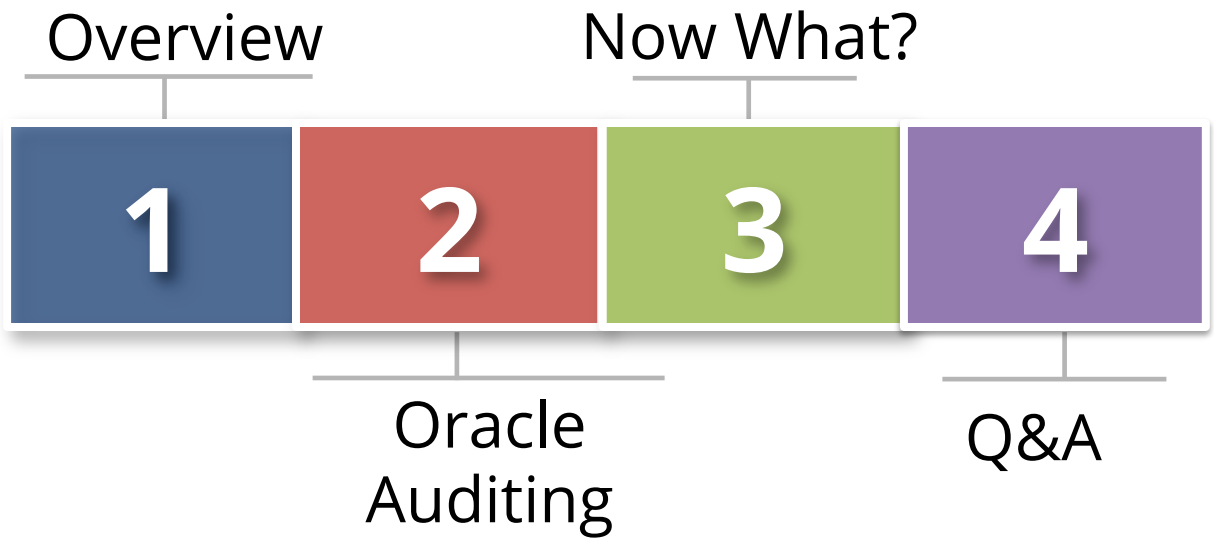
NYOUG Spring 2015
Its Only Auditing - Don't Be Afraid

