specific criteria?
- Who requested the change?
- Who is responsible for performing the change?
- Who is responsible for validating the change?
- How efficiently and effectively changes are implemented?
- Has the impact or potential problems of the change been quantified?
- How is the system monitored and audited to verify no authorized changes are occurring?

Effective Oracle EBS Change Management Process


1. Identify the need for a change
2. Prepare for the change
3. Obtain business justification
4. Obtain approvals
5. Authorize (via change approval board)
6. Schedule and coordinate the change
7. Test in appropriate environment(s)
8. Implement change
9. Verify/validate change
9a. Back out (if unsuccessful)
10. Close request

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	**Database** – use Integrigy AppSentry to test regularly **Application** – use ERP Armor as a Service 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 Contact Integrigy and ERP Risk Advisors for assistance
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 Contact Integrigy and ERP Risk Advisors for assistance

Oracle EBS Changes

- **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

Agenda

1 Change Management Overview

2 **Application Changes in Oracle EBS**

3 Database Changes in Oracle EBS

4 Auditing Oracle EBS Changes

5 Q & A

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

Security – Application (Roles and Responsibilities)

Change Management Role	Job Role
Requestor	Process Owner
Preparer	Business Analyst
Approver	Process Owner IT Management / Steering Committee
Peer Reviewer – i.e. SoD/SA checking	Compliance / Internal Audit
Implementor	Varies… ideally DBA
Verifier	IT Compliance

Expected testing / validation

- Positive and negative testing by process owner
- SoD conflicts and sensitive access risk testing – full scan / what if analysis
- Confirmation of changes after being moved to Production

Oracle EBS Application Changes

- **Any configuration or setup in EBS that may impact one or more of the following –**
  - processing of transactions or reporting material to financial statements
  - application preventative or detective controls
  - application security
- **Application seed data that may impact application transactions or reporting**
- **Application patches**
  - including application technology patches (AOL)

Change Management Challenges

- Application configurations and setups are stored in many different database tables
- Up to 500 different database tables may have to be audited to monitor the full population of application changes
- Application patches are applied by a generic user and no information is recorded about who applied the patch

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

Configurations – Application (Functional Configurations)

Change Management Role	Job Role
Requestor	Process Owner
Preparer	Business Analyst
Approver	Process Owner IT Management / Steering Committee
Peer Reviewer (i.e., SoD/SA checking)	Compliance / Internal Audit
Implementor	Varies… ideally DBA / Different Business Analyst
Verifier	IT Compliance
Expected testing / validation ▪ Positive and negative testing by process owner ▪ Confirmation of changes after being moved to Prod.	

Patches – Application or Database

Change Management Role	Job Role
Requestor	DBA
Preparer	DBA
Approver	IT Management / Steering Committee
Peer Reviewer	N/A
Implementor	DBA
Verifier	IT Compliance

Expected testing / validation – database and server patches

- Positive and negative testing by process owners – major processes
- Confirmation of changes after being moved to Production

Expected testing / validation – application patches

- Positive and negative testing by process owners – full unit and regression testing
- Confirmation of changes after being moved to Production

Agenda

1 Change Management Overview

2 Application Changes in Oracle EBS

3 **Database Changes in Oracle EBS**

4 Auditing Oracle EBS Changes

5 Q & A

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

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
  - Configurations, Extensions, Modifications, Localizations, Integrations
- RICE
  - Reports, Interfaces, Conversions and Enhancements

Change Management Challenges

- Development is done in the application UI, in the database using SQL statements, and in the operating system with many different types of files (SQL scripts, PL/SQL code, forms, web pages, shell scripts, etc.)

