Oracle 12c
Unified Auditing

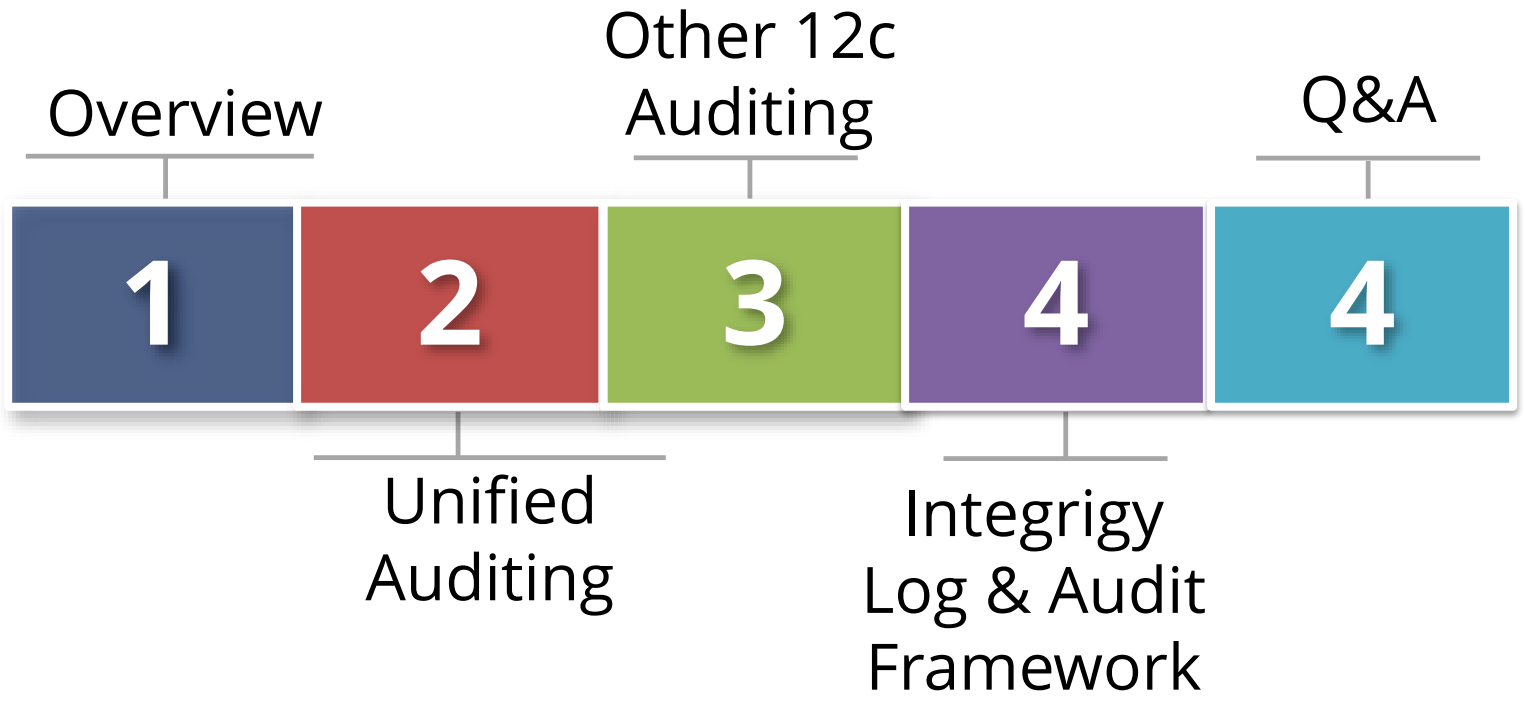
October 23, 2014

Mike Miller
Chief Security Officer
Integrigy Corporation

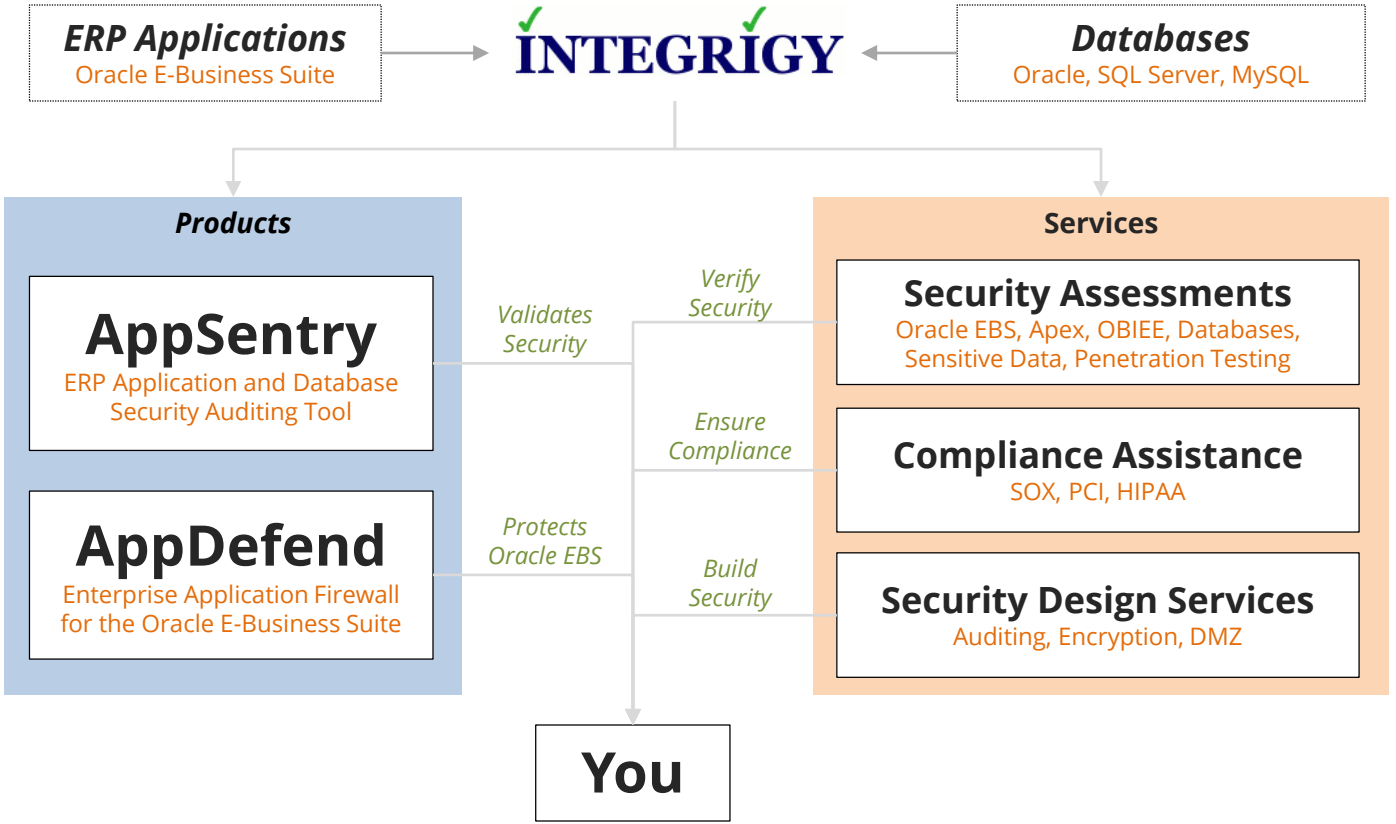
Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

