INTEGRIGY

Developing Value from Oracle's Audit Vault
For Auditors and IT Security Professionals

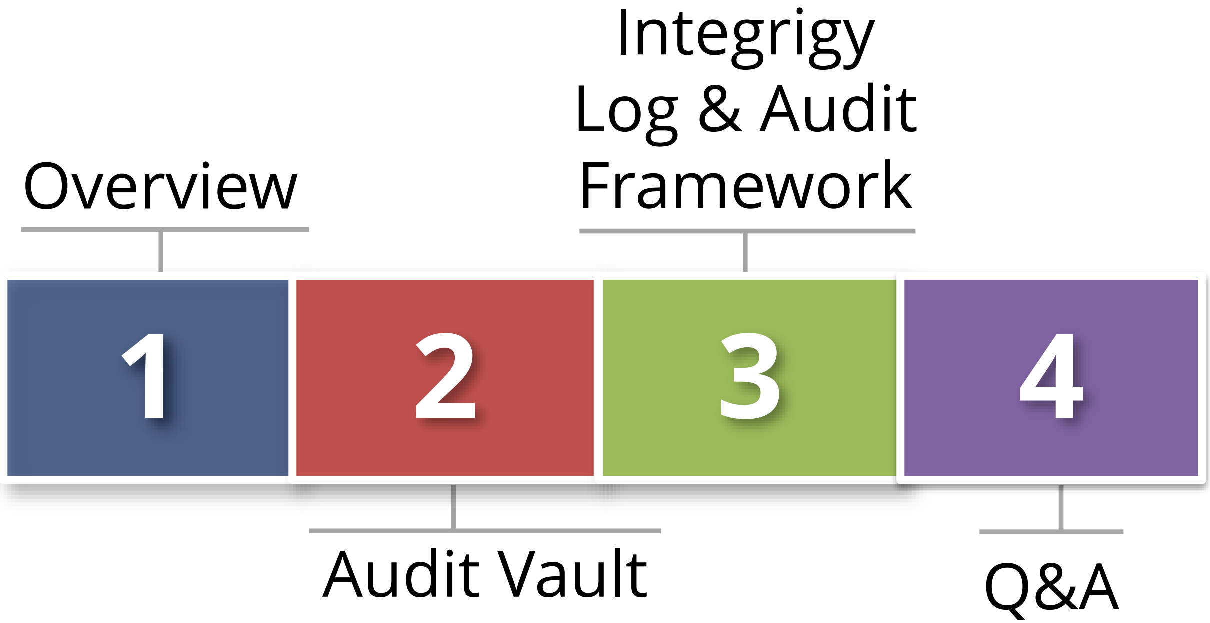
November 13, 2014

Michael Miller
Chief Security Officer
Integrigy Corporation

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

Agenda



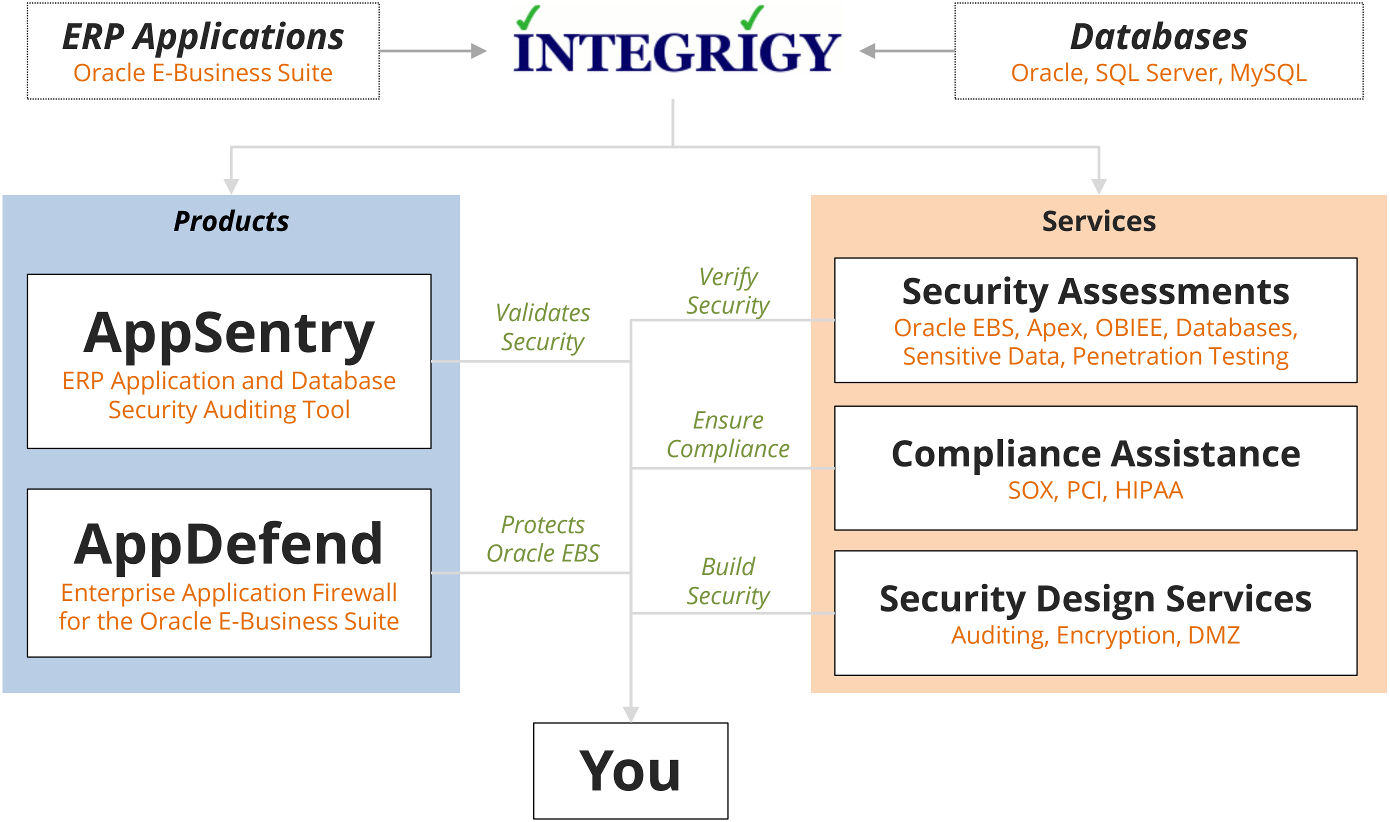
1 Overview

2 Audit Vault

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

AppDefend