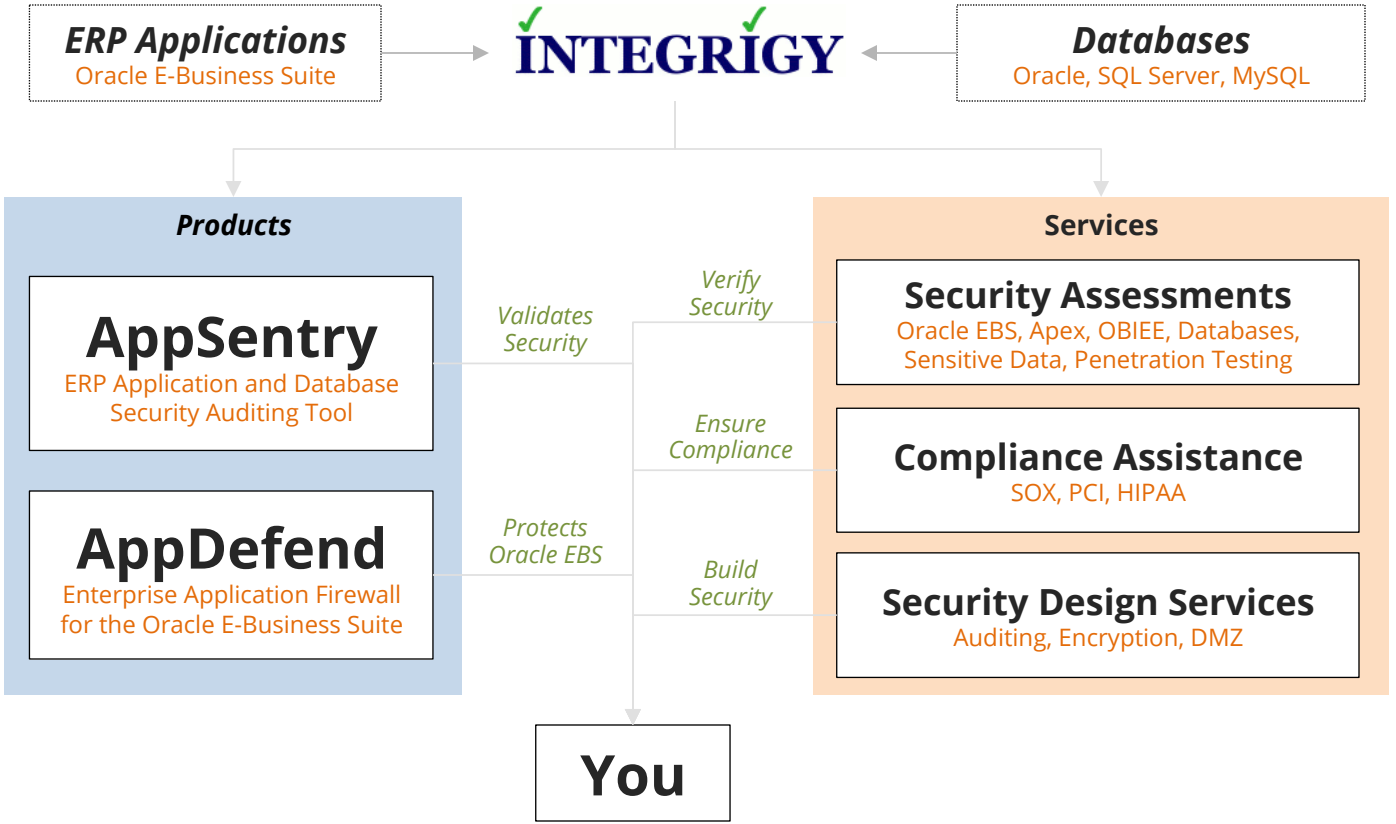
March 19, 2015

Mike Miller
Chief Security Officer
Integrigy Corporation

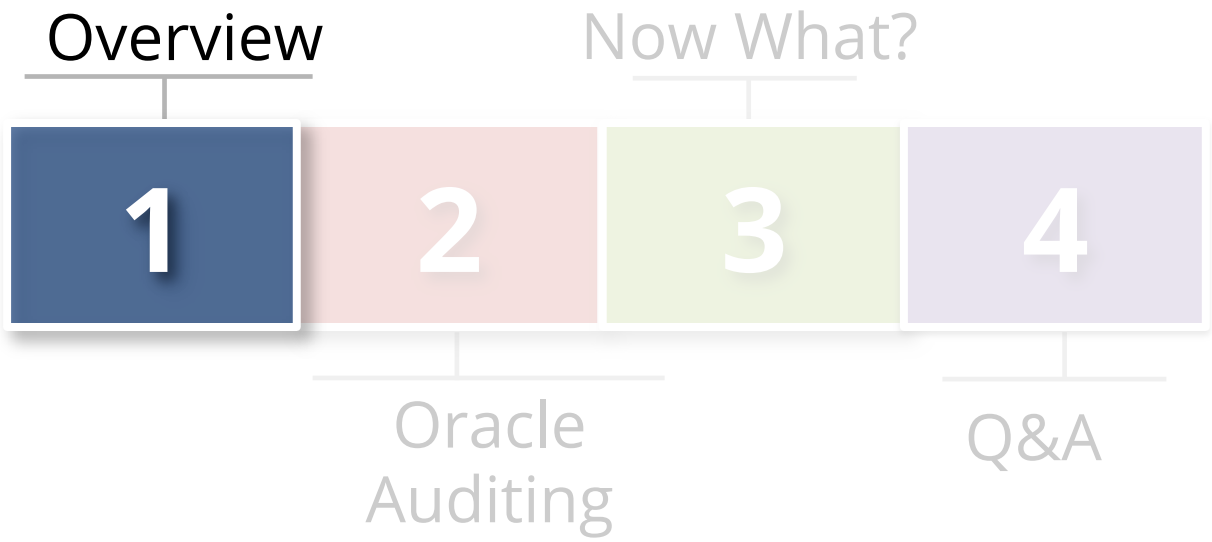
Agenda



About Integrigy



Agenda



Questions To Start

- **How many are not DBAs?**
  - IT Security or Auditor?
- **How many are using auditing today?**
  - Just using default events?
  - Sending to Syslog?
- **How many are on Oracle 12c?**
  - Using Unified Auditing?

Key Points Today

- **Should you be afraid of Oracle Auditing?**
  - No. If not you should be afraid of what you are missing.
- **Default Oracle auditing – is it good enough?**