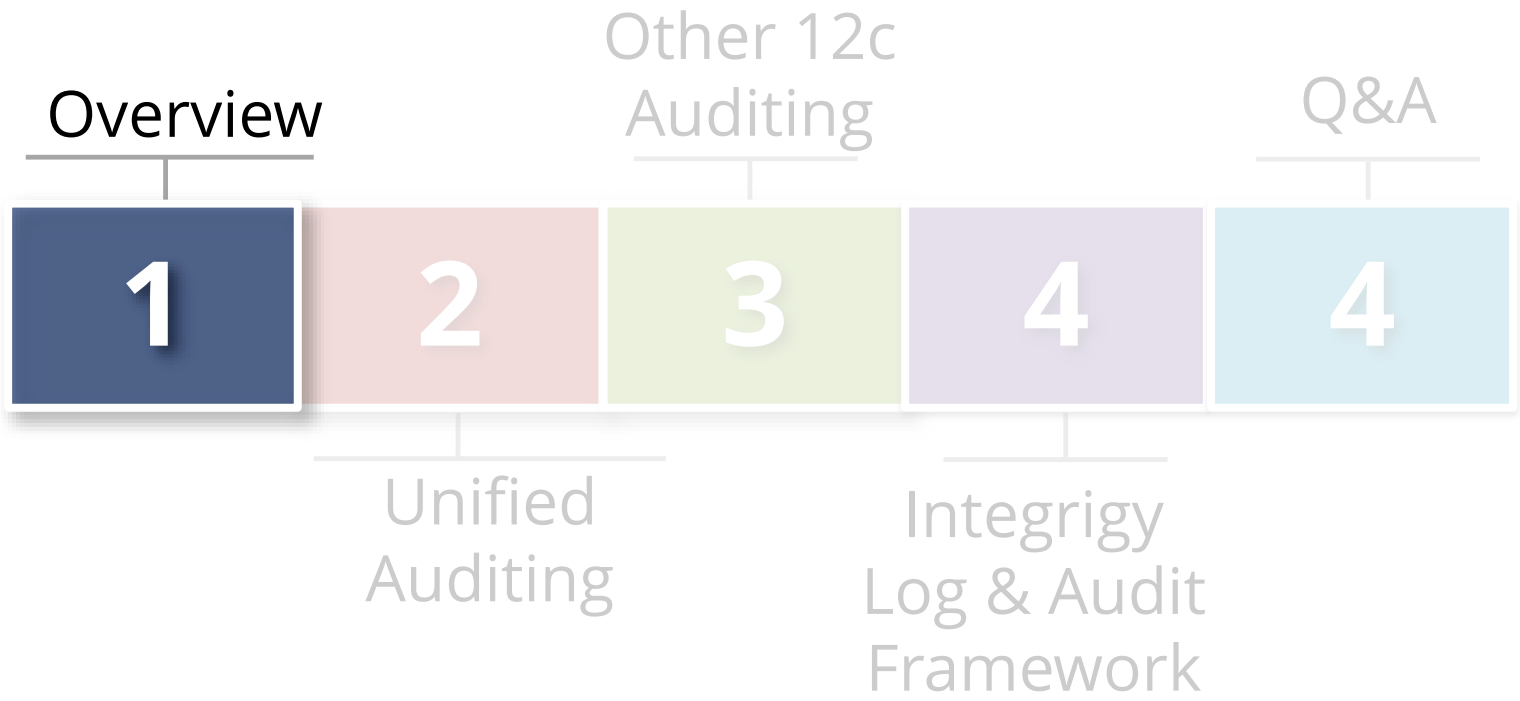
Agenda


Overview
Other 12c Auditing
Q&A
1
2
3
4
4
Unified Auditing
Integrigy Log & Audit Framework

About Integrigy



Agenda


Overview
Other 12c Auditing
Q&A
1
2
3
4
4
Unified Auditing
Integrigy Log & Audit Framework

Oracle Database Security

- **Incremental improvements in Oracle 12c**
  - Unified Auditing
  - Mandatory Auditing
  - Real Application Security
  - Data Redaction
  - Multitenant (pluggable databases)

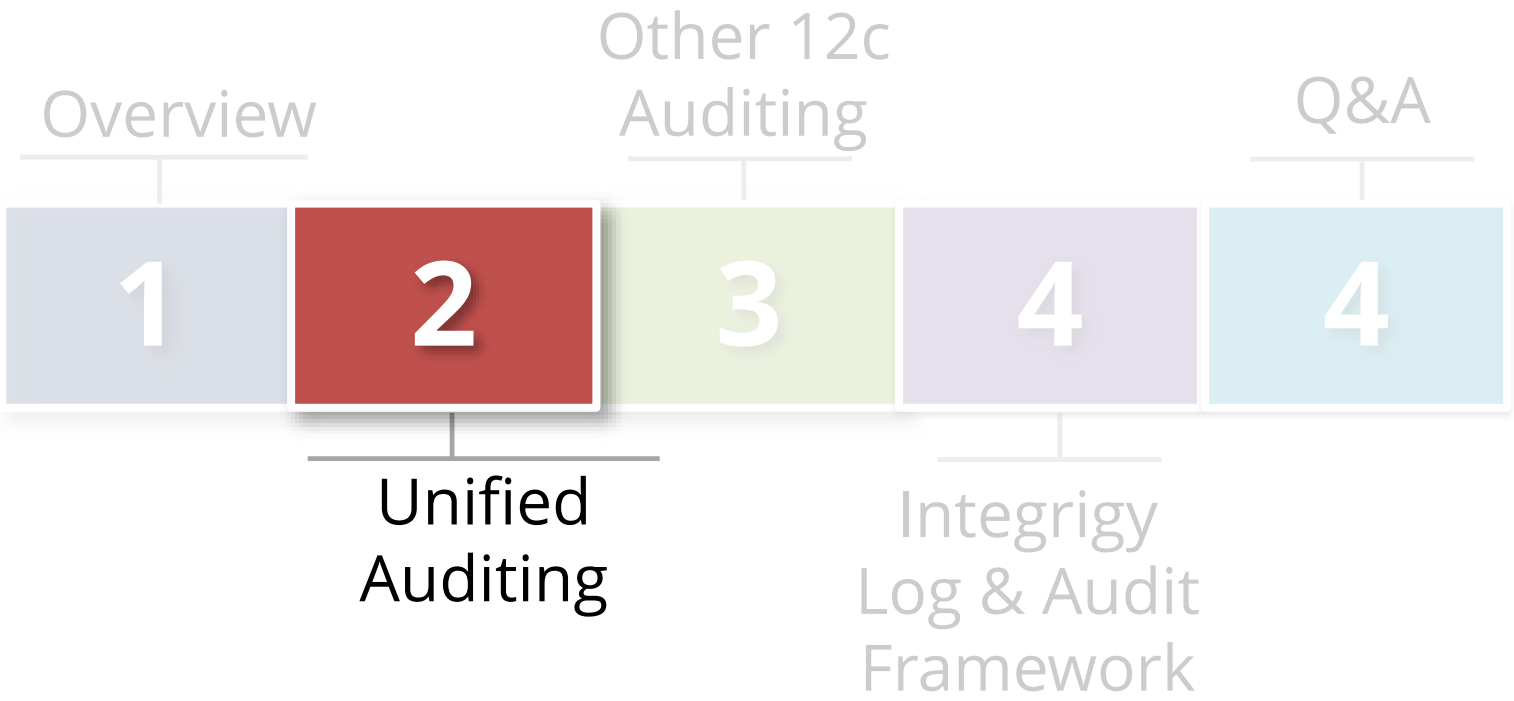
Today's Objectives for Unified Auditing

- **Everything has changed**
  - Pure mode
- **Nothing has changed**
  - Mixed mode
- **Initial survey to make decisions**
  - Impact to logging, auditing and monitoring

