



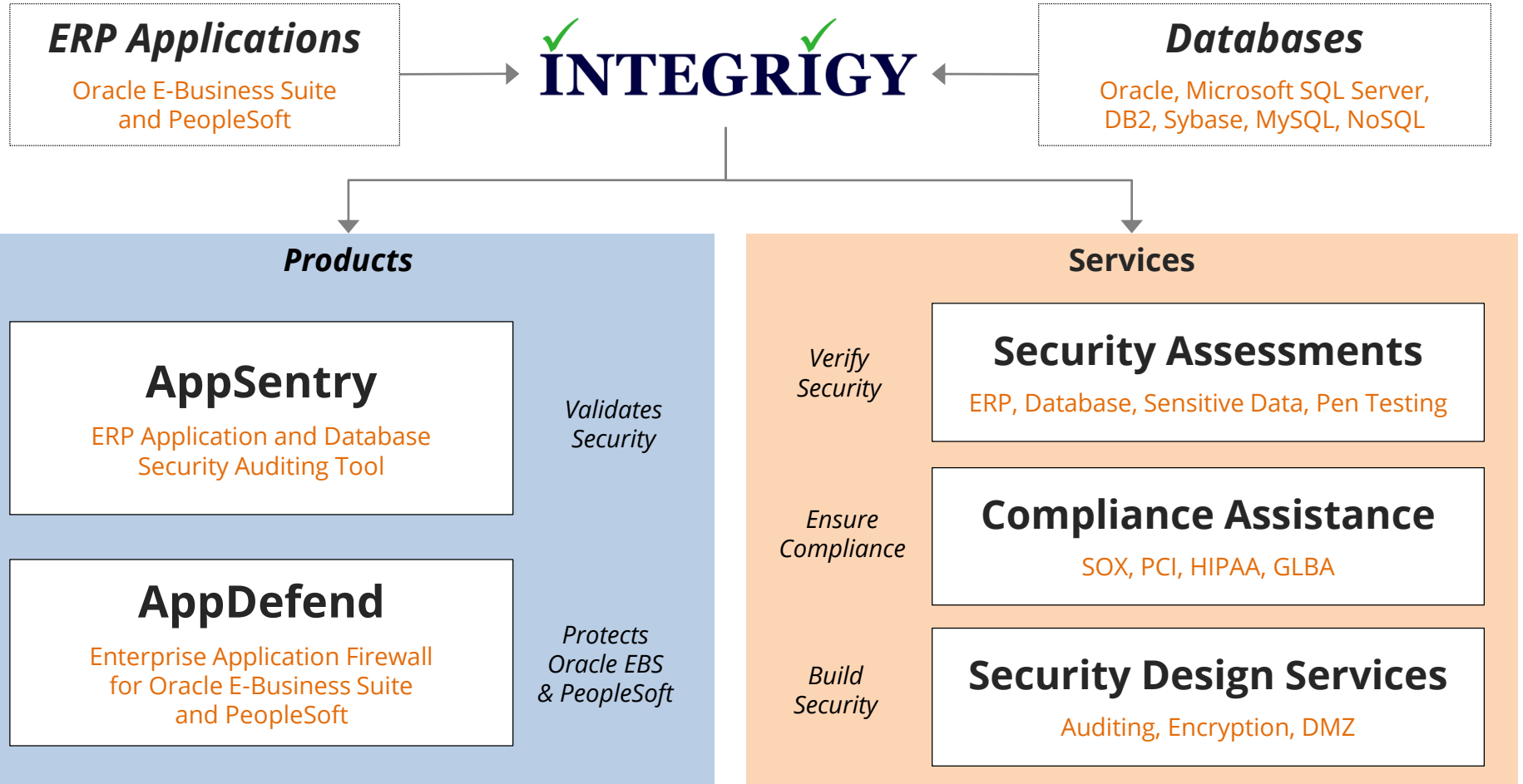
Effective Auditing and Logging in Oracle E-Business Suite