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 - 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

Customizations and Development Objects

Change Management Role	Job Role
Requestor	Process owner
Preparer	Developer Security Administrator – deploy to Responsibilities
Approver	Process Owner IT Management / Steering Committee
Peer Reviewer	Different developer
Implementor	DBA – move object / register object Security Administrator – deploy to Responsibilities
Verifier	IT Compliance
Expected testing / validation ▪ Positive and negative testing by process owner ▪ Confirmation of changes after being moved to Production	

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**

Agenda

1 Change Management Overview

2 Application Changes in Oracle EBS

3 Database Changes in Oracle EBS

4 **Auditing Oracle EBS Changes**

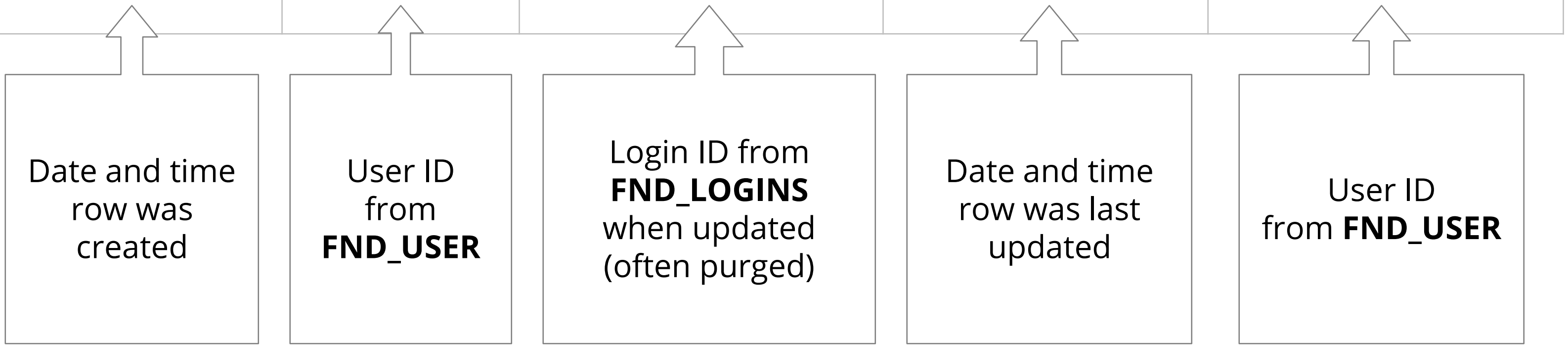
5 Q & A

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 captured.** In Forms, use *About this Record*. In HTML, enable FND Diagnostics and use *About this Page*.

