INTEGRIGY

Oracle Database
Logging and Auditing

January 15, 2015

Mike Miller
Chief Security Officer
Integrigy Corporation

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

Agenda

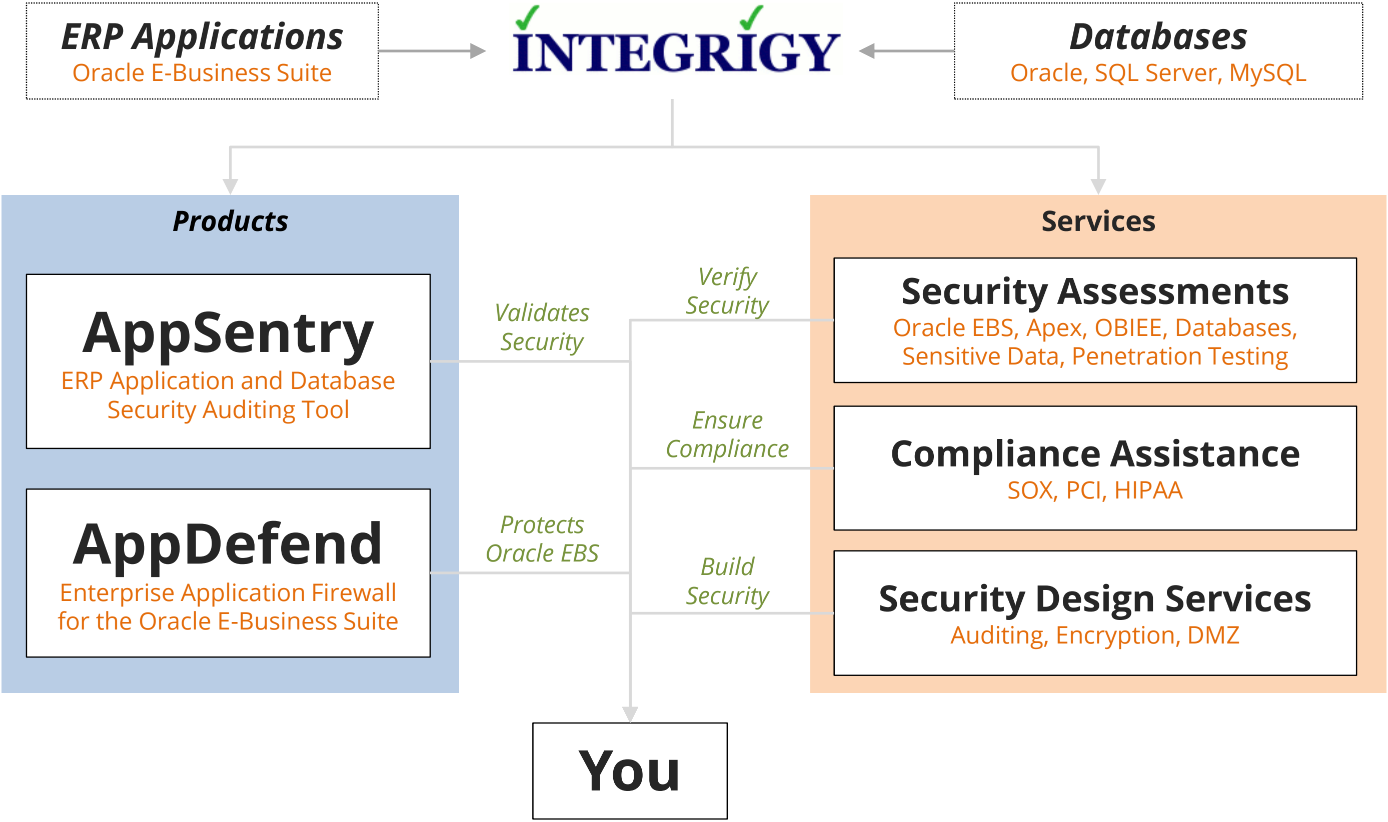
1 Overview

2 Oracle Auditing

3 Integrigy Log & Audit Framework

4 Q&A

About Integrigy



ERP Applications
Oracle E-Business Suite

INTEGRIGY

Databases
Oracle, SQL Server, MySQL

Products

AppSentry
ERP Application and Database Security Auditing Tool

Validates Security

AppDefend
Enterprise Application Firewall for the Oracle E-Business Suite

Protects Oracle EBS

Services

Verify Security

Security Assessments
Oracle EBS, Apex, OBIEE, Databases, Sensitive Data, Penetration Testing