Enterprise Application Firewall for the Oracle E-Business Suite

Validates Security

Protects Oracle EBS

Services

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

Compliance Assistance
SOX, PCI, HIPAA

Security Design Services
Auditing, Encryption, DMZ

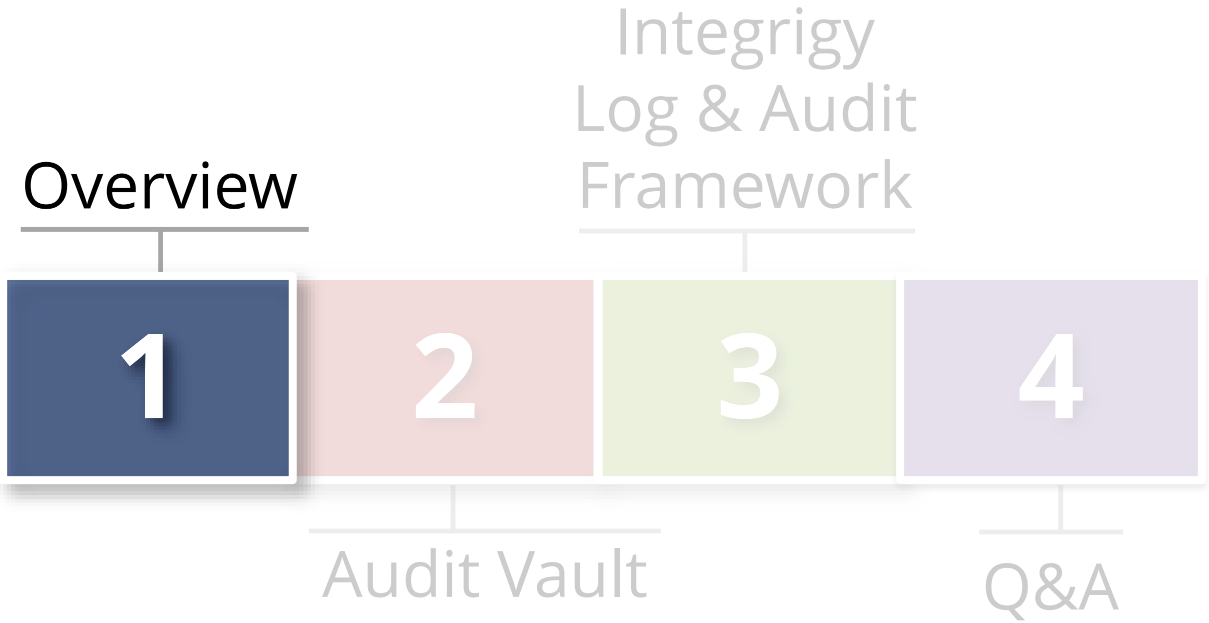
Verify Security

Ensure Compliance

Build Security

You

Agenda



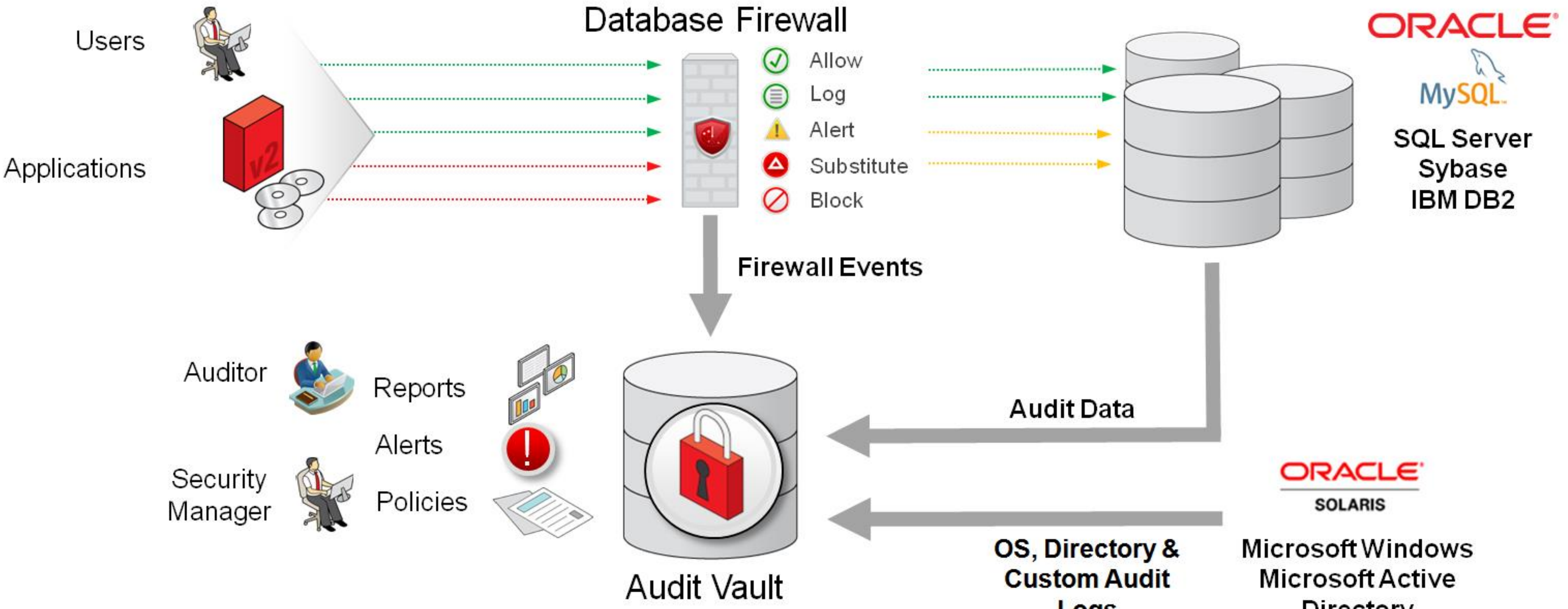
1 Overview

2 Audit Vault