October 24, 2019

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy



Integrigy Research Team

ERP Application and Database Security Research

Agenda

1

Logging and Auditing Framework

2

Oracle E-Business Suite

3

Oracle Database

4

Centralized Logging, Alerts, and Reports

5

Q & A

Agenda

1

Logging and Auditing Framework

2

Oracle E-Business Suite

3

Oracle Database

4

Centralized Logging, Alerts, and Reports

5

Q & A

Auditing and Logging the Oracle E-Business Suite

- **Audit and log in order to monitor, alert, and report on key activity and events in the Oracle EBS**
 - Requires multiple disciplines and teams to define
- **Requirements are usually difficult to clearly define**
 - Technical, Compliance, Internal Audit, and IT Security
 - DBAs often are not provided clear requirements
- **The Oracle Database and Oracle EBS offer rich log and audit functionality**
 - **Most organizations do not fully take advantage**

Auditing and Logging Requirements Definition

The Auditing and Logging requirements and design must address the following four steps –

| | |
|------------------|--|
| Capture | What activity or events must be captured? |
| Retention | How is the audit trail to be stored, protected, and archived? |
| Alert | What alerts should be generated in real-time for specific events or actions that may indicate a compromise or violation? |
| Report | What reports should be delivered to whom and how frequently? Are those individual qualified to review the reports? (Control effectiveness) |

Auditing and Logging Definition Wrong Answers

- **“All changes”**

- There are hundreds of types of changes in an Oracle EBS environment. Capturing all changes is not realistic and would produce massive volumes of data.

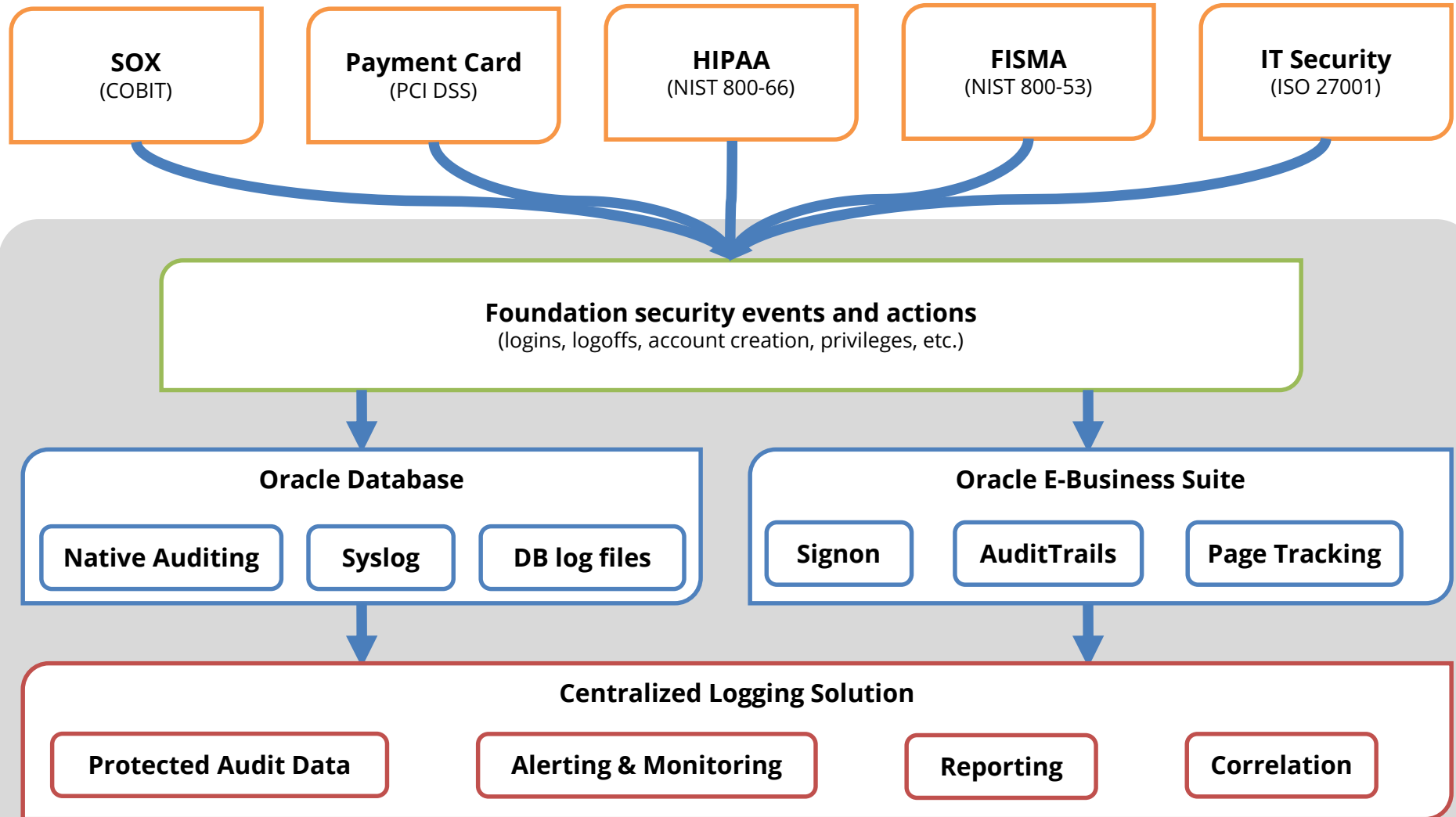
- **“DBAs must review the audit trail daily”**