  - Not really, but what you are doing with default auditing is the better question.
- **Does auditing degrade performance?**
  - It can. Too much of anything is bad.
- **What version of Oracle are we talking about?**
  - Oracle 12c changes everything.

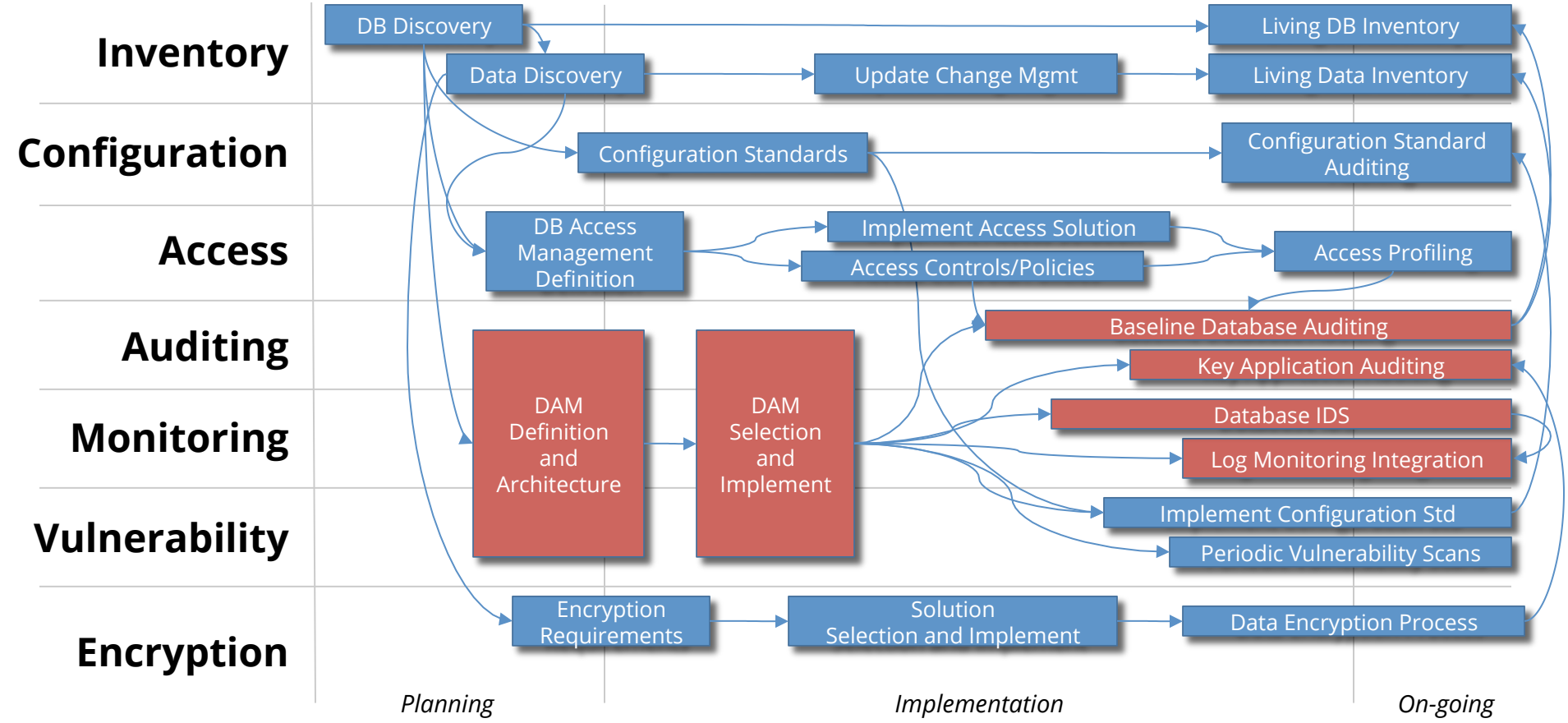
Security Is A Process

- **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



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**.

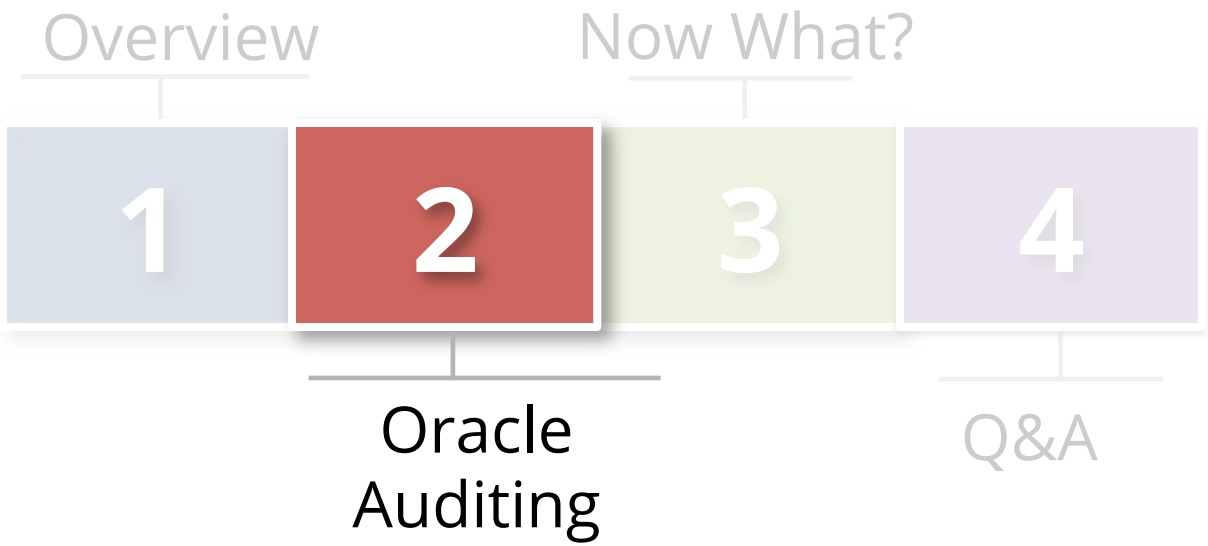
- **Not using auditing**
- **Auditing poorly defined**
- **No review of audit data**
- **No mapping of business requirements to auditing, alerts, or reports**
- **Zero value to the organization**