3 Integrigy Log & Audit Framework

4 Q&A

Oracle Audit Vault and Database Firewall



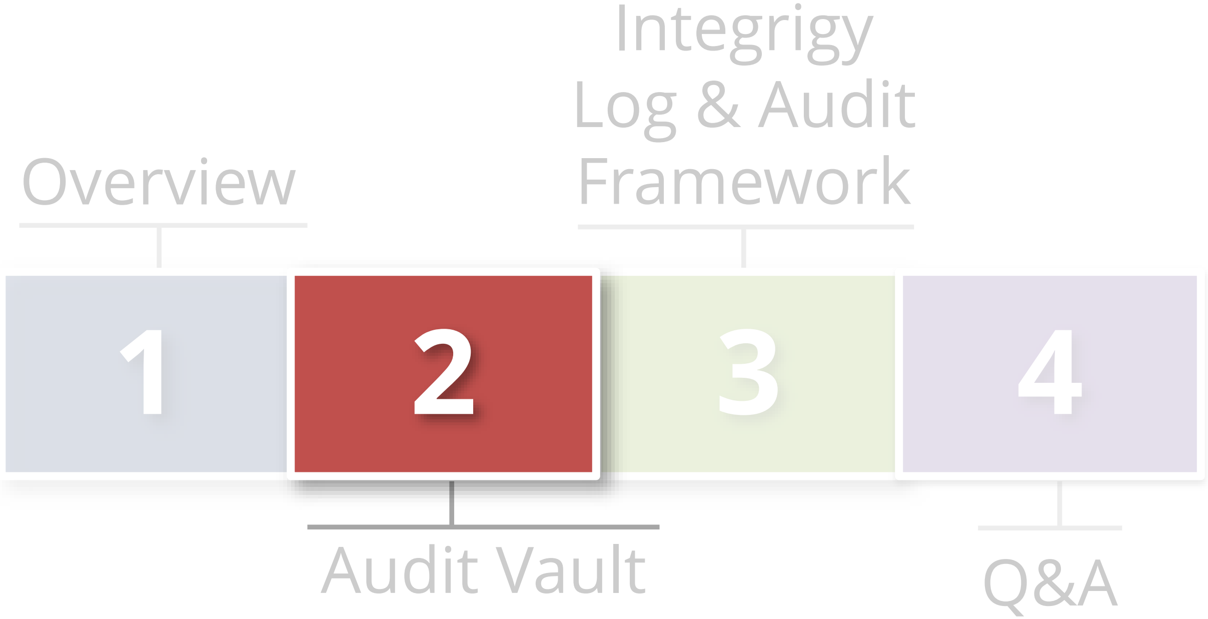
Oracle Audit Vault

- **One appliance for both Audit Vault and Firewall**
  - Virtual or physical

- **Secured appliance**
  - Database
  - Application and report server

- **Configure Audit Vault first**
  - First define hosts and secured targets
  - Database Firewall feeds Audit Vault
  - Database Vault feeds Audit Vault