- For segregation of duties, the DBAs should only be reviewing portions of the audit trail. The database audit trail captures SQL statements – who is qualified to review these reports?

- **“All critical activity back to a named user”**

- Oracle EBS is very challenging to track DBA activity to a named DBA due to the use of the SYS, SYSTEM, and APPS database accounts.

Integrigy Framework for EBS Auditing and Logging



Integrigy Framework Events


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.

| | |
|---|---|
| <i>E1 - Login</i> | <i>E8 - Modify role</i> |
| <i>E2 - Logoff</i> | <i>E9 - Grant/revoke user privileges</i> |
| <i>E3 - Unsuccessful login</i> | <i>E10 - Grant/revoke role privileges</i> |
| <i>E4 - Modify auth mechanisms</i> | <i>E11 - Privileged commands</i> |
| <i>E5 - Create user account</i> | <i>E12 - Modify audit and logging</i> |
| <i>E6 - Modify user account</i> | <i>E13 - Create, Modify or Delete object</i> |
| <i>E7 - Create role</i> | <i>E14 - Modify configuration settings</i> |

Integrigy Framework 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 EBS |
| Level 3 | Extend logging to include functional logging and more complex alerting and monitoring |

Agenda

1

Logging and Auditing Framework

2

Oracle E-Business Suite

3

Oracle Database

4

Centralized Logging, Alerts, and Reports

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 | <ul style="list-style-type: none">▪ Captures logins, responsibility selection, and form usage. |
| EBS Page Access Tracking (PAT) | <ul style="list-style-type: none">▪ Tracks Oracle Applications Framework (OAF) page usage. |
| EBS Audit Trails | <ul style="list-style-type: none">▪ EBS managed triggers on defined tables to capture changes to specific columns. |
| EBS Module Specific | <ul style="list-style-type: none">▪ Certain EBS modules capture changes or information on activity. One example is HCM Date Tracking. |
| Snapshot/Trigger | <ul style="list-style-type: none">▪ 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▪ Snapshot = Integrigy AppSentry, ConfigSnapshot |

Oracle EBS Sign-on Audit

Standard EBS functionality to log logins, responsibility use, and Forms navigation. Enabled by the system profile option **Sign-on: Audit Level** and the default is None (12.1) or Form (12.2).

| 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.

- **Enabled through Oracle Applications Manager**
 - Monitoring -> Application Usage Reports -> Configuration
 - Select level of monitoring and applications to be tracked
- **For reporting, concurrent program must be scheduled to populate data**