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

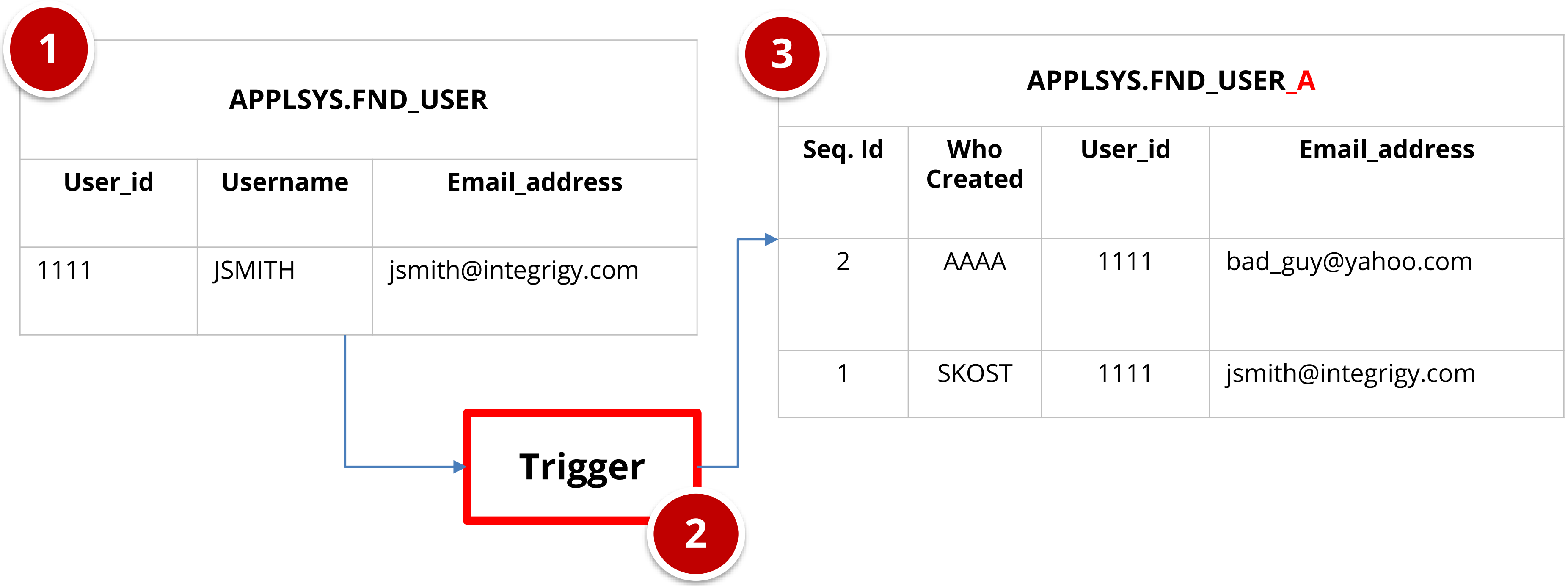
User ID from **FND_USER**

Oracle EBS Auditing and Logging Methods

EBS Sign-on Audit	▪ Captures logins, responsibility selection, and form usage.
EBS Page Access Tracking (PAT)	▪ Tracks Oracle Applications Framework (OAF) page usage.
EBS Module Specific	▪ Certain EBS modules capture changes or information on activity. One example is HCM Date Tracking.
EBS Audit Trails	▪ EBS managed triggers on defined tables to capture changes to specific columns.
Snapshot/Trigger	▪ Third-party tools to snapshot data or perform trigger-based auditing. Trigger-based is preferred as it captures all changed, however, more expensive to implement and maintain. ▪ **Trigger** = Caosys CS*Audit, Fastpath, SafePaas, Oracle GRC (end of life) ▪ **Snapshot** = Integrigy AppSentry, ConfigSnapshot

Oracle EBS Audit Trails

EBS Audit Trails functionality stores row changes to EBS tables in **shadow tables** using database triggers. Only tracks insert, update, and deletes to tables defined in Oracle EBS. See MOS Note ID 60828.1 for more information.



1

APPLSYS.FND_USER

User_id	Username	Email_address
1111	JSMITH	jsmith@integrigy.com

2

Trigger

3

APPLSYS.FND_USER_A

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

Minimum Set of Oracle EBS Audit Trails Tables

- **Audit Trail tables**
  - **EBS security** – users, responsibilities, menus, functions, …
  - **EBS configuration** – system profile options
  - **EBS customizations** – forms, executables, concurrent programs, alerts
  - **EBS module configuration** – flex fields, data groups, …
  - **EBS Audit Trails configuration**
- **Inclusion criteria**
  - High security, compliance, or change impact
  - Low volume
  - Limited master data tables such as vendor bank accounts
  - No transactional tables