Agenda



1 Overview

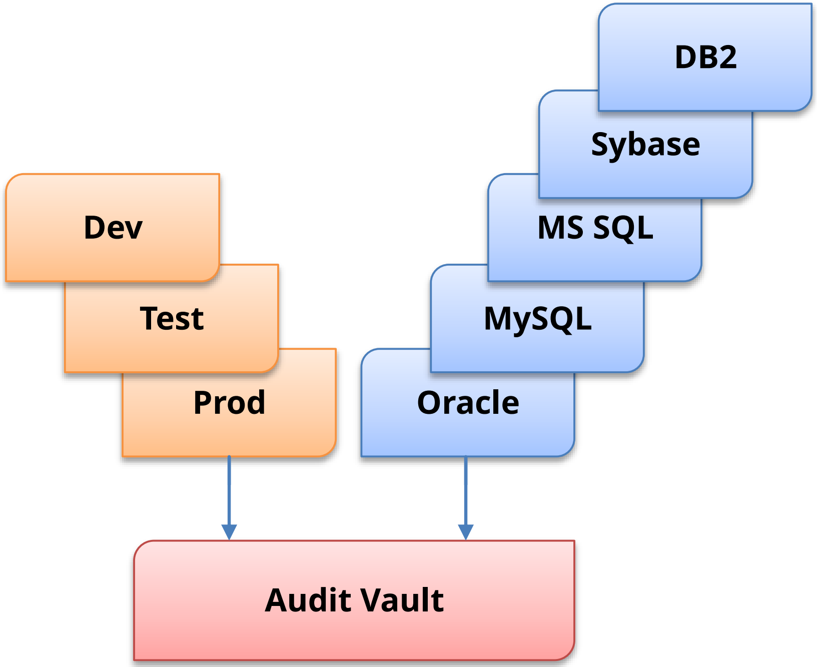
2 Audit Vault

3 Integrigy Log & Audit Framework

4 Q&A

About the Oracle Audit Vault

- **Tool built for Auditors and IT security professionals**
  - Alert suspicious activity
  - Detect and prevent insider threats
- **Oracle Audit Vault is a vault**
  - Warehouse of audit logs
- **Secure At-Source**
  - Does not generate the logs



With The Audit Vault Auditors Can …

- **Manage and apply audit policies to databases**
  - **Centrally provision** database audit settings to support security and compliance policies
  - Manage collection of audit settings on the databases
  - Compare against existing audit settings on database to required security and compliance policies

- **View dashboards**
  - Enterprise IT Security and audit overviews
  - Alerts and Reports
  - Audit Policies

Advantages of Oracle Audit Vault

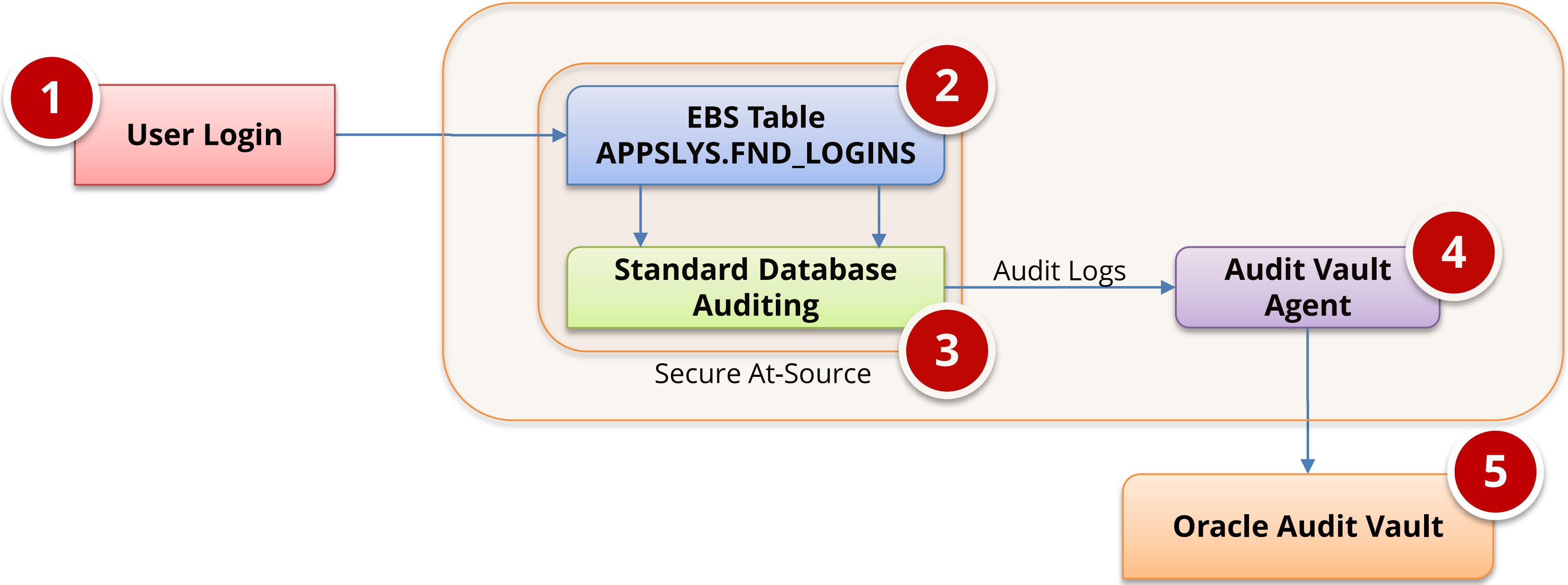
- **Leverage native database auditing beneath Apps**
  - Turn ON database auditing under application for compliance specific events (DDL, DBA logins)
  - Low performance impact
  - Fine-grained-audit (FGA) specific to sensitive tables