Ensure Compliance

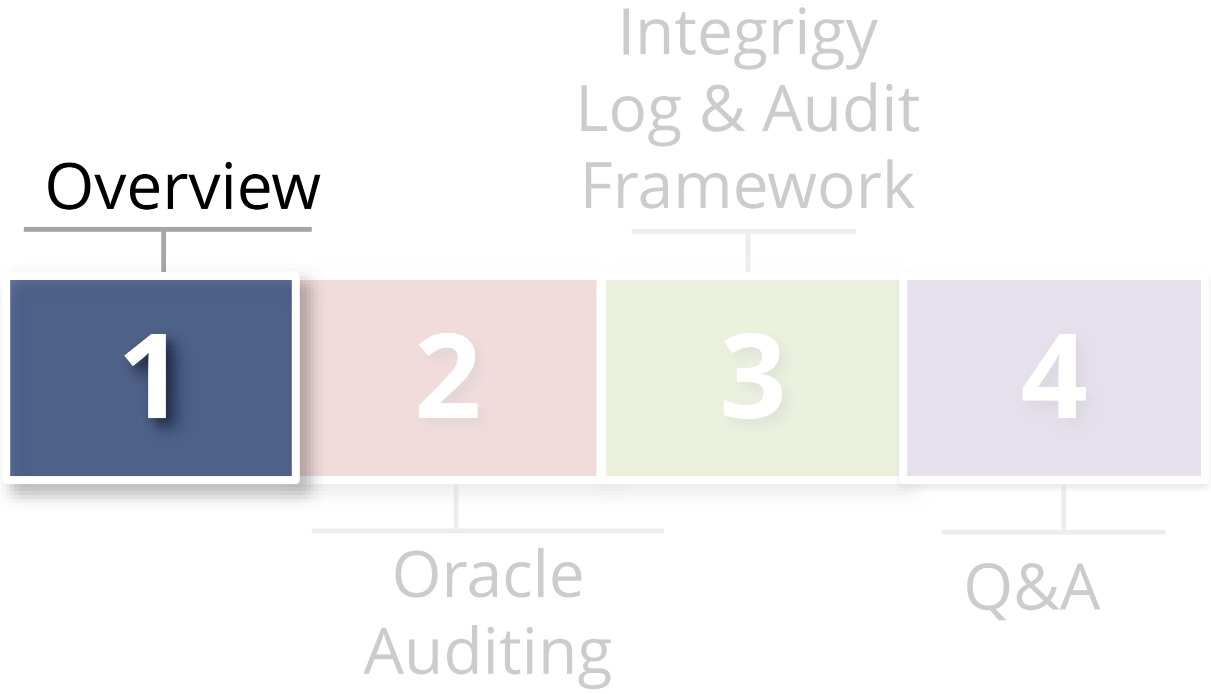
Compliance Assistance
SOX, PCI, HIPAA

Build Security

Security Design Services
Auditing, Encryption, DMZ

You

Agenda



1 Overview

2 Oracle Auditing

3 Integrigy Log & Audit Framework

4 Q&A

Security Is A Process

- **Tools do not provide security, people do**
  - Tools only enable and automate

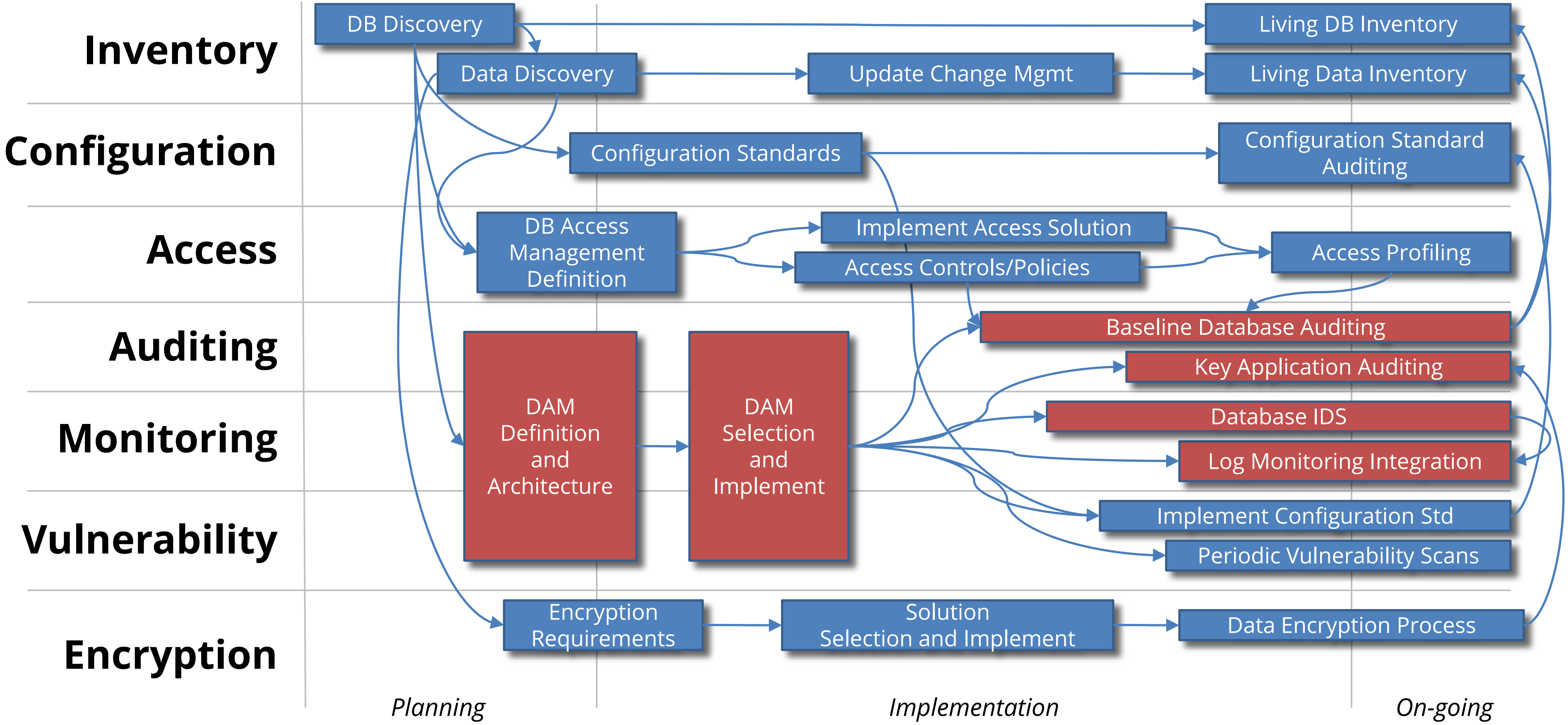
- **Security is not provided by any one product, upgrade, or patch**
  - Security provided by on-going lifecycle and configuration management

- **Database security is a process**
  - Auditing is only one of several required tools to be used to provide database security