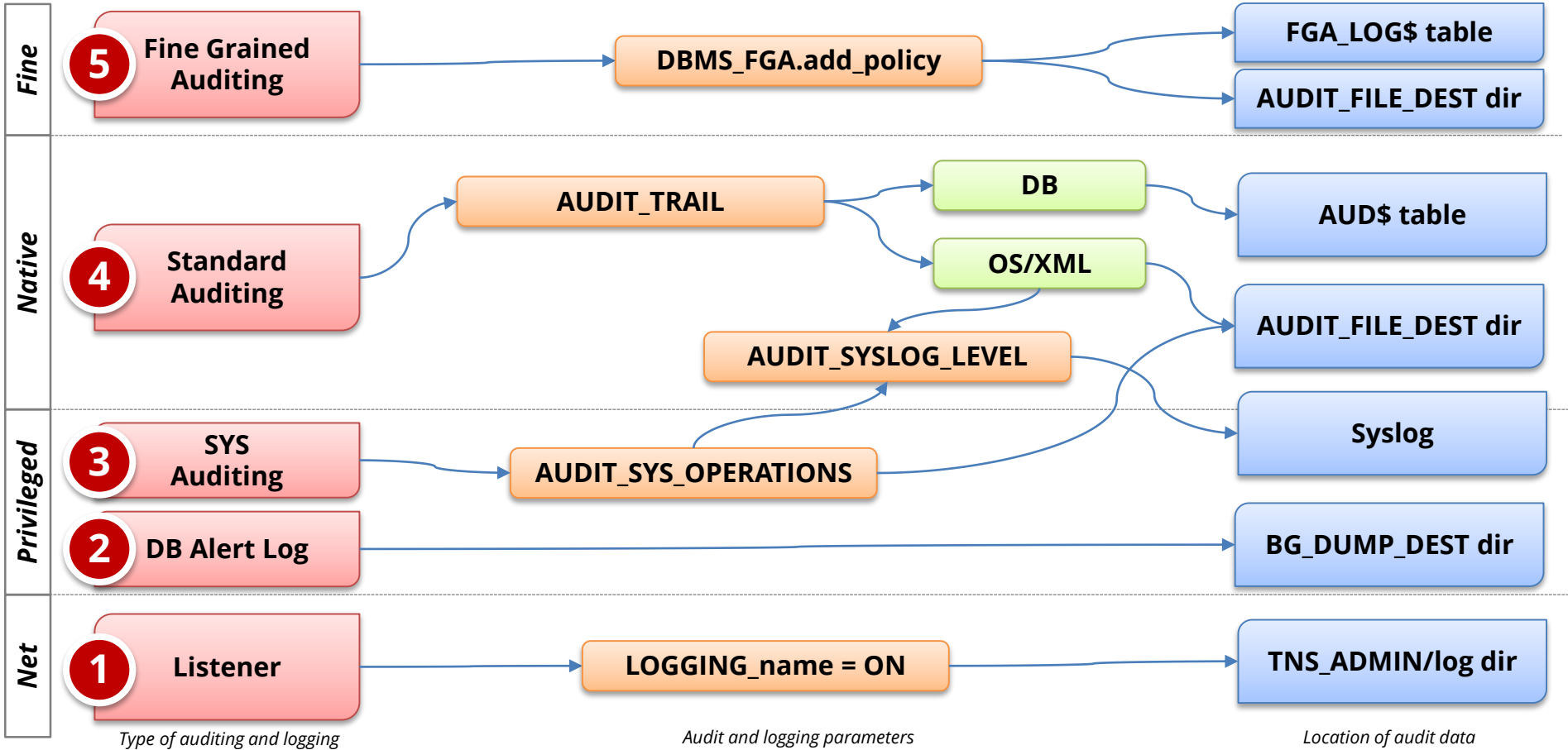
Auditing and Logging

- **Log so can audit, monitor, and alert**
  - Related but separate disciplines
- **Requirements are difficult**
  - Technical, Compliance, Audit, and Security
- **The Oracle database offers rich log and audit functionality**
  - **Most organizations do not fully take advantage**
  - **Oracle 12c can change this**

Agenda


Overview
Other 12c Auditing
Q&A
1
2
3
4
4
Unified Auditing
Integrigy Log & Audit Framework

Pre-Oracle 12c Database Auditing



Unified Auditing Has Two Modes

- **Pure**
  - Only 12c Unified Audit functionality available
- **Mixed (Default)**
  - Has both traditional and Unified Auditing
  - Provided as introduction and transition

Mixed Mode

- **All traditional audit features and functionality work same as before**
  - Default Oracle 12c

- **Unified Audit Trail populated in parallel to traditional auditing**
  - Because default policy ORA_SECURECONFIG
  - Purge or disable ORA_SECURECONFIG Doc ID 1624051.1