- **Application end-user identity propagation**
  - Pass "Client identifier” from mid-tier or initialize after connection – recorded in Audit trail

- **Extensible reporting capabilities**
  - 100+ standard reports
  - Build customer reports using BI Publisher

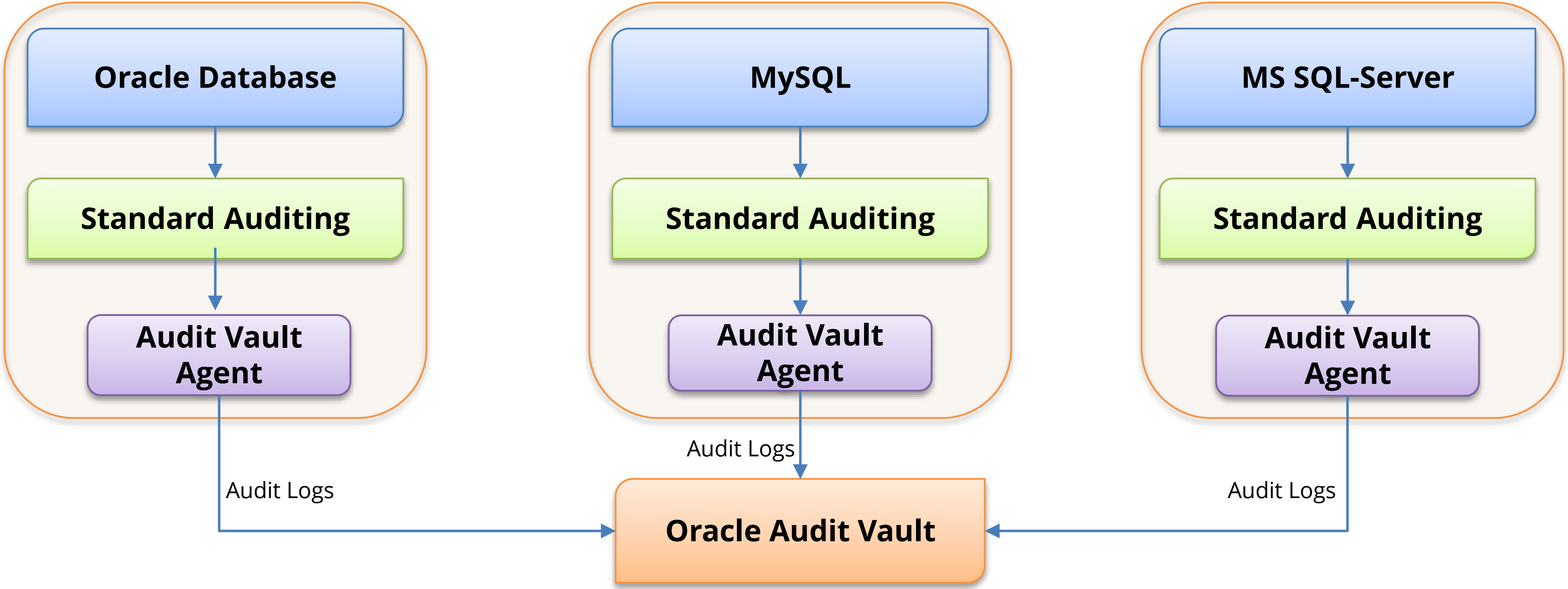
Secure At-Source Approach

The Oracle Audit Vault uses the concept of **Secure At-Source** to protect application log and audit tables at the source.