Database Security Program Components

Inventory	▪ An inventory of all databases and sensitive data locations ▪ Methods and processes to maintain the inventories
Configuration	▪ A measureable database security standard and baseline ▪ Periodic validation with compliance to the standard
Access	▪ Database access management policies, procedures, and tools ▪ Database access profiling and monitoring
Auditing	▪ Database auditing requirements, processes, and definitions ▪ Centralized auditing retention and reporting solution
Monitoring	▪ Database real-time security monitoring and intrusion detection ▪ Database monitoring definition and tools
Vulnerability	▪ Vulnerability assessment and management for databases ▪ Vulnerability remediation strategy and processes
Encryption	▪ Database encryption requirements, strategy, and toolset for protecting sensitive data

Database Security Process



Inventory

DB Discovery

Data Discovery

Update Change Mgmt

Living DB Inventory

Living Data Inventory

Configuration

Configuration Standards

Configuration Standard Auditing

Access

DB Access Management Definition

Implement Access Solution

Access Controls/Policies

Access Profiling

Auditing

Baseline Database Auditing

Key Application Auditing

Monitoring

DAM Definition and Architecture

DAM Selection and Implement

Database IDS

Log Monitoring Integration

Vulnerability

Implement Configuration Std

Periodic Vulnerability Scans

Encryption

Encryption Requirements

Solution Selection and Implement

Data Encryption Process

Planning

Implementation

On-going

Auditing and Logging

- **Log to enable audit, monitor, and alert**
  - Related but separate disciplines
- **Requirements are difficult**
  - Technical, Compliance, Audit, and Security
- **Need information as basis for action**
  - **Most organizations ignore or underutilize auditing**

Zero Value Database Auditing

Database auditing in most organizations done simply for a **compliance checkbox**.

- **Not using auditing**
- **Auditing poorly defined**
- **No review of audit data**
- **No mapping of business requirements to auditing, alerts, or reports**
- **Zero value to the organization**

Fidelity is the Key to Auditing

Done Wrong	Done Right
System performance impacted	No impact or system overhead
Too much or too little information	Generates actionable information
Ignored	Used

“If your database is a symphony orchestra, auditing done right will allow you to hear the kettle drums playing off key.”

Agenda

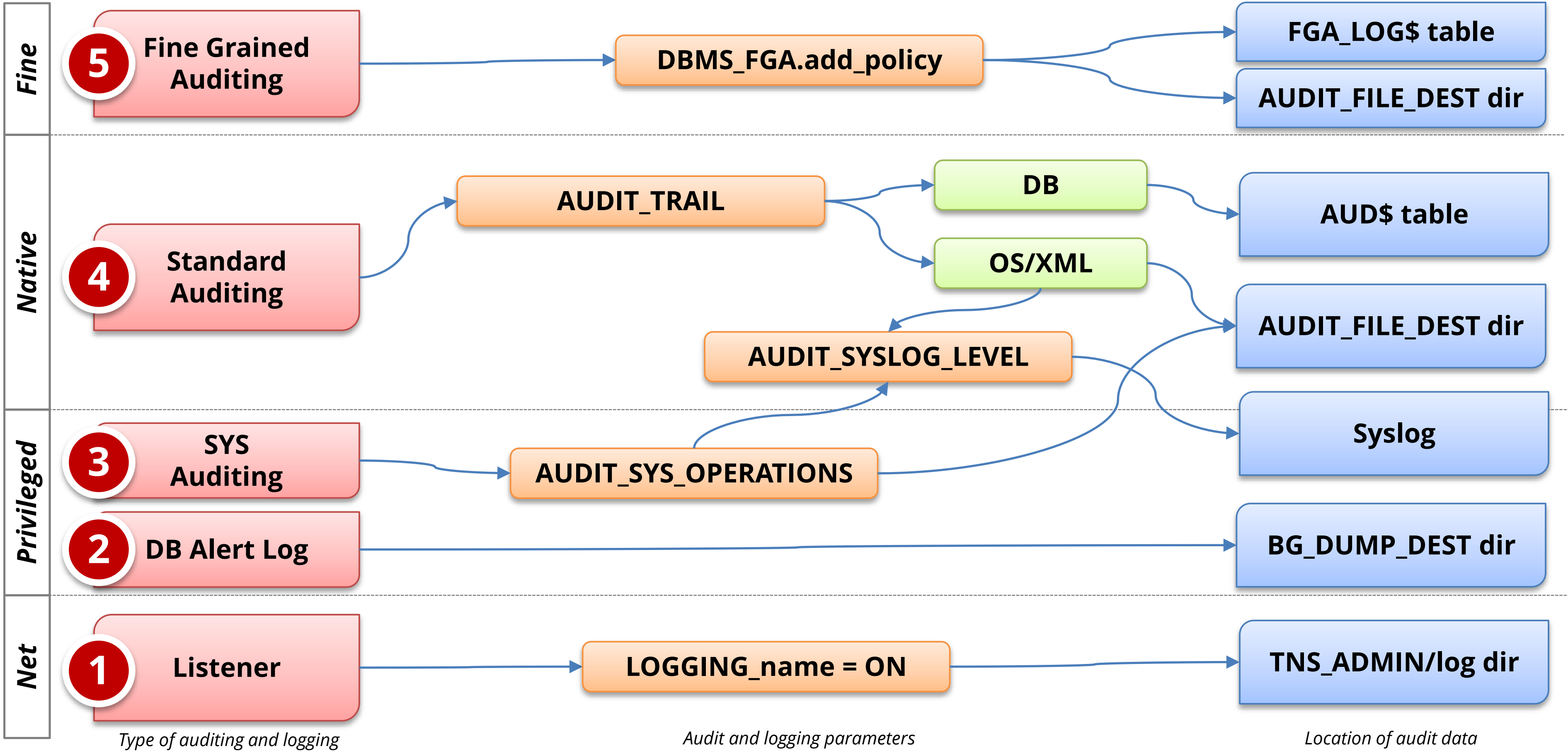
1 Overview

2 Oracle Auditing

3 Integrigy Log & Audit Framework

4 Q&A

Pre-Oracle 12c Database Auditing



System Operations Auditing

- **Mandatory, Always-on-auditing**
  - Startup, shutdown, logon with SYS privileges
  - Written to operating system
  - Cannot turn off