| 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 Other Logging

Unsuccessful Logins

EBS Report

- Signon Audit Unsuccessful Logins

EBS Tables

- APPLSYS.FND_UNSUCCESSFUL_LOGINS
- ICX.ICX_FAILURES

Concurrent Requests

EBS Report

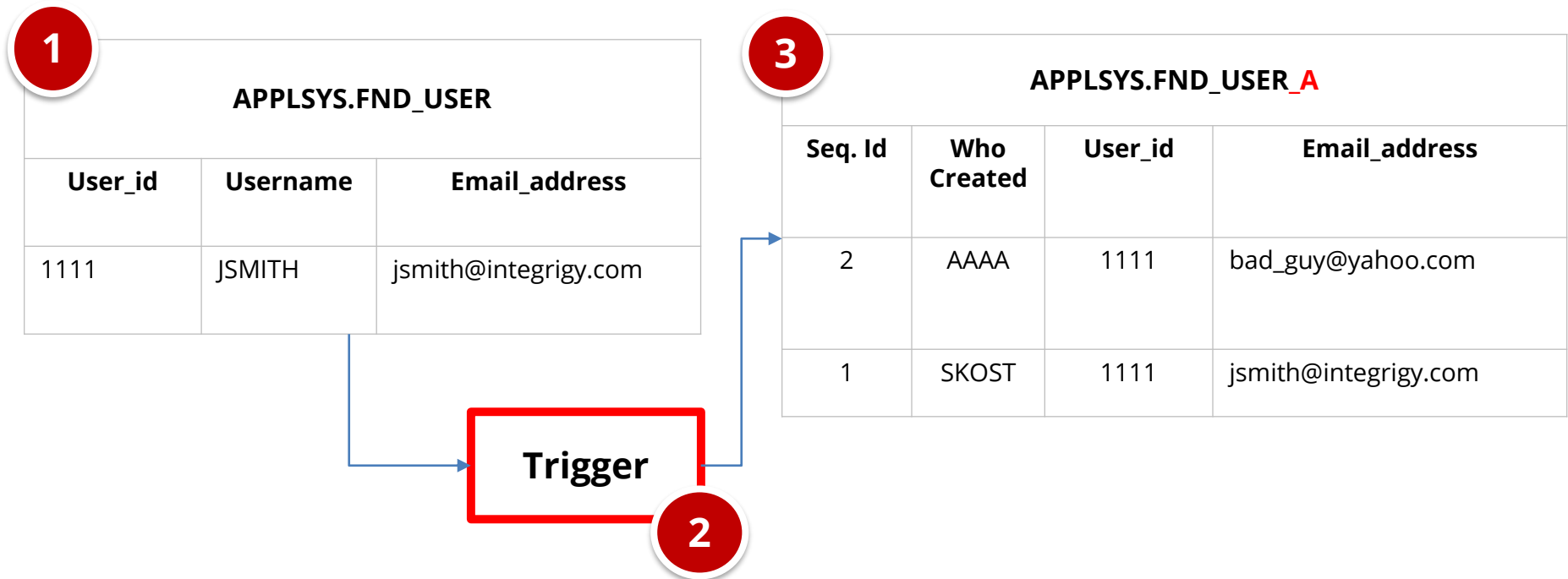
- Signon Audit Concurrent Requests

EBS Tables

- APPLSYS.FND_CONCURRENT_REQUESTS

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.



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_MENU 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 |