SYS.UNIFIED_AUDIT_TRAIL IS A VIEW

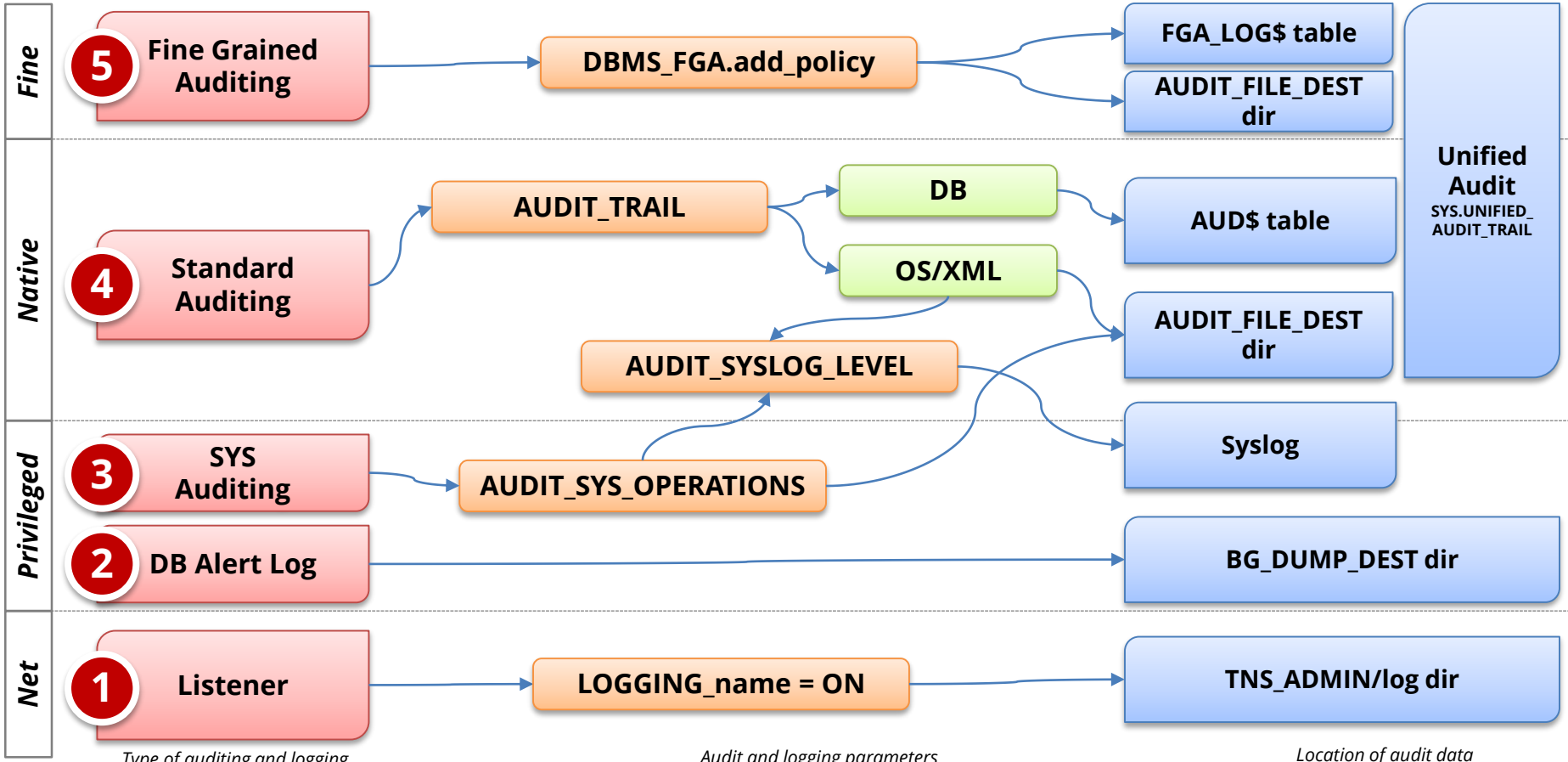
Column Description*	Number of Columns
Standard auditing including SYS audit records	44
Real Application Security (RAS) and RAS auditing	17
Oracle Label Security	14
Oracle Data Pump	2
Fine grained audit (FGA)	1
Data Vault (DV)	10
Oracle RMAN	5
SQL*Loader Direct Load	1
Total	94

*Key column is AUDIT_TYPE

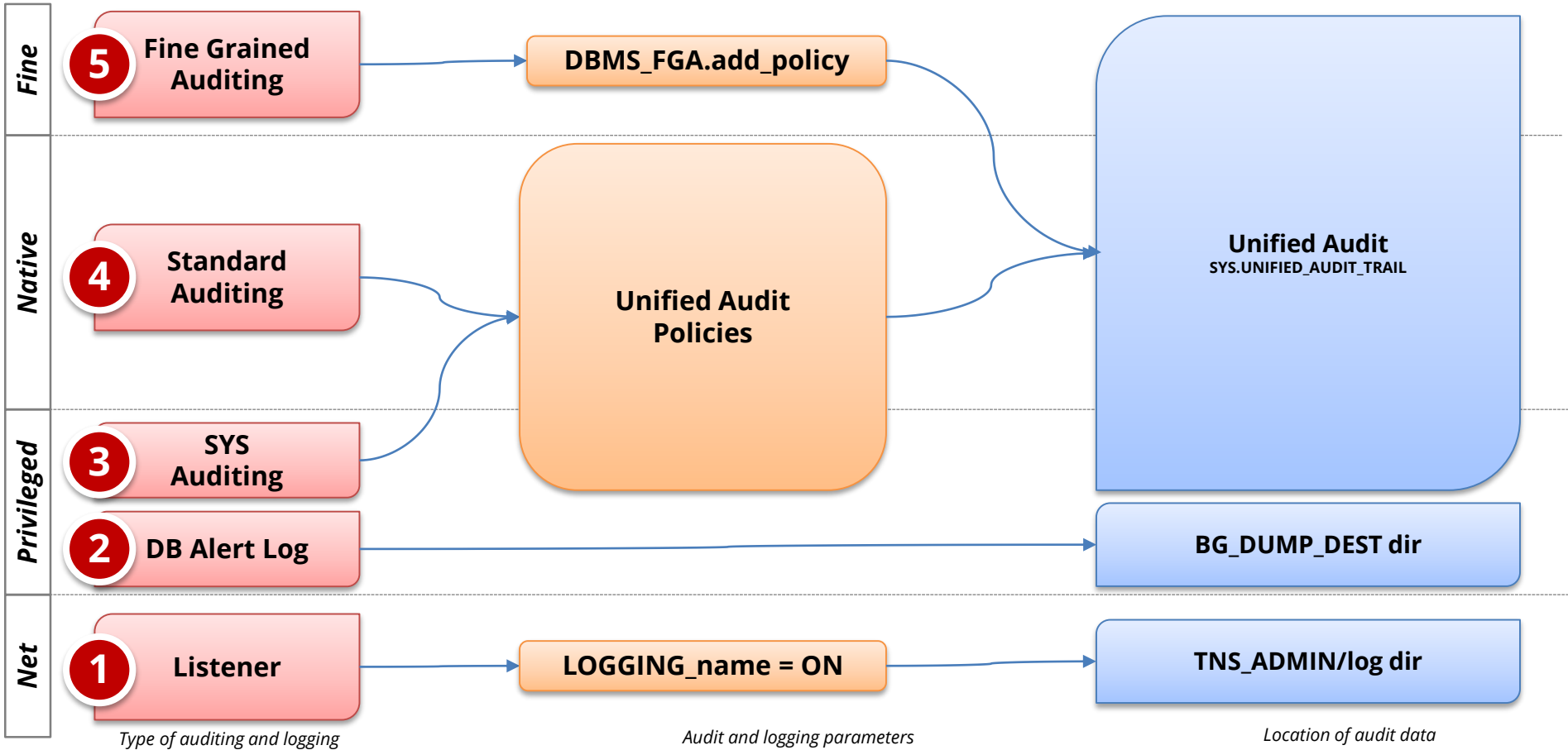
Pure Mode

- **Not default, but is the future**
  - Re-link kernel to use
- **Traditional sources no longer populated**
- **Has new parameters and syntax**
  - Old init.ora parameters ignored
- **Uses OracleSecure files**
  - No syslog
- **Can revert back to Mixed Mode**

Oracle 12c Database Auditing - Mixed



Oracle 12c Database Auditing - Pure



Mixed vs. Pure Mode Audit Configurations

System Parameters	Mixed Mode	Pure Mode
AUDIT_TRAIL	Same as 11g	Not used
AUDIT_FILE_DEST	Same as 11g	Not used
AUDIT_SYS_OPERATIONS	Same as 11g	Not used
AUDIT_SYSLOG_LEVEL	Same as 11g	Not used
UNIFIED_AUDIT_SGA_QUEUE_SIZE	Same as 11g	Used

New Policy Based Audit Syntax

- **Use create/alter audit policy statement***

```
CREATE AUDIT POLICY policy_name
   { {privilege_audit_clause [action_audit_clause ]
[role_audit_clause ]}
       | { action_audit_clause  [role_audit_clause ] }
       | { role_audit_clause }
    }
   [WHEN audit_condition EVALUATE PER
{STATEMENT|SESSION|INSTANCE}]
   [CONTAINER = {CURRENT | ALL}];
```