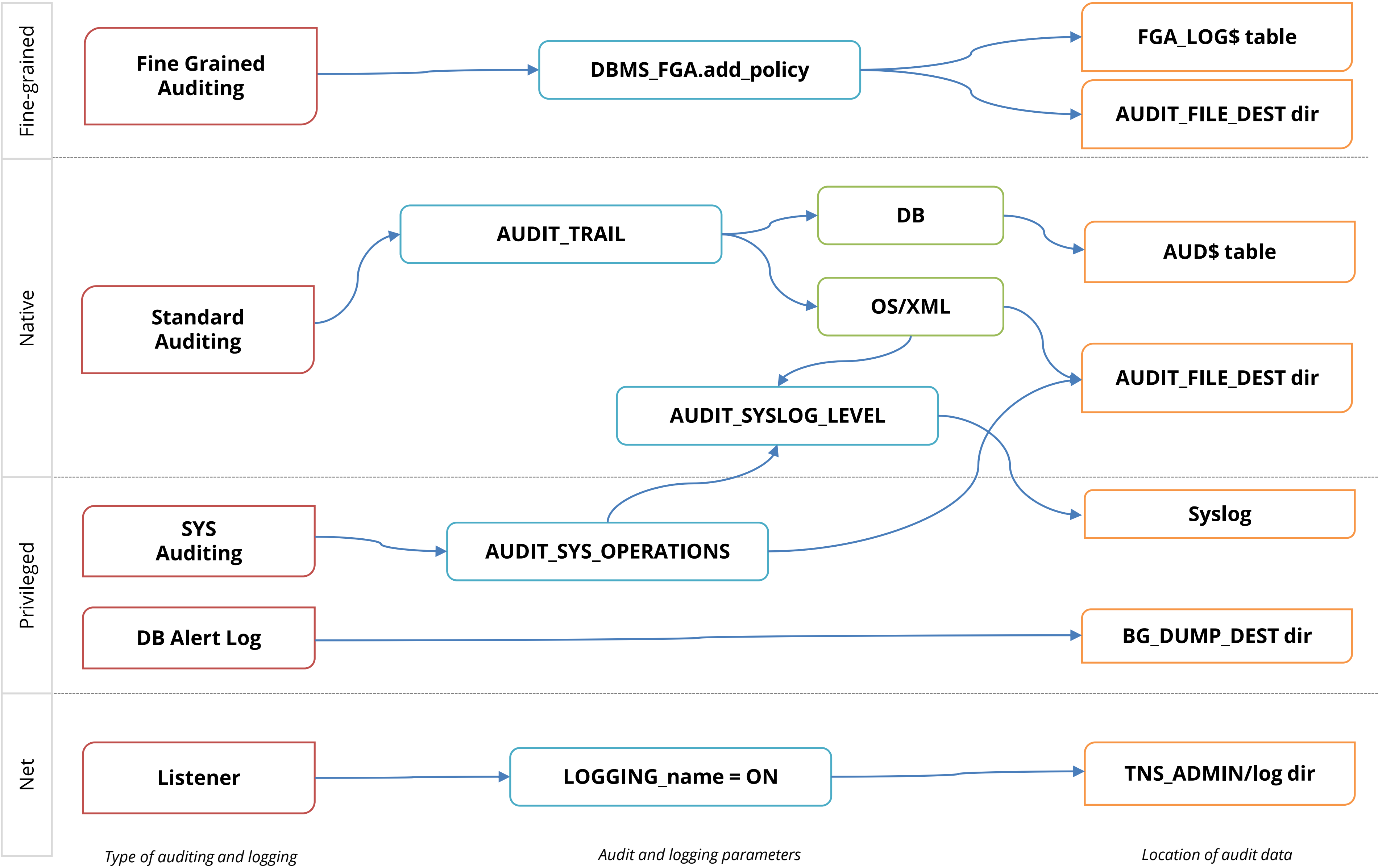
Framework Events	Oracle EBS Audit Trail Tables
E4 - Modify authentication mechanisms	FND_PROFILE_OPTIONS (also E12, E14) FND_PROFILE_OPTION_VALUES (also E12, E14)
E5 - Create user account **E6 - Modify user account**	FND_USER
E7 - Create role **E8 - Modify role**	FND_RESPONSIBILITY
E9 - Grant/revoke 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