- **SYS Operations Auditing (AUDIT_SYS_OPERATIONS)**
  - What did the SYS, SYSDBA, SYSOPER users do?
  - Written to operating system
  - Parameter to enable (HIGHLY RECOMMENDED)

Standard/Traditional Auditing (TA)

- **Traditional Auditing**
  - Oracle 12c replaces TA with Oracle Unified Auditing (OUA)
  - TA continues to be 12c default (Mixed Mode)

- **Part of standard license**
  - Comprehensive, mature and secure
  - 25 events audited by default
  - Logs to database (default) or O/S
  - Parameter to enable

Traditional Auditing (TA)

- Statement Auditing
  - What SQL statements generate auditing
  - E.g. update by user scott
- Privilege Auditing
  - What privileges when used generate auditing
  - E.g. create user
- Object Auditing
  - Specific object
  - E.g. select on per_all_people_f

- 300+ TA audit commands
  - For complete listing refer to: sys.stmt_audit_option_map
- TA Audit options
  - By Access/By Session
  - When successful/unsuccessful
- Can disable auditing
  - NOAUDIT is an option
- Output to DB, OS, XML
  - Syslog (Use XML for AVDF)

Refer to our whitepaper for more information: Guide to Database Auditing

Fine Grained Auditing (FGA)

- **Conditional statement auditing**
  - Select SSN or salary > $200k when SQL query direct from database not from application

- **Part of enterprise license**
  - Define using SYS.DBMS_FGA package
  - Logs to database or O/S

Database Listener and Alert Logs

- **Database Alert Log**
  - Messages and errors

- **Listener Log**
  - Database connection info

- **V$DIAG_ALERT_EXT**
  - Database view shows both the Alert and Listener Logs

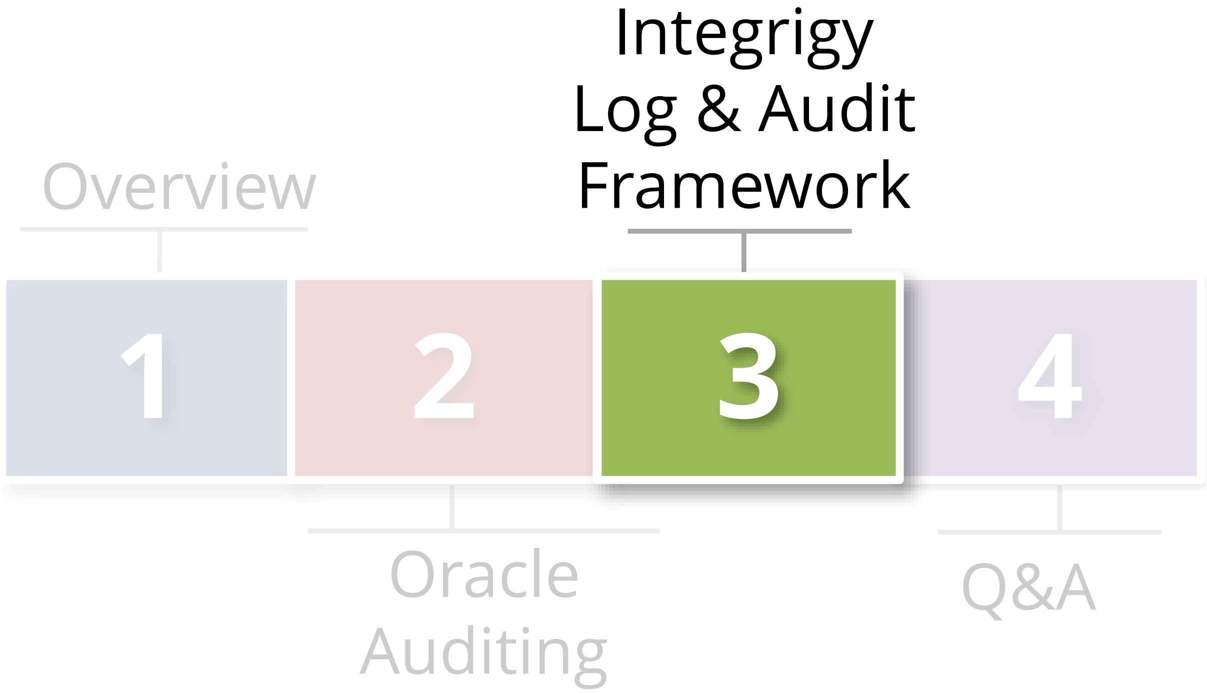
Other Audit Logs

Other Oracle Logs
Real Application Security (RAS)*
Oracle Label Security (OLA)
Oracle Data Pump
Database Vault (DV)
Oracle RMAN
SQL*Loader Direct Load

*Oracle 12c only

Outside Database
Operating System
Network
Load Balancer
Storage
Backup Tools
Application