*DBMS_FGA used to configure fine-grained column and event handlers

Unified Audit Example

```
CREATE AUDIT POLICY logon_pol
ACTIONS LOGON
WHEN 'INSTR(UPPER(SYS_CONTEXT(''USERENV'',
      ''CLIENT_PROGRAM_NAME'')), ''SQLPLUS'') > 0`
AND  'SYS_CONTEXT (''USERENV'', ''HOST'')
     NOT IN (''`prod_db_rac1'',''`prod_db_rac2'')'

EVALUATE PER SESSION;

AUDIT POLICY logon_pol BY APPS;
```

Unified Audit Policies Installed by Default

Policy Name	Default Enabled	Description
ORA_SECURECONFIG	Yes	Secure configuration audit. Same as default 11g auditing.
ORA_RAS_POLICY_MGMT	No	Oracle Real Application Security admin actions for RAS users, roles, and policies
ORA_RAS_SESSION_MGMT	No	Run-time RAS session and namespace actions
ORA_ACCOUNT_MGMT	No	Commonly used user account and privilege settings for create user, role and privilege grants
ORA_DATABASE_PARAMETER	No	Audits commonly used Oracle Database parameter settings

Unified Auditing Separation of Duties

- **Two new roles with Oracle 12c**
  - **AUDIT_ADMIN** – define and maintain audit policies
  - **AUDIT_VIEWER** – view and analyze audit data

New Schema for Unified Audit Data

- **AUDSYS** – New schema used solely for storage Unified Audit trail data in SYSAUX
  - Pure Mode uses Oracle SecureFiles

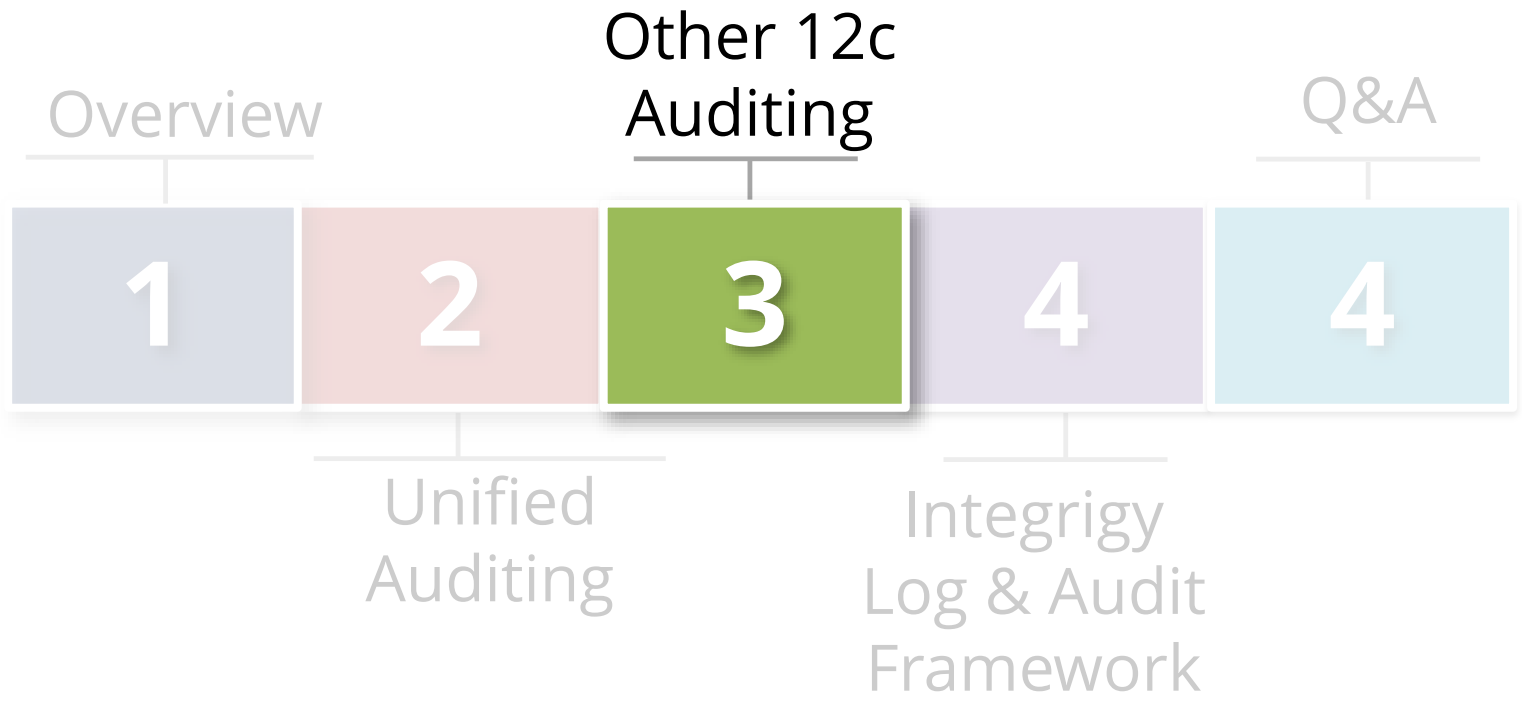
- **AUD$** and **FGA_LOG$** system tables and objects remain in the SYS schema

Improved Performance

- **Auditing now implemented in SGA**
  - Negligible overhead

- **Two queuing modes**
  - **Immediate-write**: immediately written
  - **Queued-Write** (default): periodically dequeued

Agenda


Overview
Other 12c Auditing
Q&A
1
2
3
4
4
Unified Auditing
Integrigy Log & Audit Framework

Pluggable Databases and Common Audit

- **Oracle 12c Multitenant option (Pluggable databases)**
  - Separate license NOT enabled by default
- **For Oracle 12c pluggable databases audit policies can be:**
  - **Common –** Available to all pluggable databases (PDB)s. Enable common audit policies only for common users for common objects.
  - **Local -** These policies apply only to a single pluggable database. By default, audit policies are local to the current PDB.

Oracle 12c Mandatory Auditing

- **New Oracle 12c always-on-auditing for SYSDBA**
  - SYS, SYSDBA, SYSOPER, SYSASM, SYSBACKUP, SYSDG, SYSKM

- **Mandatory Auditing Events (SYS.UNIFIED_AUDIT_TRIAL)**
  - CREATE AUDIT POLICY
  - ALTER AUDIT POLICY
  - DROP AUDIT POLICY
  - AUDIT
  - NOAUDIT
  - Database Vault configurations
  - DBMS_FGA PL/SQL package
  - DBMS_AUDIT_MGMT PL/SQL package
  - ALTER TABLE attempts on the AUDSYS audit trail

Real Application Security

- **New with Oracle 12c**
  - Next generation VPD
- **Define users separately from DBA_USERS**
  - DBA_XS_USERS
  - Can directly connect to the database
- **Log RAS users using Unified Audit Trail**
  - XS$NULL vs. xs_user_name
- **RAS role and event auditing is separate**

Oracle Client Identifier

Application	Example of how used
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 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)')