Expanded Set of Oracle EBS Audit Trails Tables

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

Oracle Database Auditing and Logging



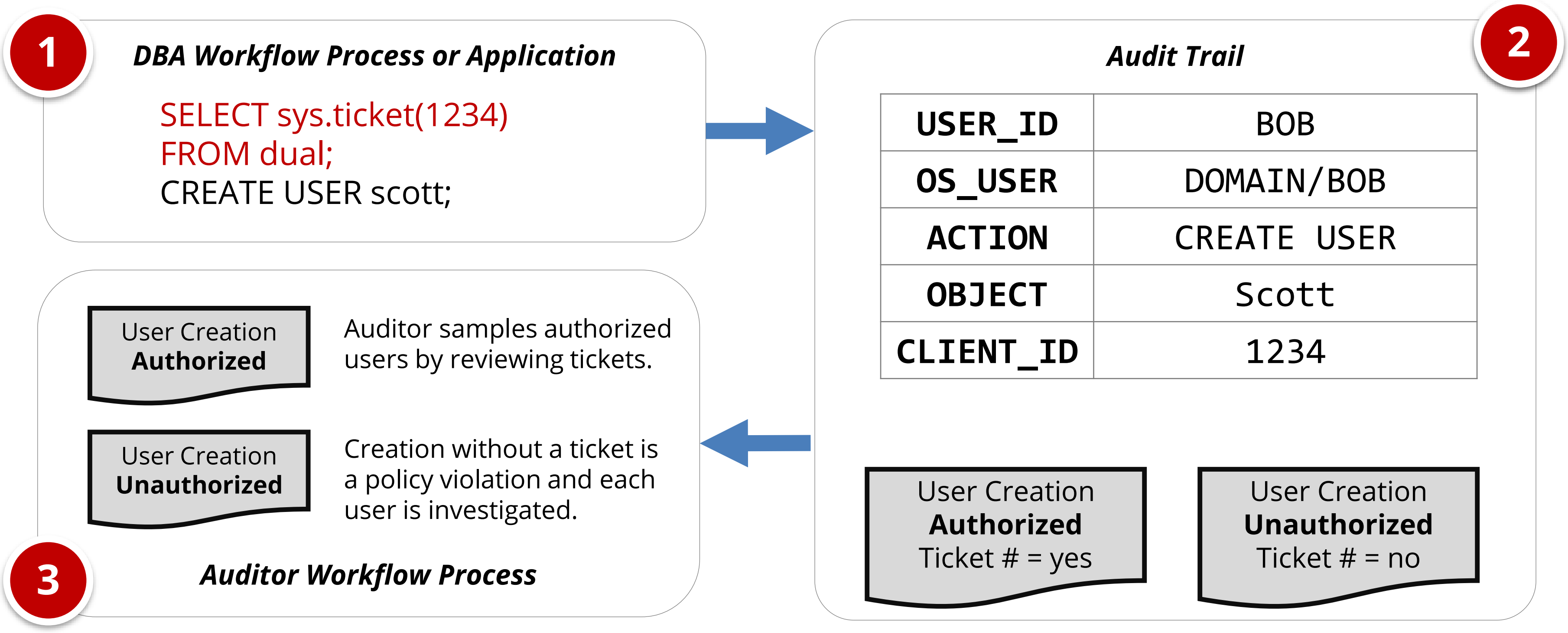
Oracle EBS Database Change Auditing

Framework Event	Object	Oracle Audit Statement	Resulting Audited SQL Statements
E1, E2, E3	**Session**	session	Database logons and failed logons
E5, E6	**Users**	user	create/alter/drop user
E7, E8	**Roles**	role	create/alter/drop role
E13	**Database Links** **Public Database Links**	database link public database link	create/drop database link create/drop public database link drop public database link
E11	**System**	alter system	alter system
E14	**Database**	alter database	alter database
E9, E10	**Grants (system privileges and roles)**	system grant	grant revoke
E4	**Profiles**	profile	create/alter/drop profile
E11, E14	**SYSDBA and SYSOPER**	sysdba sysoper	All SQL executed with sysdba and sysoper privileges

See Integrigy Framework whitepaper for complete database auditing recommendations

Change Management Tracking – Create User Example

Capture change ticket numbers and other information for a database session based on special SQL executed by database users or applications.



1

DBA Workflow Process or Application

```
SELECT sys.ticket(1234)
FROM dual;
CREATE USER scott;
```

2

Audit Trail

USER_ID	BOB
OS_USER	DOMAIN/BOB
ACTION	CREATE USER
OBJECT	Scott
CLIENT_ID	1234

User Creation
Authorized
Ticket # = yes

User Creation
Unauthorized
Ticket # = no

User Creation
Authorized

Auditor samples authorized users by reviewing tickets.

User Creation
Unauthorized

Creation without a ticket is a policy violation and each user is investigated.