Agenda



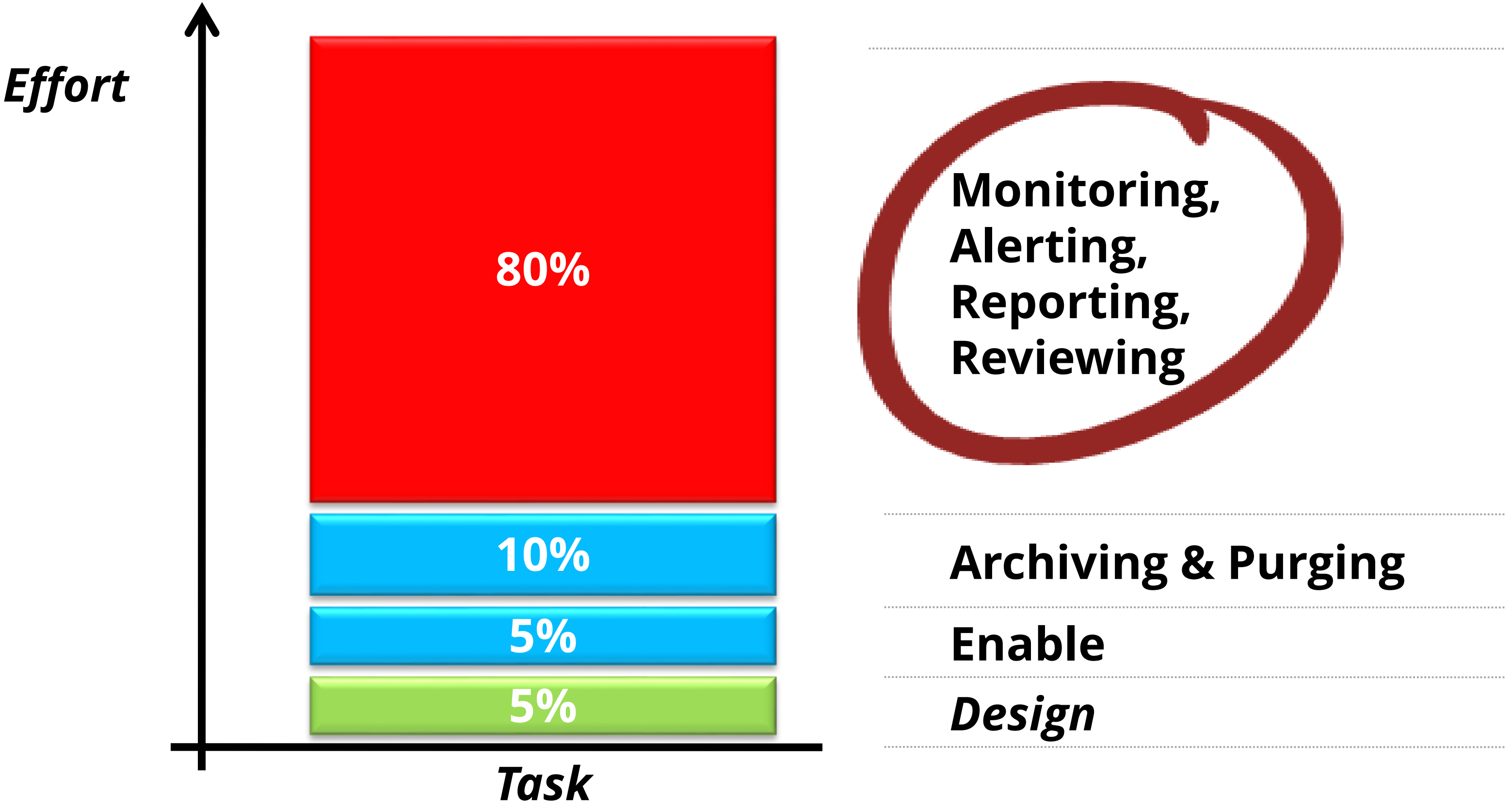
1 Overview

2 Oracle Auditing

3 Integrigy Log & Audit Framework

4 Q&A

Database Auditing Effort by Task



Goals for Database Auditing and Monitoring

Intelligent and business-focused auditing and monitoring

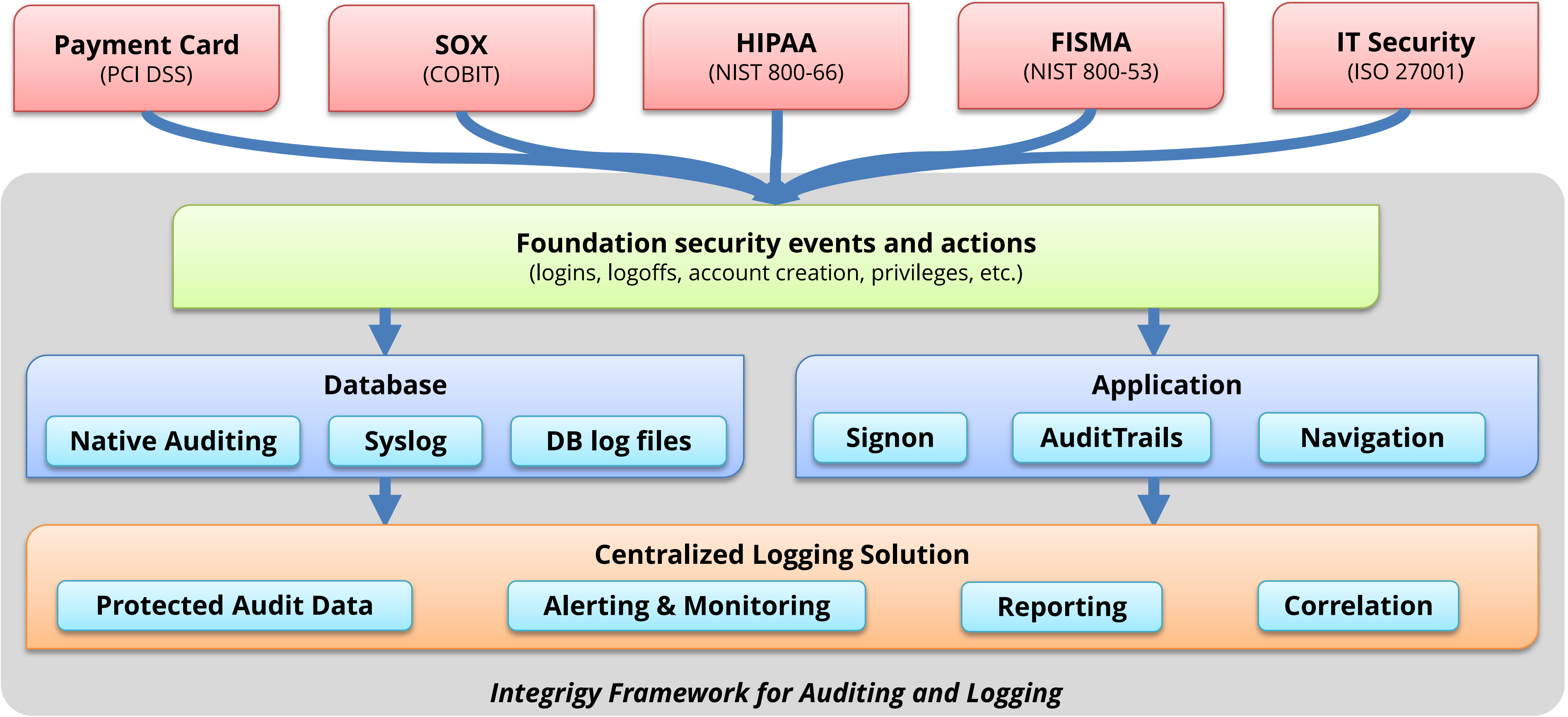
- Transform audit data into actionable information
- Use auditing as mitigating control when necessary
- Auditing is in harmony with database security program to proactively identify non-compliance
- Solve compliance and security challenges – change ticket tracking and workflow