Unified Audit Examples of Client_Identifier

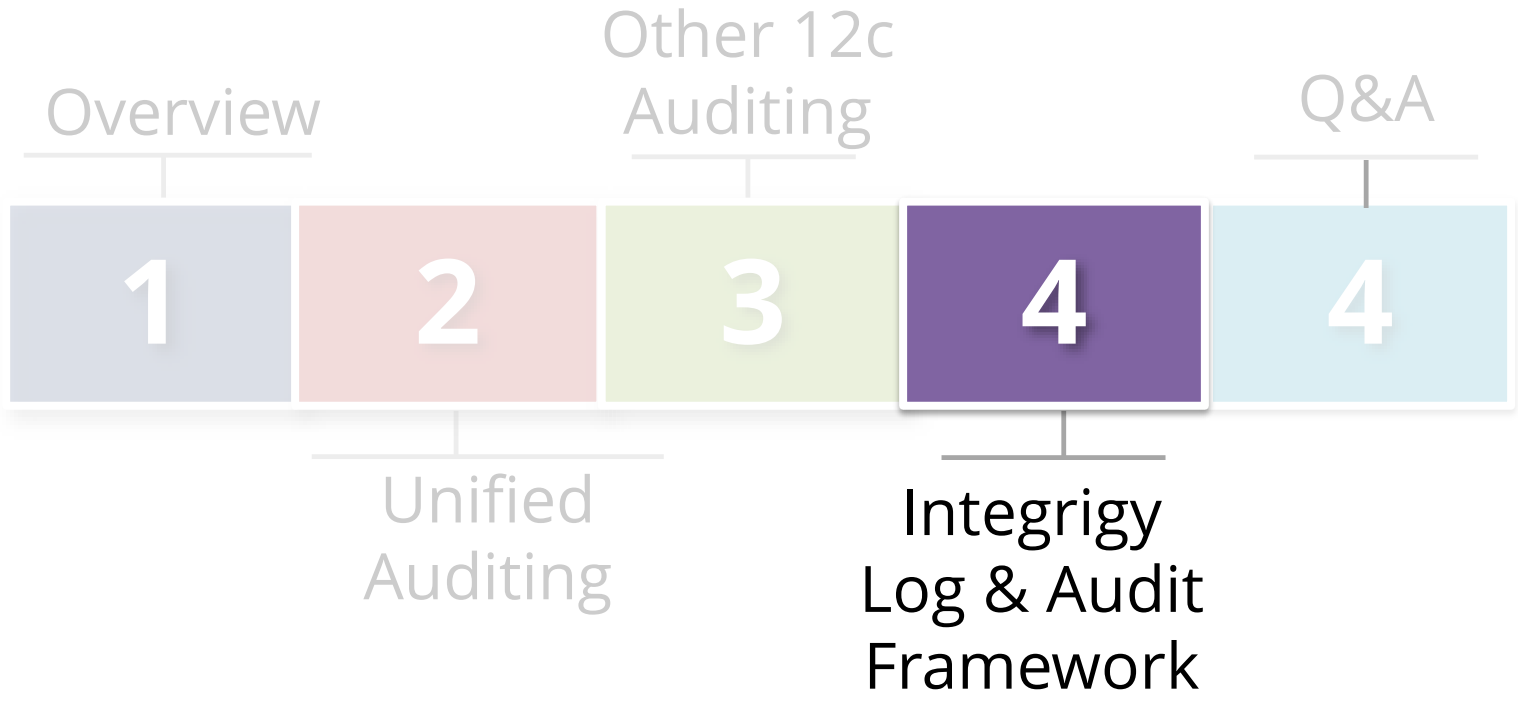
```
CREATE AUDIT POLICY sales_clerk_mm_pol
ACTIONS DELETE ON OE.ORDERS
WHEN 'SYS_CONTEXT(''USERENV'', ''CLIENT_IDENTIFIER'')
      = ''`mmiller'''
EVALUATE PER STATEMENT;

AUDIT POLICY sales_clerk_mm_pol by APPS;
```

11g Auditing Features to Note

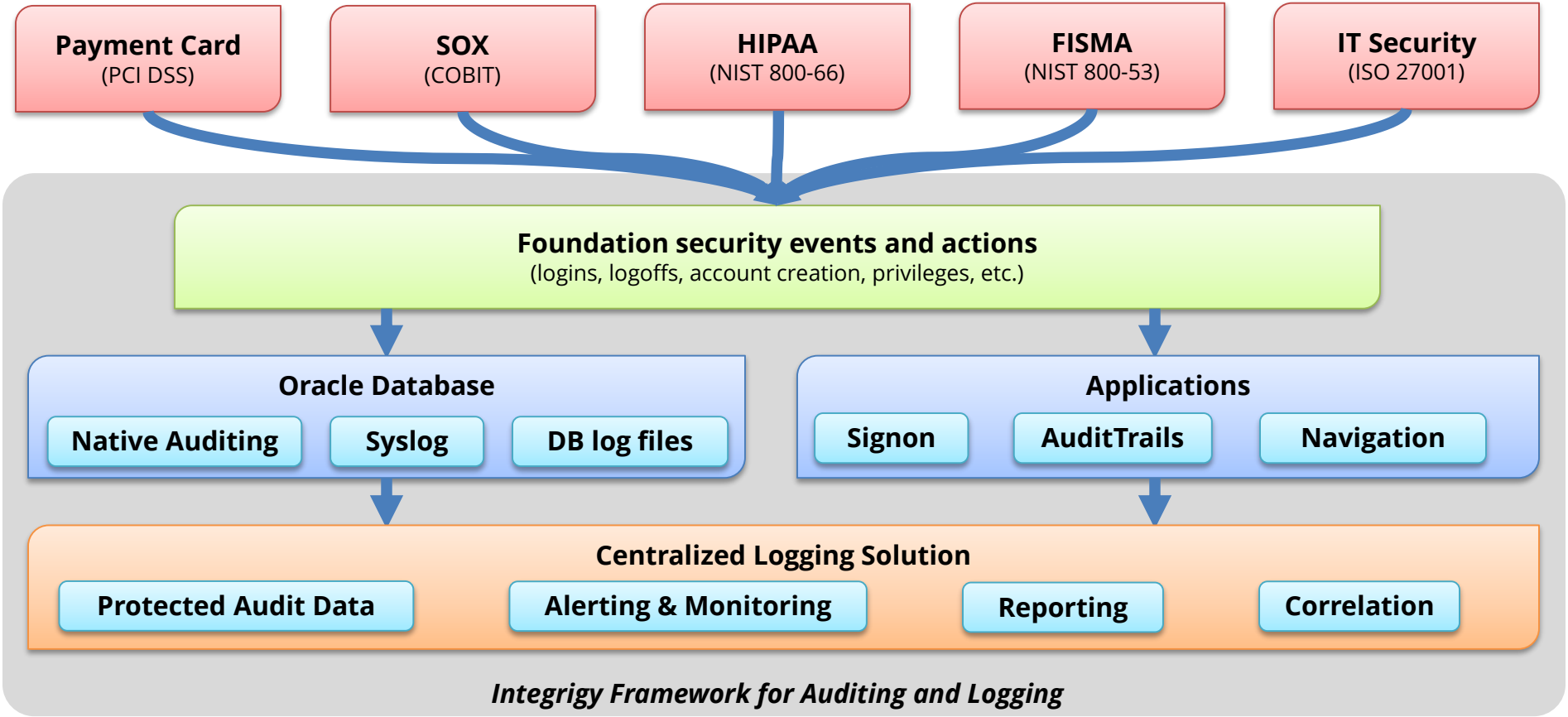
- **Alert log access in a view**
  - SYS.X$DBGALERTEXT