Database Auditing

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

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

Agenda

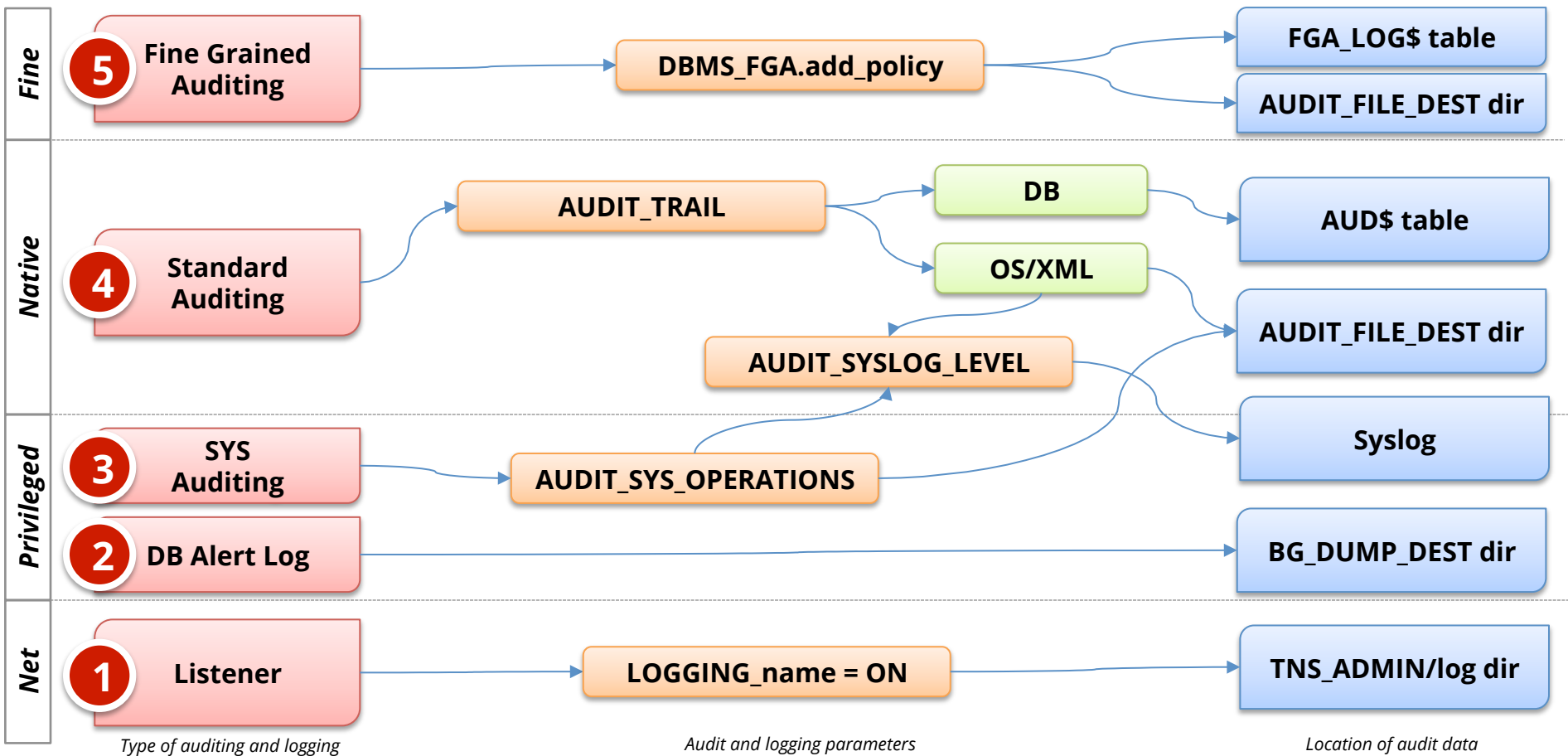


First Point – Is There Impact on Performance?

- **Yes auditing impacts performance**
  - Seen and heard about percentages of 2 to 200%
  - Is proportional to how much you audit

- **Everything changes with Oracle 12c**
  - Oracle Unified Auditing (OUA) is a re-write and the future
  - “Significant” performance improvement

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 SYS.AUD$ (default) or O/S
  - Manage purging with DBMS_AUDIT_MGMT

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
- Qualifiers
  - By Access/By Session
  - When successful/unsuccessful
- Can disable auditing
  - NOAUDIT is an option
- Output to DB, OS, XML
  - Syslog recommended

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

Default 11.2.0.4 Traditional Auditing

ALTER ANY PROCEDURE
ALTER ANY TABLE
ALTER DATABASE
ALTER PROFILE
ALTER SYSTEM
ALTER USER
AUDIT SYSTEM
CREATE ANY JOB
CREATE ANY LIBRARY
CREATE ANY PROCEDURE
CREATE ANY TABLE
CREATE EXTERNAL JOB
CREATE PUBLIC DATABASE LINK
CREATE SESSION
CREATE USER
DROP ANY PROCEDURE
DROP ANY TABLE
DROP PROFILE
DROP USER
EXEMPT ACCESS POLICY
GRANT ANY OBJECT PRIVILEGE
GRANT ANY PRIVILEGE
GRANT ANY ROLE
ROLE
DATABASE LINK
SYSTEM AUDIT
PROFILE
PUBLIC SYNONYM
SYSTEM GRANT

Primary Issues with Default Auditing

- **Is blind to your sensitive and PII data**
  - Tables with sensitive data may need Object auditing
  - Need to audit for grants to key tables and directories

- **Not protected and too often not acted on**
  - Sends audit logs to database itself
  - No alerting

Fine Grained Auditing (FGA)

- **Specific and conditional auditing (Boolean Check)**
  - Select SSN or salary > $200k when SQL query direct from database NOT from application
  - Protects **BOTH** base tables and associated views
  - SYS.FGA_LOG$ or DBA_COMMON_AUDIT_TRAIL
  - Don’t apply to LOBs

- **Part of Enterprise license**
  - Define using SYS.DBMS_FGA package
  - Logs to database or O/S
  - Manage purging with DBMS_AUDIT_MGMT

Example FGA Policy

```
DBMS_FGA.ADD_POLICY (
  object_schema      =>  'HR',
  object_name        =>  'PER_ALL_PEOPLE_F',
  policy_name        =>  'XXXX_FGA_NOT_GUI_PPF',
  audit_condition    =>  ' XX_FGA.XX_FGA_UTIL.SF_RUFFIAN_GATE_3 = 0 ',
  audit_column       =>  'national_identifier, date_of_birth',
  handler_schema     =>  NULL, -- used for calling alerts
  handler_module     =>  NULL, -- used for calling alerts
  enable             =>  TRUE,
  statement_types    =>  'SELECT',
  audit_trail        =>  DBMS_FGA.DB, -- Extended may expose sensitive data
  audit_column_opts  =>  DBMS_FGA.ANY_COLUMNS);
```