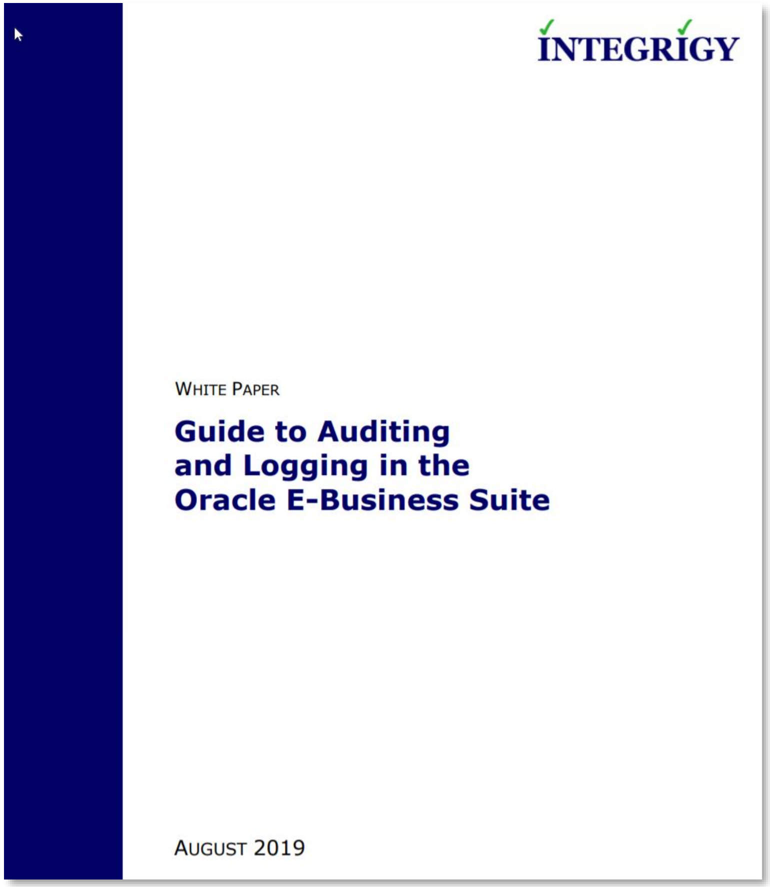
3

Auditor Workflow Process

Oracle EBS Centralized Logging

- **Integrate Oracle EBS with centralized logging solution to capture, protect, and report on audit data**
  - Use Splunk, ElasticSearch, AppSentry, or other commercial solutions
  - Purpose built functionality for correlation, monitoring, and unified alerting
- **Audit data must be retrieved from multiple database tables and operating system files**
  - No single source of audit data within Oracle EBS
- **Oracle EBS Audit Data Sources**
  - Database Audit Trail = AUD$, FGA_LOG$
  - Database SYS Audit Trail = adump/*.xml (1 file per session)
  - EBS Sign-on Audit = FND_LOGIN*, … (5 total)
  - EBS Page Access Tracking = JTF_PF_* (7 total)
  - EBS Audit Trails = shadow tables *_A (one per table – 25 to 200 total tables)

Integrigy Oracle EBS Whitepapers



INTEGRIGY

White Paper

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

August 2019

The Integrigy Framework for Auditing and Logging in Oracle E-Business Suite is available for download from our website.

www.integrigy.com/security-resources

Agenda

1 Change Management Overview

2 Application Changes in Oracle EBS

3 Database Changes in Oracle EBS

4 Auditing Oracle EBS Changes

5 Q & A

Integrigy and ERP Risk Advisors 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**

Jeffrey Hare, CPA CISA CIA
Founder and CEO
ERP Risk Advisors

web – **www.erpra.net**
e-mail – **info@erpra.net**
linkedin – **linkedin.com/company/erp-risk-advisors**
youtube – **https://www.youtube.com/channel/UCP9VwHbnX3gZqO0kP9E8TxQ**

Copyright © 2020 Integrigy Corporation and ERP Risk Advisors