- **V$DIAG_ALERT_EXT view shows both the Alert and Listener Logs:**
  - For alert log use: Where trim(COMPONENT_ID)='rdbms';
  - For listener log use: WHERE trim(COMPONENT_ID)='tnslsnr';

Agenda


Overview
Other 12c Auditing
Q&A
1
2
3
4
4
Unified Auditing
Integrigy Log & Audit Framework

Integrigy Framework for Auditing and Logging



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**

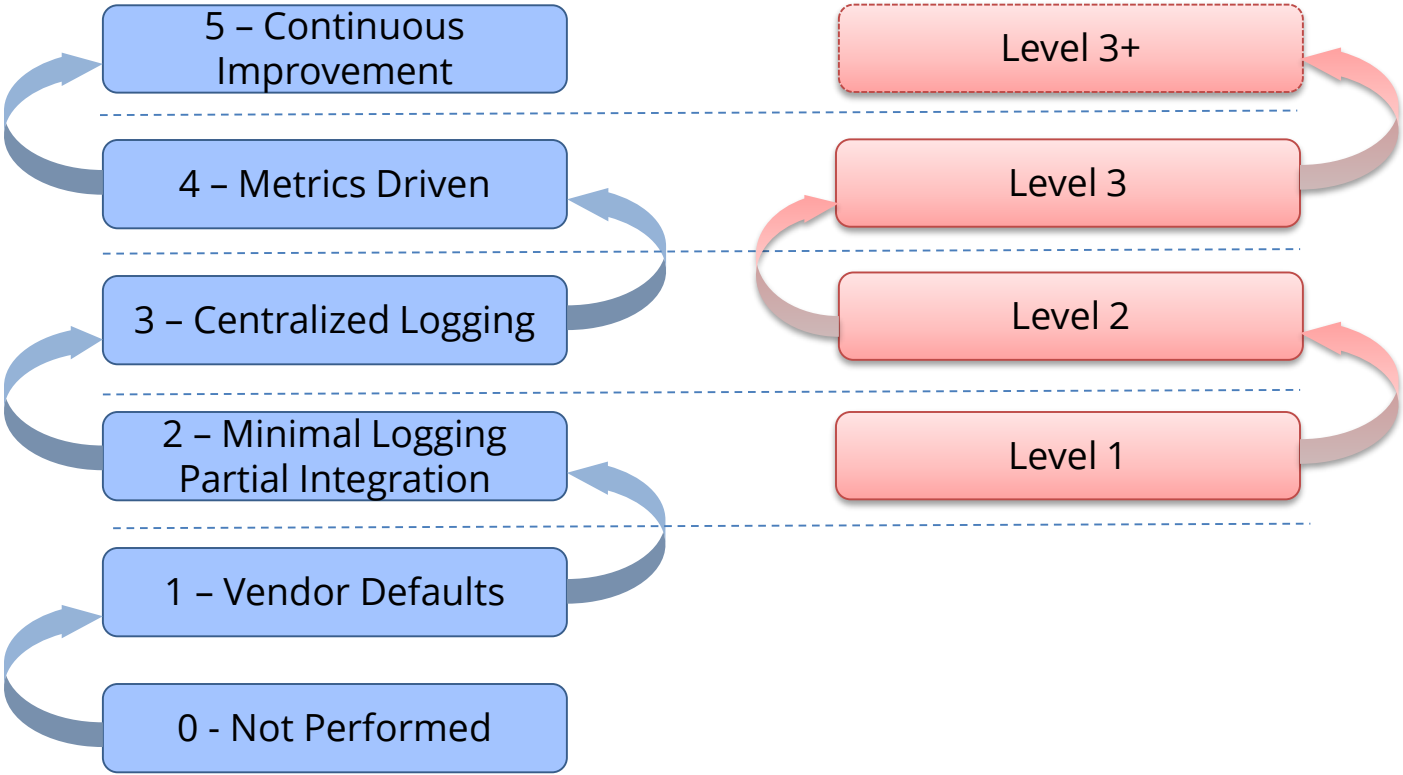
Foundation Security Events Mapping

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

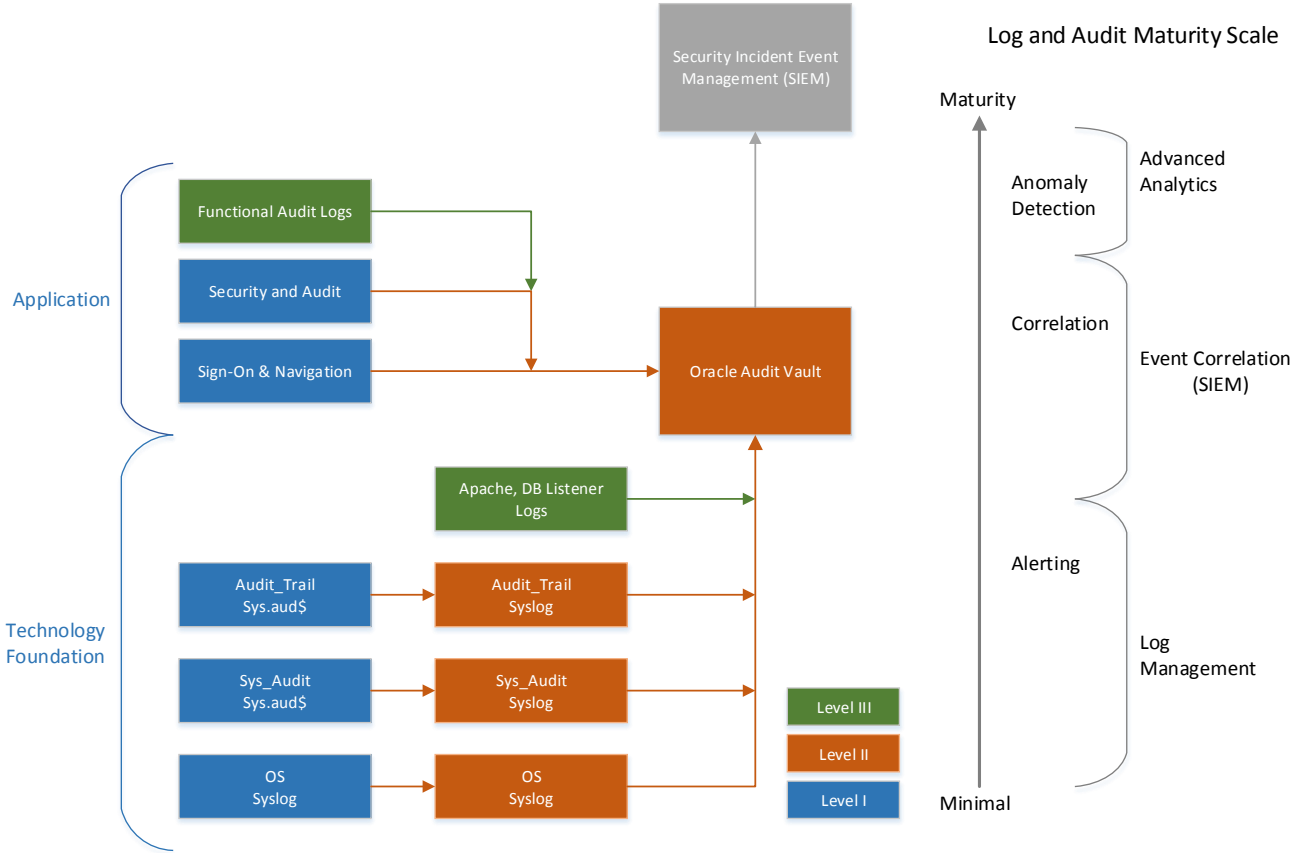
Level 1	Enable **baseline auditing and logging** for application/database and implement security monitoring and auditing alerts
Level 2	Send audit and log data to a **centralized logging** solution outside the Oracle Database and Application(s)
Level 3	Extend logging to include **functional logging**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