Audit Trails - Destinations and Values

Session Value	V$SESSION View	SYS_CONTEXT Function	SYS.AUD$ DBA_AUDIT_*	FGA_LOG$ AUDIT_TRAIL	Audit Vault
DB User Name	✓	✓	✓	✓	✓
Schema Name	✓	✓			
OS User Name	✓	✓	✓	✓	✓
Machine	✓	✓	✓	✓	✓
Terminal	✓	✓	✓		✓
Program	✓				✓
IP Address		✓	✓		✓
Client Process ID	✓				
Module	✓	✓			
Action	✓	✓			
Client Info	✓	✓			✓
Client ID	✓	✓	✓	✓	✓

Auditing Session Data

Database User Name	**OS User Name**	**Schema Name**
IP Address	**Machine/ User host**	**Terminal**
Program	**Client Process ID**	**Module**
Action	**Client Info**	**Client ID**

Auditing Session Data – Spoofable

Database User Name	~~OS User Name~~	~~Schema Name~~
IP Address	~~Machine/ User host~~	~~Terminal~~
~~Program~~	~~Client Process ID~~	~~Module~~
~~Action~~	~~Client Info~~	~~Client ID~~

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

Outside Database
Operating System
Network
Load Balancer
Storage
Backup Tools
Application

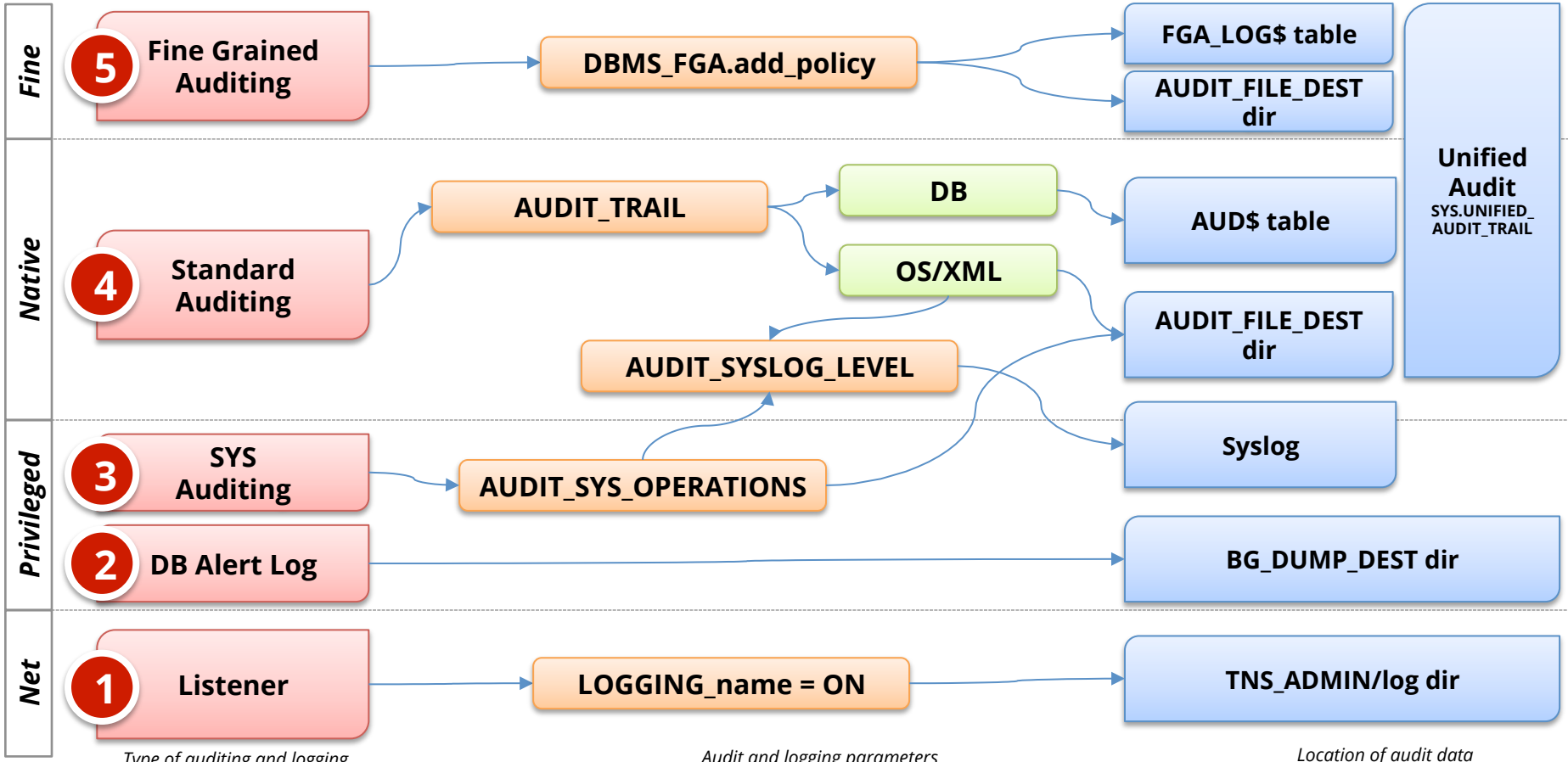
*Oracle 12c only

Oracle 12c Unified Auditing

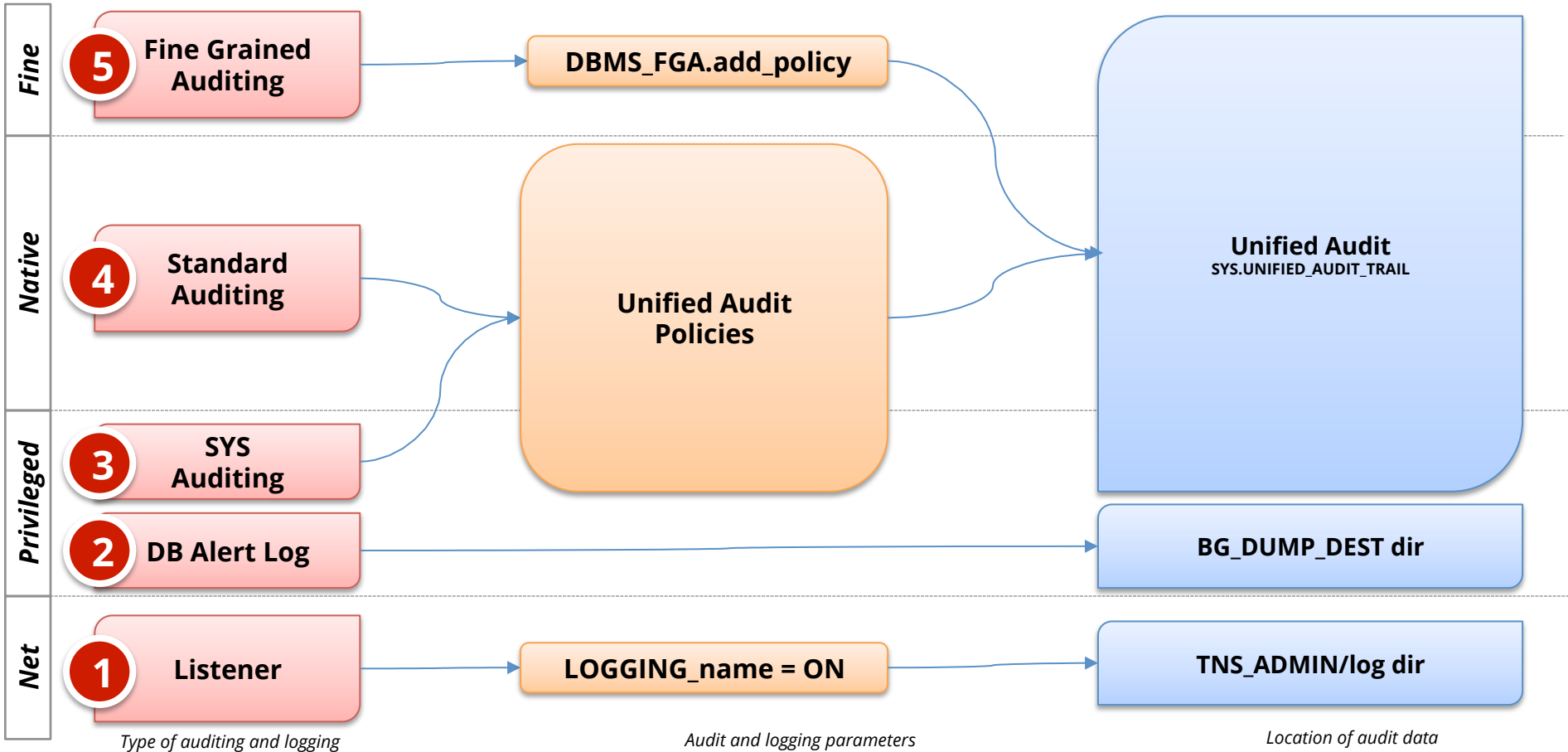
- **Everything changes**
  - Pure mode

- **Nothing changes**
  - Mixed mode (Default)
  - Unified Audit Trail populated in parallel to traditional auditing
  - Purge or disable ORA_SECURECONFIG Doc ID 1624051.1