Why Do You Need an Auditing Framework?

- **Value is generated through audit data**
  - Need information as basis for action

- **Integrigy's Framework for Database Auditing is a Methodology**
  - Defines what should be logged and audited
  - Defines what should be alerted and reported on
  - Starting point and direction for database logging

Integrigy Framework for Database Auditing



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.)

Database

- Native Auditing
- Syslog
- DB log files

Application

- Signon
- AuditTrails
- Navigation

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**

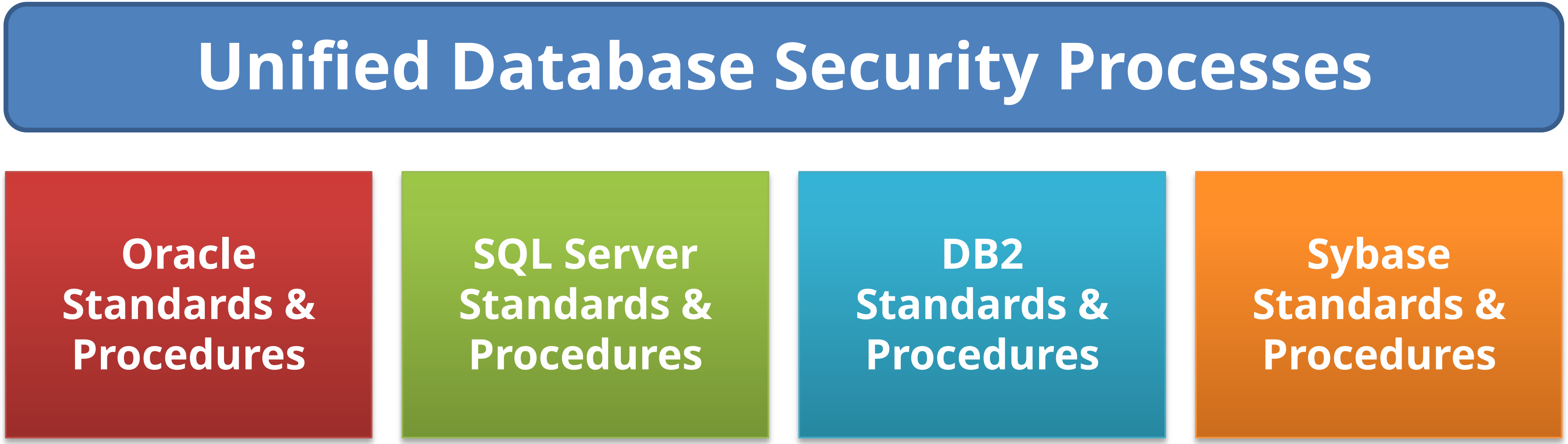
Foundation Security Events Mapping

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

Framework = Consistency

Database Security Program Silos

Processes should be unified, but standards and procedures need to be vendor specific.