Agenda

1

Logging and Auditing Framework

2

Oracle E-Business Suite

3

Oracle Database

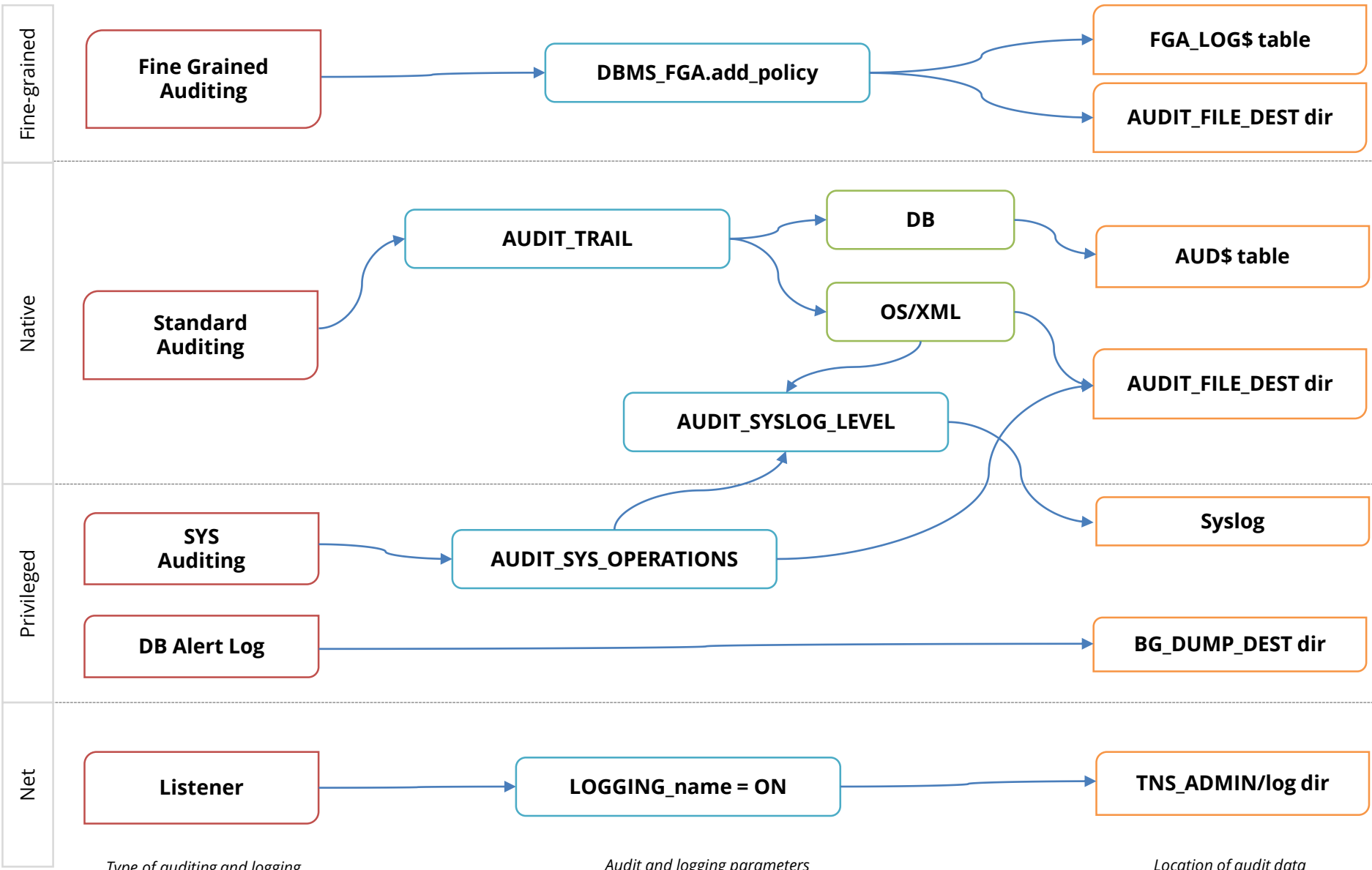
4

Centralized Logging, Alerts, and Reports

5

Q & A

Oracle Database Auditing and Logging



Type of auditing and logging

Audit and logging parameters

Location of audit data

Oracle Database Auditing and Logging Methods

| | |
|---------------------------------|--|
| Native Database Auditing | <ul style="list-style-type: none">▪ Auditing of SQL statements in the database based on enabled audits.▪ Can be written to database (AUD\$), OS, or Syslog. |
| SYS Operations Auditing | <ul style="list-style-type: none">▪ Auditing of all SQL statements executed by SYS user and SYSDBA role.▪ Only written to OS or Syslog, not the database. |
| Fine-grained Auditing | <ul style="list-style-type: none">▪ Auditing of specific SQL statements based on audit rules such as column > 10000.▪ Written to FGA_LOG\$. |

Oracle Database 12c and 19c Auditing Changes

- **Oracle Database 12c introduced new auditing functionality – Unified Auditing**
 - Single audit trail location (UNIFIED_AUDIT_TRAIL) consolidating database audit trail (AUD\$), fine-grained auditing (FGA_LOG\$), and Database Vault (DVSYS.AUDIT_TRAIL\$)
 - Additional features include audit policies, auditing custom roles, new auditing schema (AUDSYS)
 - Bugs and performance issues in 12.1, resolved in 19c
 - No writing audit trail to Syslog in 12.1, added in 18c
- **Traditional (pre-12c) auditing is still available in 12c and 19c**

Recommended Database Logging – Security Events

| 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 Integrity Framework whitepaper for complete database auditing recommendations