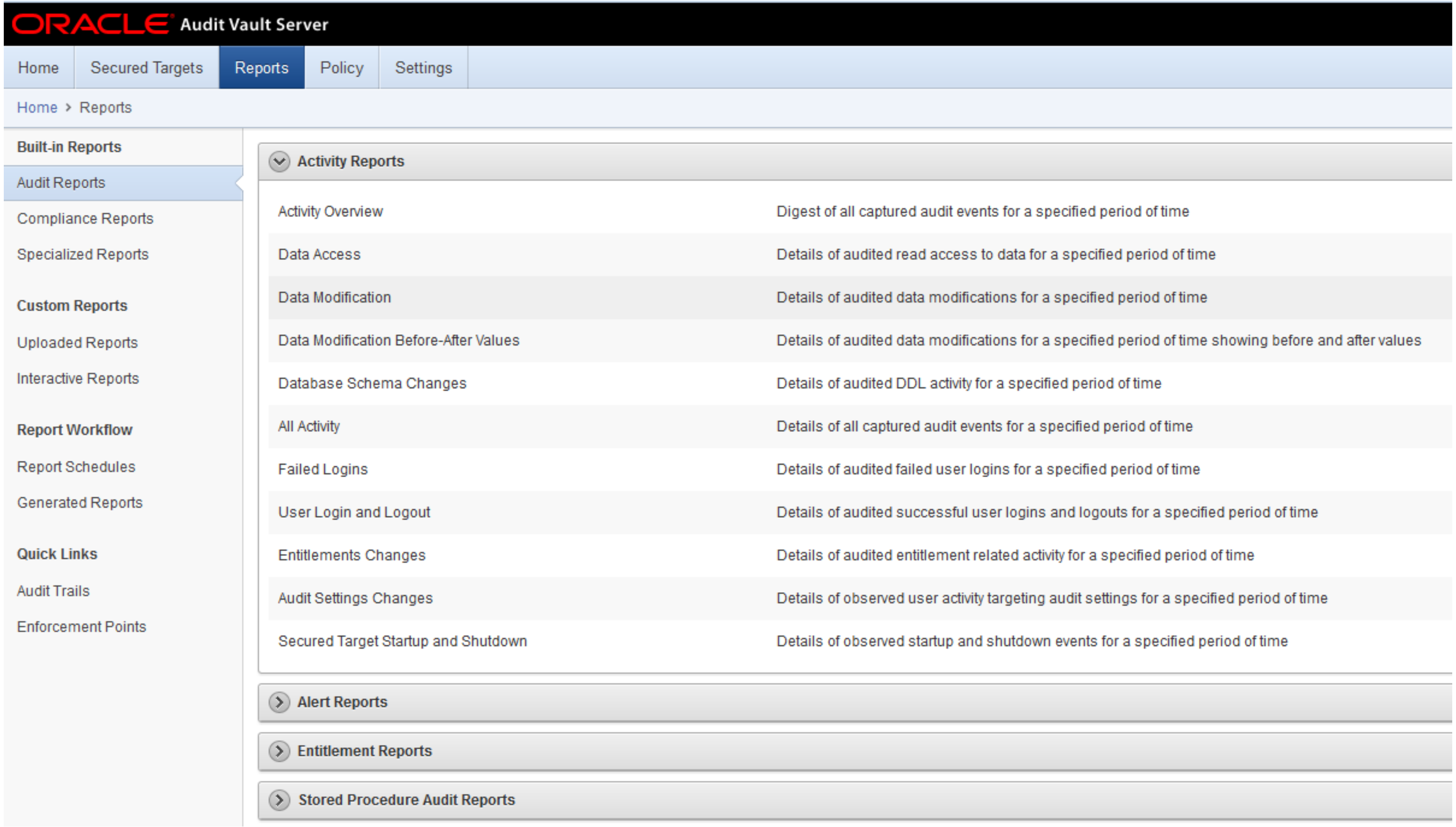


How Audit Vault Works

Agents are deployed and activated on source systems to forward audit log data. Agents are managed through the Audit Vault application.