Unified Database Security Processes

Oracle Standards & Procedures

SQL Server Standards & Procedures

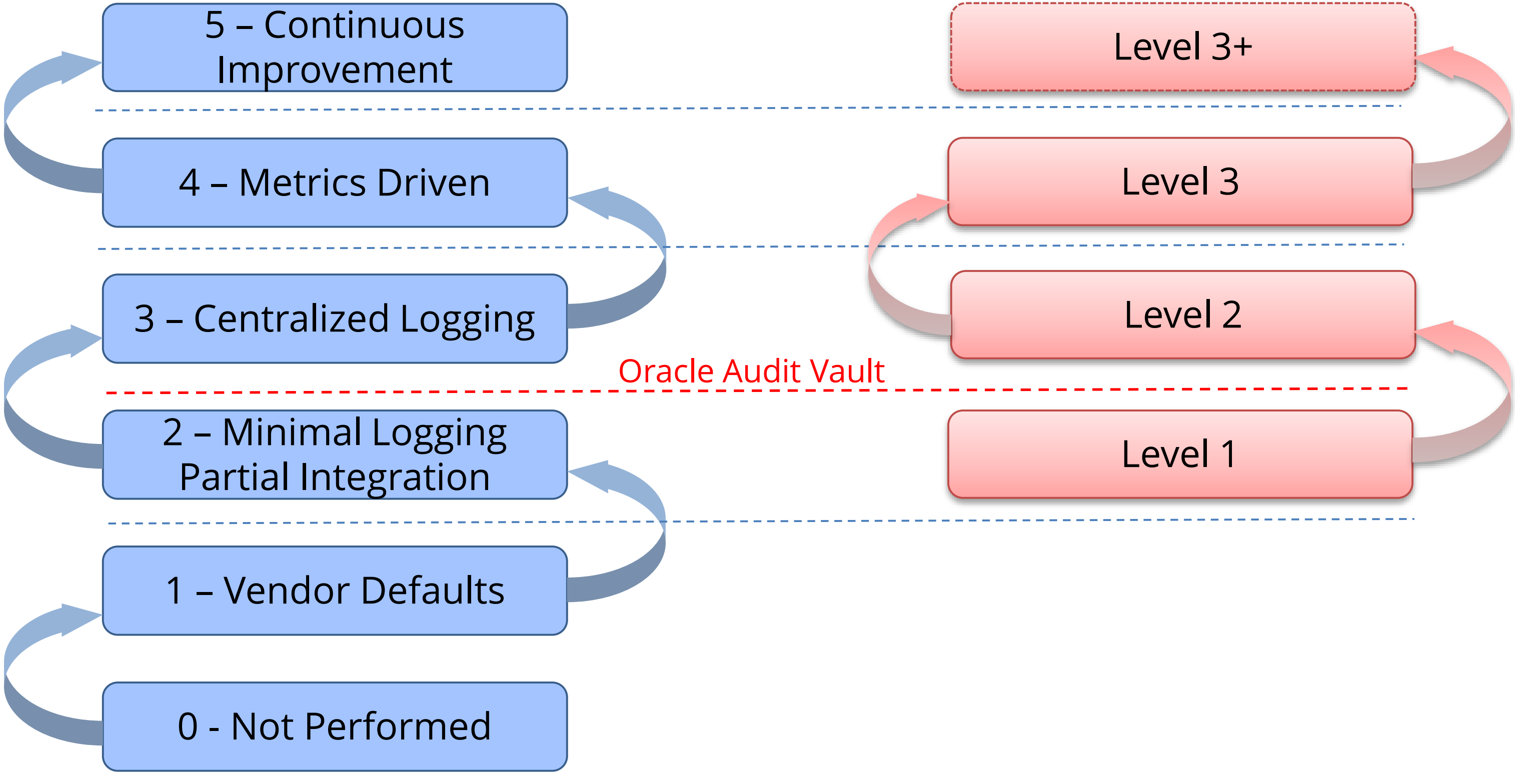
DB2 Standards & Procedures

Sybase Standards & Procedures

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 Database and Application such as the **Oracle Audit Vault**
Level 3	Extend logging to include **FGA** & **functional logging** and more complex alerting and monitoring. Protect sensitive data.

Logging Maturity Model



Common Maturity Model (CMM)

Integrigy Framework

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
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
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 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

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

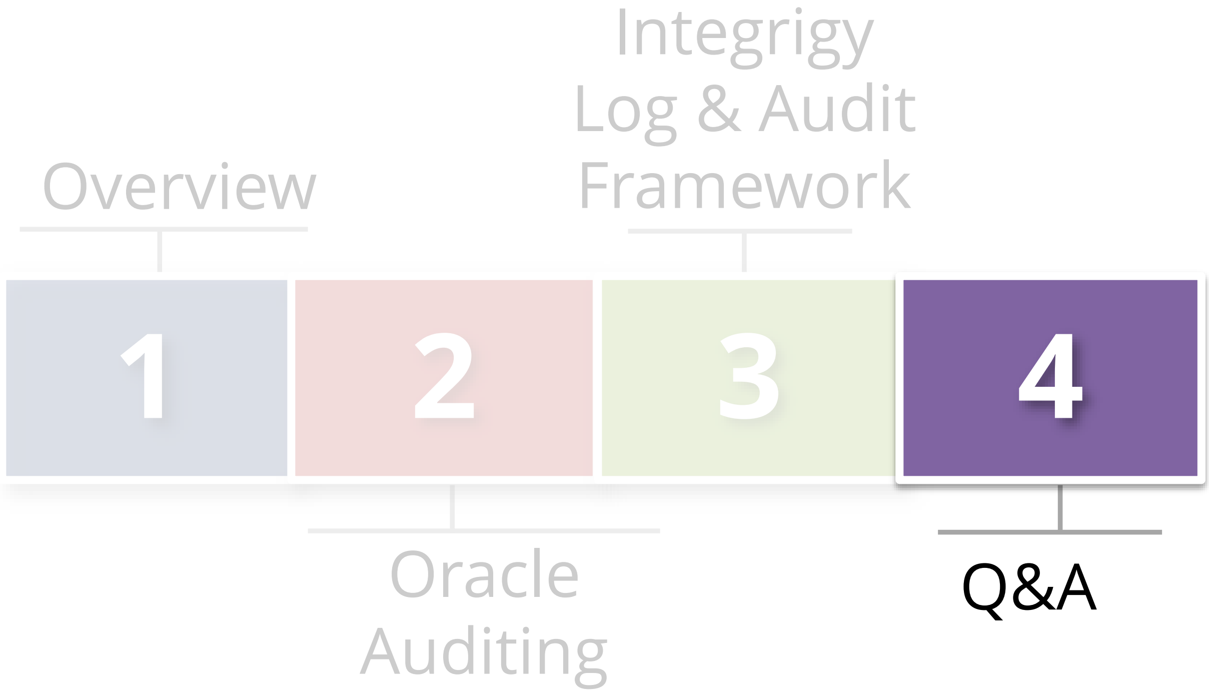
Next steps in maturity

- **Change ticket tracking**
  - DBA enters ticket number
  - Audit statements include ticket number SQL like create user
- **Web application user**
  - Use client identifier to track application end-user
  - Correlations and alerting