Oracle 12c Database Auditing - Mixed



Oracle 12c Database Auditing - Pure



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

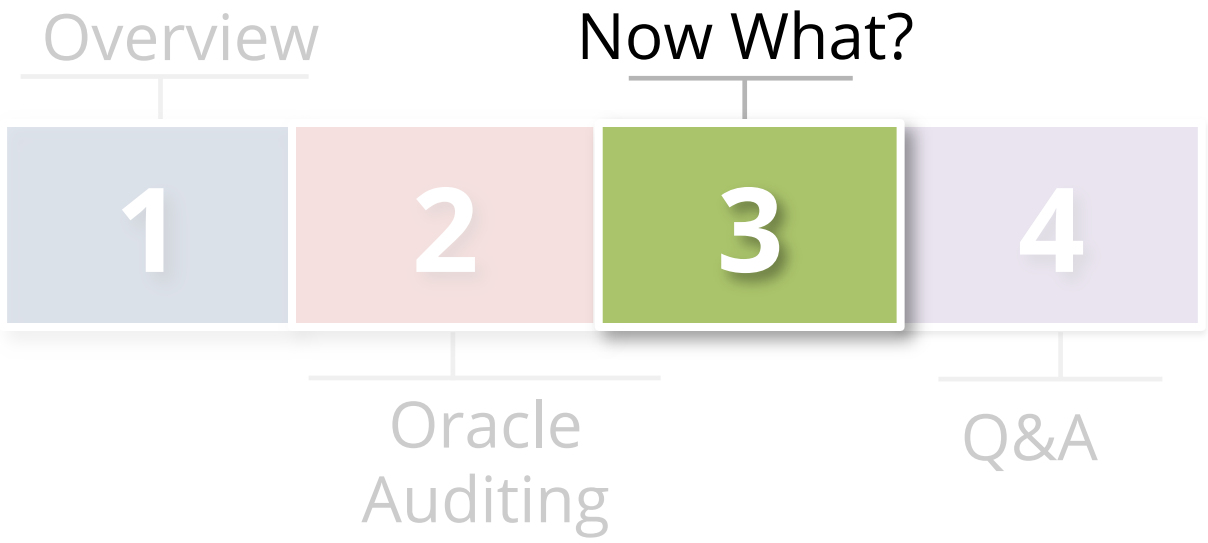
New Unified Audit Policy Based Syntax

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

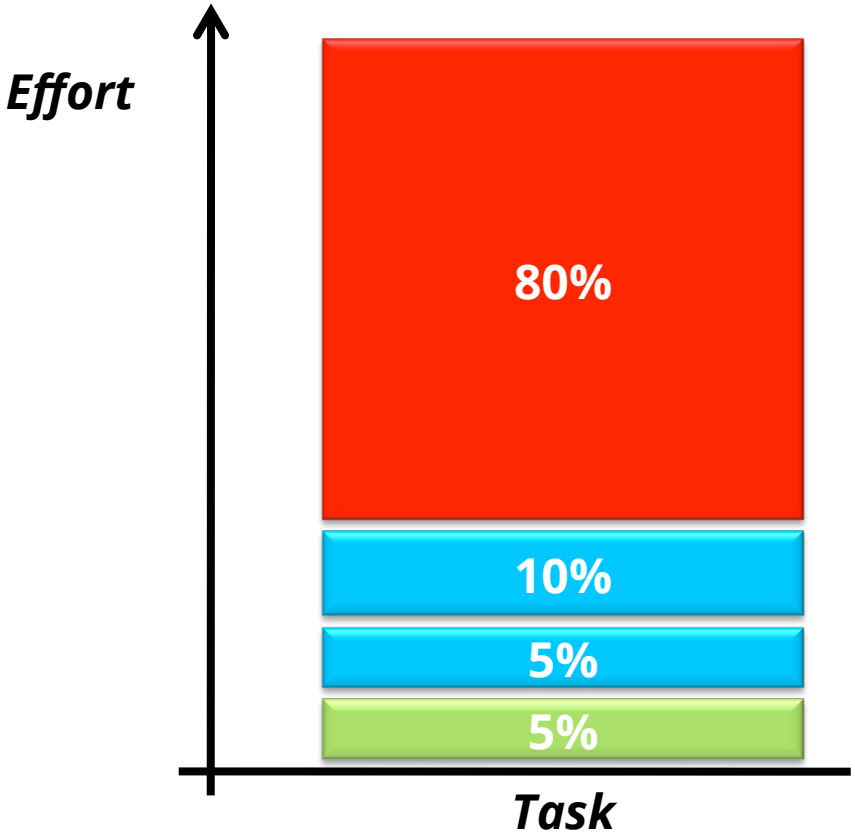
```
CREATE AUDIT POLICY policy_name
   { {privilege_audit_clause [action_audit_clause ]
[role_audit_clause ]}
       | { action_audit_clause  [role_audit_clause ] }
       | { role_audit_clause }
    }
   [WHEN audit_condition EVALUATE PER {STATEMENT|
SESSION|INSTANCE}]
   [CONTAINER = {CURRENT | ALL}];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

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

Agenda



Database Auditing Effort by Task



Monitoring, Alerting, Reporting, Reviewing

Archiving & Purging

Enable

Design

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

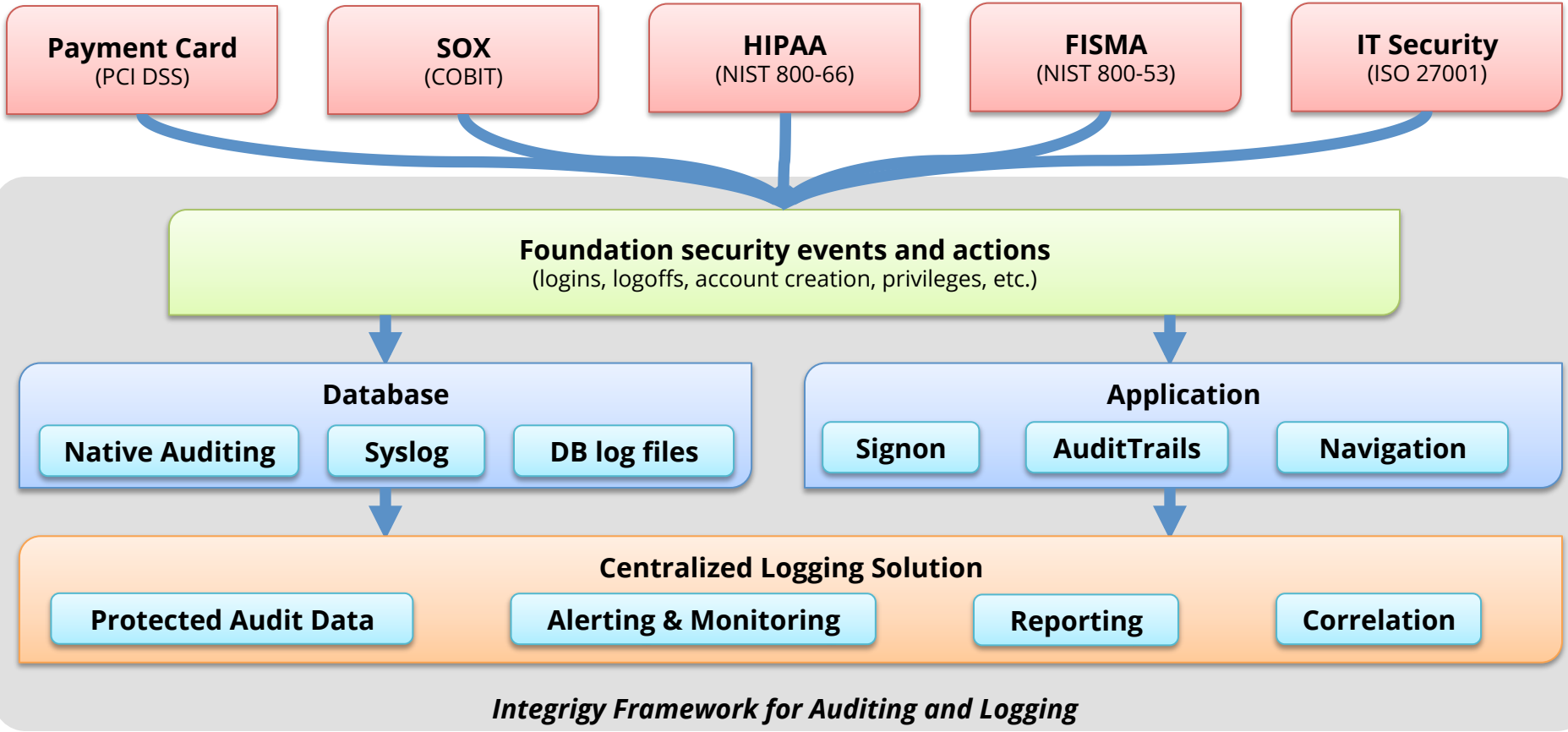
Ad-hoc Auditing Does Not Work – Use Framework

- **Standardize on common set of foundation events**
  - Need standardized information as basis for action
  - Need increases with number of databases
  - Apply to **ALL** databases

- **Discretely define**
  - What should be logged and audited
  - What should be alerted and reported on