100+ Standard Reports



Activity Reports

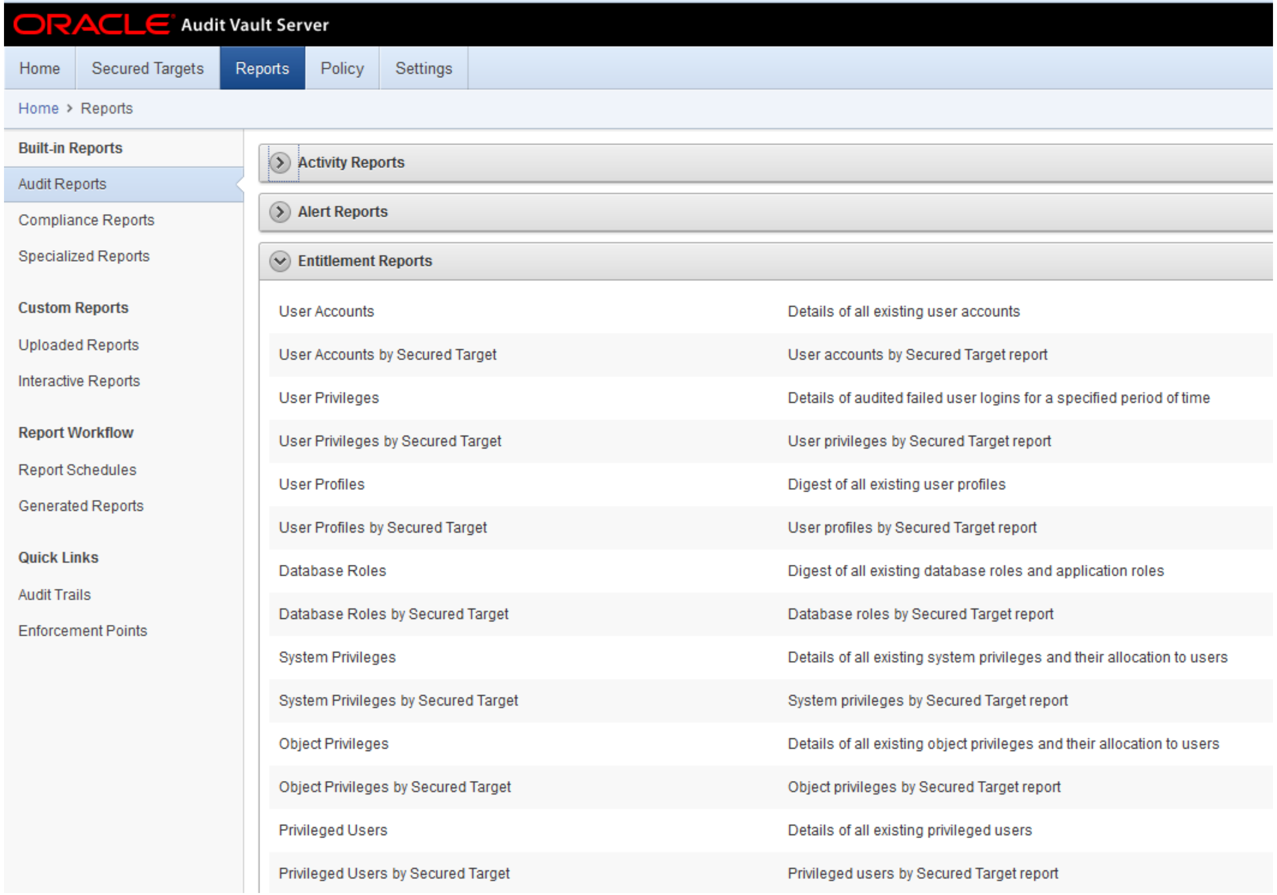
Activity Overview	Digest of all captured audit events for a specified period of time
Data Access	Details of audited read access to data for a specified period of time
Data Modification	Details of audited data modifications for a specified period of time
Data Modification Before-After Values	Details of audited data modifications for a specified period of time showing before and after values
Database Schema Changes	Details of audited DDL activity for a specified period of time
All Activity	Details of all captured audit events for a specified period of time
Failed Logins	Details of audited failed user logins for a specified period of time
User Login and Logout	Details of audited successful user logins and logouts for a specified period of time
Entitlements Changes	Details of audited entitlement related activity for a specified period of time
Audit Settings Changes	Details of observed user activity targeting audit settings for a specified period of time
Secured Target Startup and Shutdown	Details of observed startup and shutdown events for a specified period of time