Logging Maturity Model

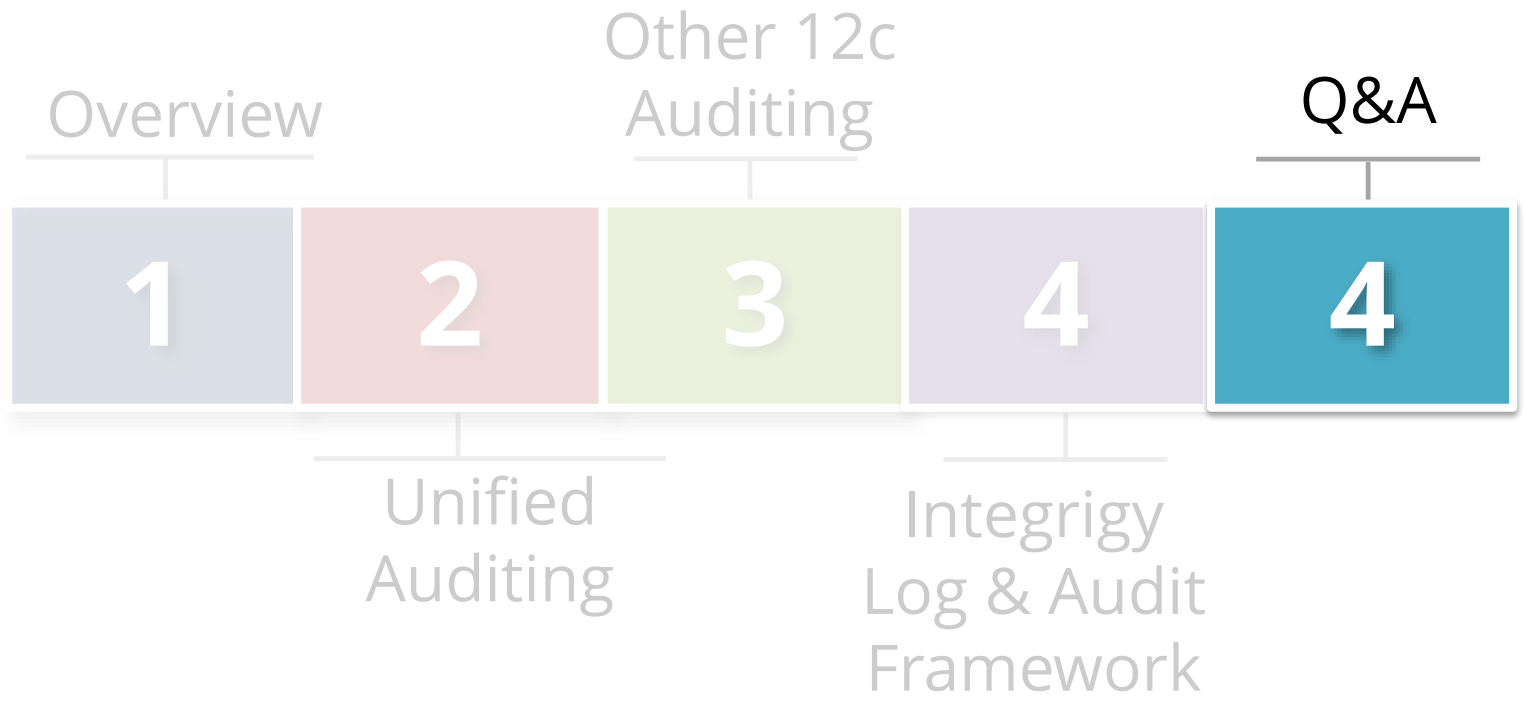


Common Maturity Model (CMM) ***Integrigy Framework***

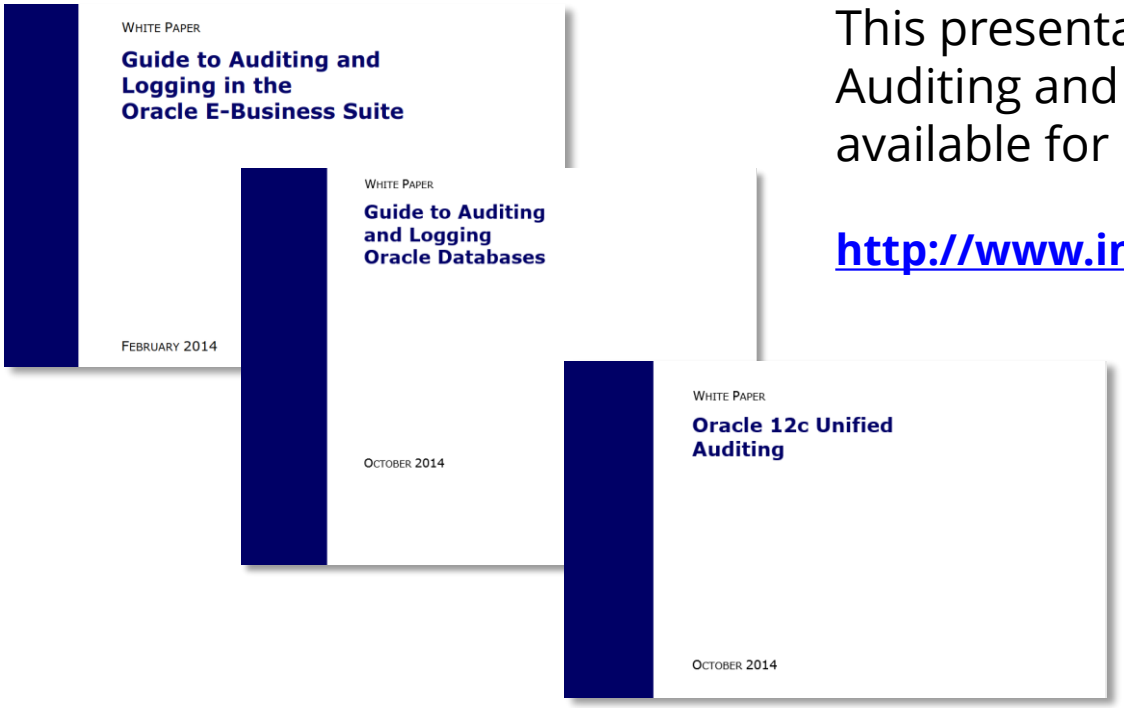
Integrigy Framework for Auditing and Logging



Agenda


Overview
Other 12c Auditing
Q&A
1
2
3
4
4
Unified Auditing
Integrigy Log & Audit Framework

Integrigy Oracle Whitepapers



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**