  - Where is stored and how long is retrained

- **If looking for a starting point and/or direction**
  - http://www.integrigy.com/security-resources/integrigy-guide-database-auditing-and-logging

Recommended Framework for Database Auditing



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.

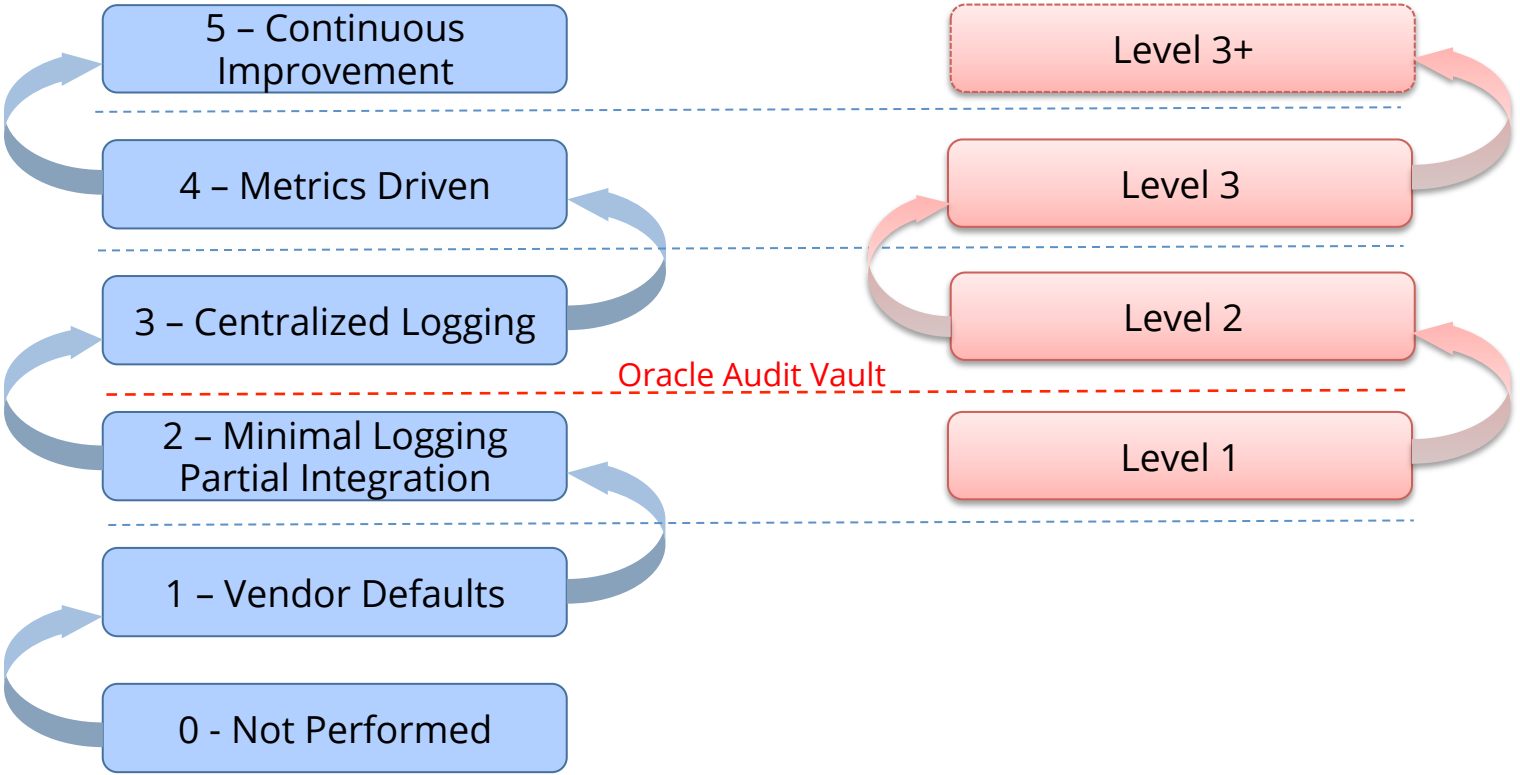
Unified Database Security Processes

- **Oracle Standards & Procedures**
- **SQL Server Standards & Procedures**
- **DB2 Standards & Procedures**
- **Sybase Standards & Procedures**

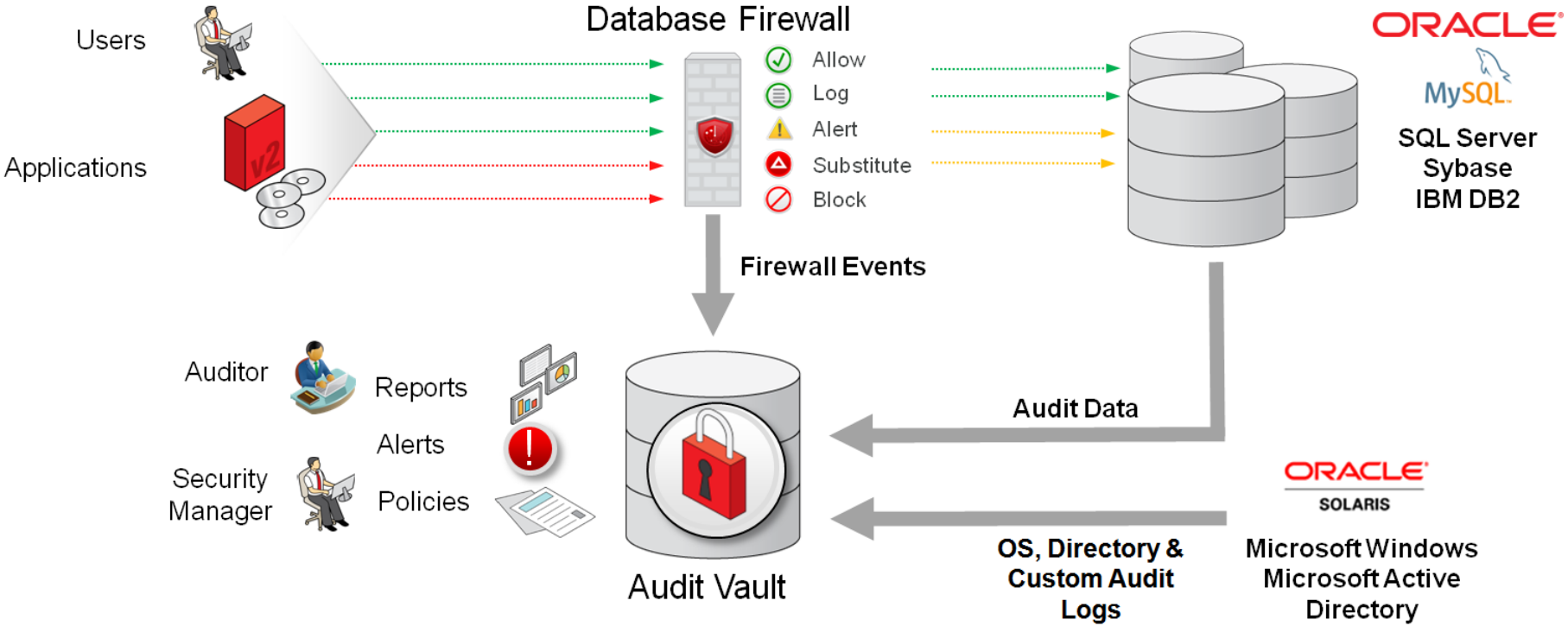
Integrigy Audit Framework Maturity Model

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 sensitive data and PII objects. Include **FGA** & **functional logging** and more complex alerting and monitoring.

Integrigy Audit Framework Maturity Maturity Model



Oracle Audit Vault and Database Firewall



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

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

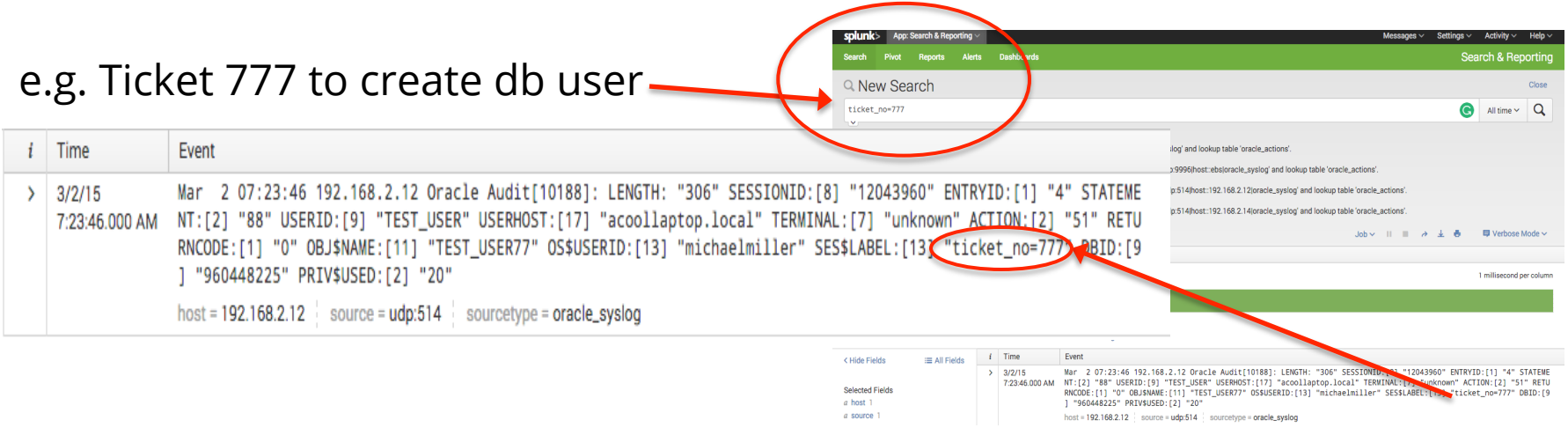
Framework	What to Monitor
E1	Key functional setup and configuration activity
E1	SYSADMIN usage pattern
E6, E11	E-Business Suite Proxy user grants
E5, E11	Database account creation and privilege changes