Change Ticket Tracking - Create User Example

Capture 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

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

User Creation
Authorized
Ticket # = yes

User Creation
Unauthorized
Ticket # = no

Agenda

1

Logging and Auditing Framework

2

Oracle E-Business Suite

3

Oracle Database

4

Centralized Logging, Alerts, and Reports

5

Q & A

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

Centralized Logging – Oracle Database

- **Send Oracle Database audit trail to external logging solution using Syslog**
 - Available starting with 10.2 – not available in 12.1
 - AUDIT_TRAIL=OS
 - AUDIT_SYSLOG_LEVEL = "facility.priority"
 - Configure host Syslog to forward to external collector
 - Can be configured to write to local syslog for DBAs
- **Sent in near real-time, so audit trail is protected**
- **Database audit trail and SYS operations included**
 - FGA auditing is not included and still stored in FGA_LOG\$ - fixed in 19c

Centralized Auditing – Oracle EBS

- **All audit and logging data stored in multiple database tables**
 - Sign-on Audit = FND_LOGIN*, ... (5 total)
 - Page Access Tracking = JTF_PF_* (7 total)
 - Audit Trails = shadow tables *_A (one per table – 25+ total)
- **Configure centralized logging solution to retrieve data from tables periodically**
 - Splunk DB Connect add-on
 - Use views or queries to de-normalize data for readability and to avoid look-up in logging solution

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 tables under Audit Trails |

| 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 |

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 <u>application</u> attempts – more than 5 users more than 5 times within the hour |
| E3 | Horizontal unsuccessful <u>direct database</u> 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 <ul style="list-style-type: none">Logins to standard unused database accounts like CTXSYS |

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 |

Next Steps – Additional Log Files

- **Apache logs**
 - Access, error, security, mod_rewrite
- **Oracle Database alert log**
 - alert.log
- **Database listener log**
 - listener.log/log.xml
- **Correlation within logging solution**
 - FND_LOGIN to IP address

Next Steps – Oracle EBS Audit Trails

| 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

Agenda

1

Logging and Auditing Framework

2

Oracle E-Business Suite

3

Oracle Database

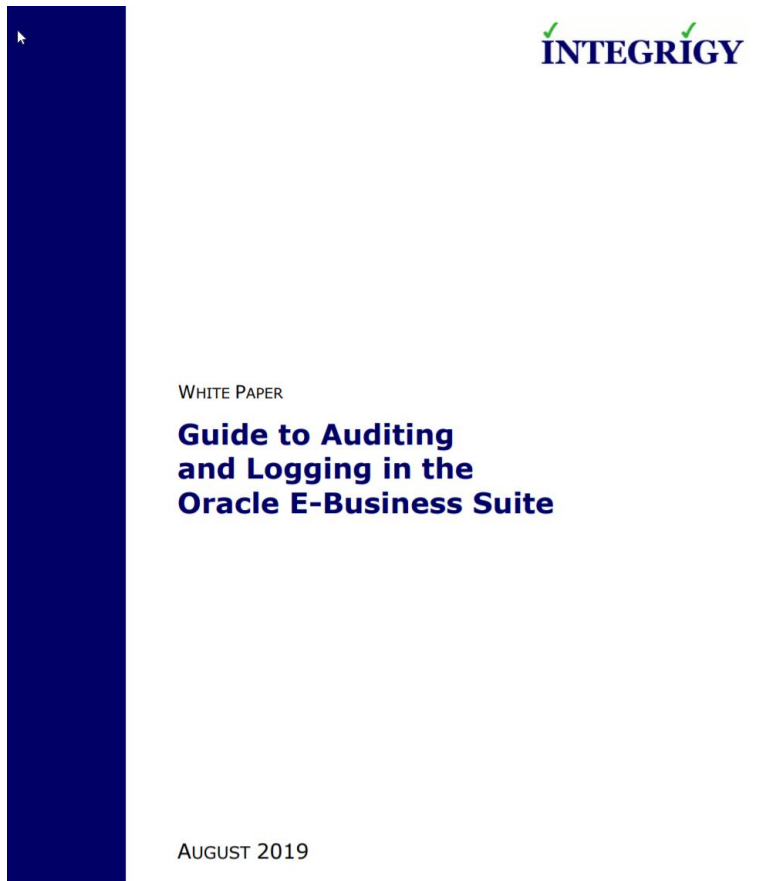
4

Centralized Logging, Alerts, and Reports

5

Q & A

Integrigy Oracle EBS Whitepapers



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

www.integrigy.com/security-resources

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**