Use The Oracle Client Identifier

Application	Example of how used
Oracle E-Business Suite	As of Release 12, the Oracle E-Business Suite automatically sets and updates CLIENT_IDENTIFIER to the FND_USER.USERNAME of the user logged on. Prior to Release 12, follow Support Note How to add DBMS_SESSION.SET_IDENTIFIER(FND_GLOBAL.USER_NAME) to FND_GLOBAL.APPS_INITIALIZE procedure (Doc ID 1130254.1)
PeopleSoft	Starting with PeopleTools 8.50, the PSOPRID is now additionally set in the Oracle database CLIENT_IDENTIFIER attribute.
SAP	With SAP version 7.10 above, the SAP user name is stored in the CLIENT_IDENTIFIER.
Oracle Business Intelligence Enterprise Edition(OBIEE)	When querying an Oracle database using OBIEE the connection pool's username is passed to the database. To also pass the middle-tier username, set the user identifier on the session. Edit the RPD connection pool settings and create a new connection script to run at connect time. Add the following line to the connect script: CALL DBMS_SESSION.SET_IDENTIFIER('VALUEOF(NQ_SESSION.USER)')

Agenda



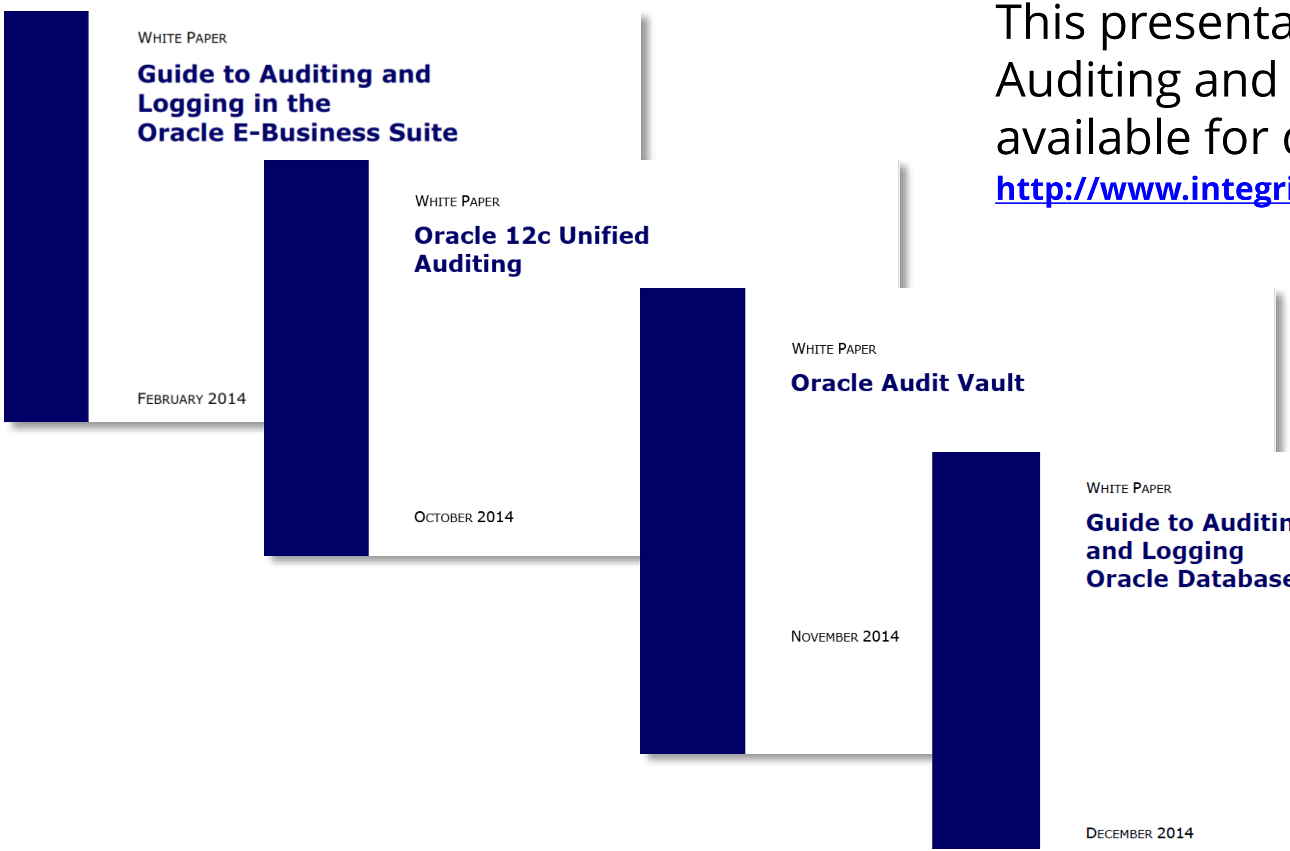
1 Overview

2 Oracle Auditing

3 Integrigy Log & Audit Framework

4 Q&A

Integrigy Oracle Whitepapers



WHITE PAPER

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

FEBRUARY 2014

WHITE PAPER

Oracle 12c Unified Auditing

OCTOBER 2014

WHITE PAPER

Oracle Audit Vault

NOVEMBER 2014

WHITE PAPER

Guide to Auditing and Logging Oracle Databases

DECEMBER 2014

This presentation is based on our Auditing and Logging whitepapers available for download at – http://www.integrigy.com/security-resources

Contact Information

Michael Miller

Chief Security Officer

Integrigy Corporation

web: **www.integrigy.com**

e-mail: **info@integrigy.com**

blog: **integrigy.com/oracle-security-blog**

youtube: **youtube.com/integrigy**