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

Use The Oracle Client Identifier to Track DBAs

- **Add change ticket numbers to audit stream**
  - Reconcile key database events to incident and change tickets
  - Use DBMS_SESSION.SET_IDENTIFIER('ticket_no='||v_ticket);
  - Combine with Secure Application Role to gate access to DBA role

e.g. Ticket 777 to create db user

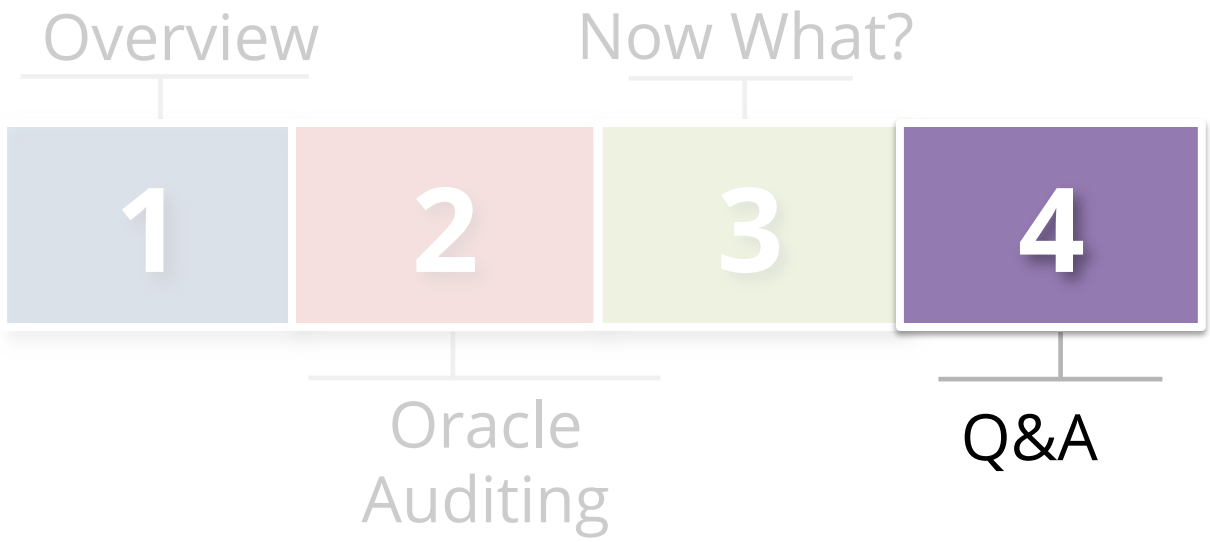


Use The Oracle Client Identifier to Track Users

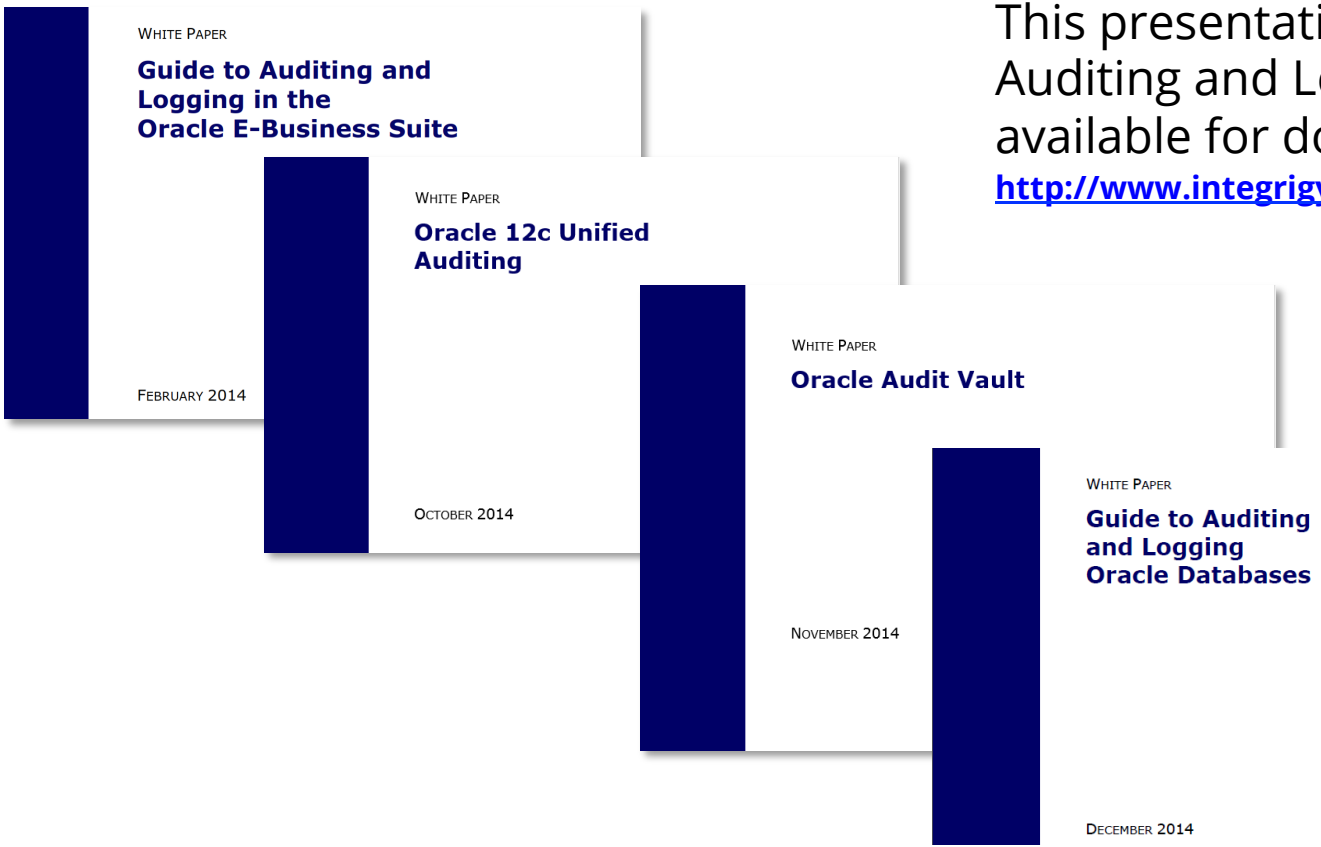
Application*	Example of how used
Oracle E-Business Suite	As of Release 12, the Oracle E-Business Suite automatically sets and updates CLIENT_IDENTIFIER to the FND_USER.USERNAME of the user logged on. Prior to Release 12, follow Support Note How to add DBMS_SESSION.SET_IDENTIFIER(FND_GLOBAL.USER_NAME) 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.
OBIEE	To pass the middle-tier username, 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)')

*Note: Client Identifier is passed to the audit trail. When connection pools are used will only see for active sessions.

Agenda



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: **mmiller@integrigy.com**

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

youtube: **youtube.com/integrigy**