Alert Reports

Entitlement Reports

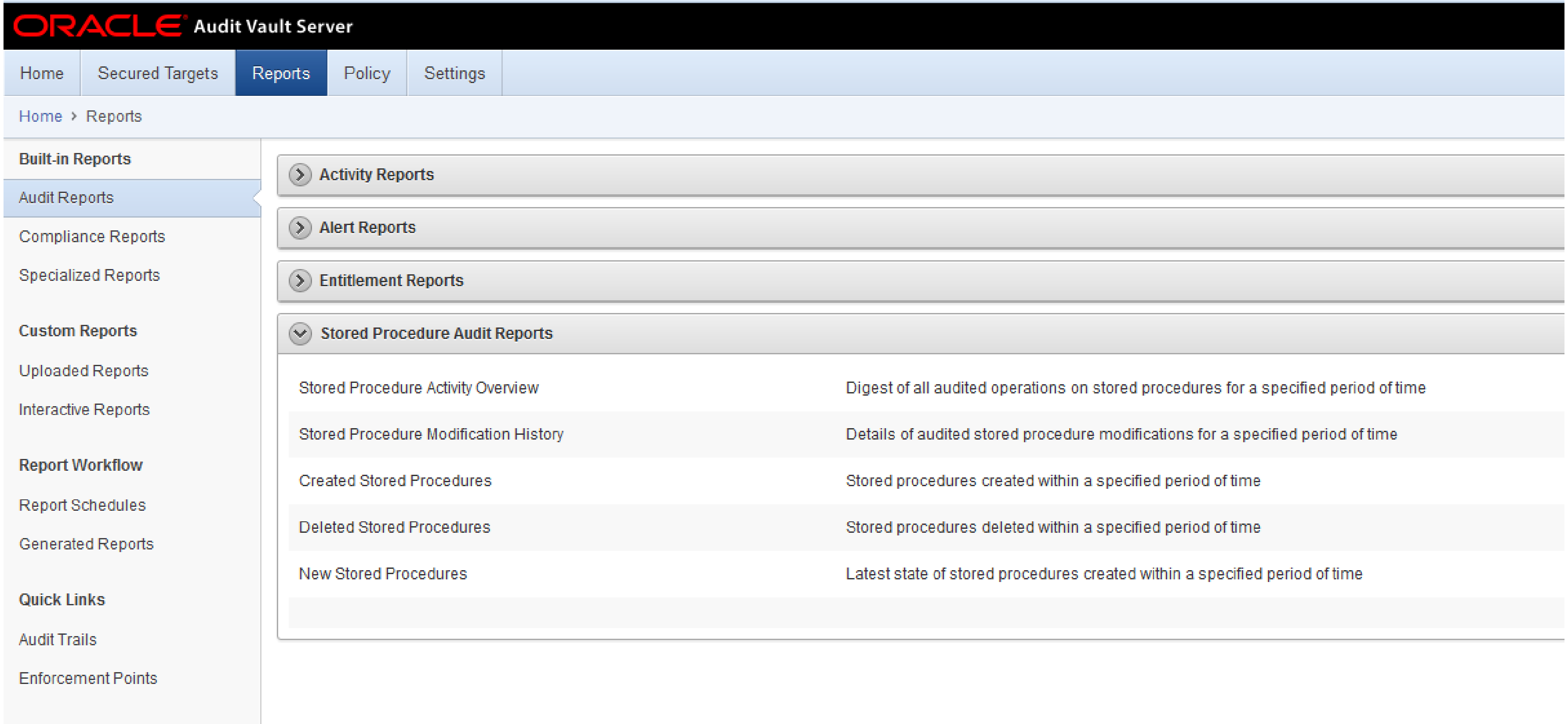
Stored Procedure Audit Reports

Entitlement Reports



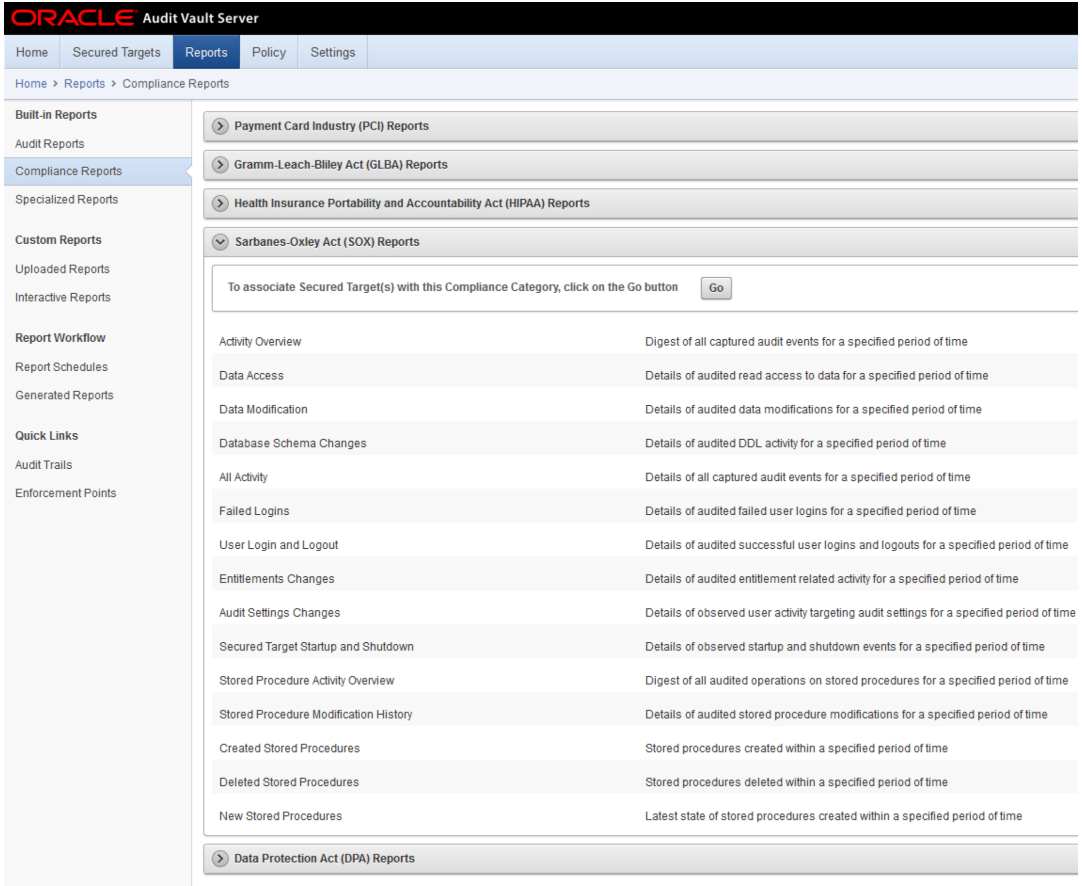
User Accounts	Details of all existing user accounts
User Accounts by Secured Target	User accounts by Secured Target report
User Privileges	Details of audited failed user logins for a specified period of time
User Privileges by Secured Target	User privileges by Secured Target report
User Profiles	Digest of all existing user profiles
User Profiles by Secured Target	User profiles by Secured Target report
Database Roles	Digest of all existing database roles and application roles
Database Roles by Secured Target	Database roles by Secured Target report
System Privileges	Details of all existing system privileges and their allocation to users
System Privileges by Secured Target	System privileges by Secured Target report
Object Privileges	Details of all existing object privileges and their allocation to users
Object Privileges by Secured Target	Object privileges by Secured Target report
Privileged Users	Details of all existing privileged users
Privileged Users by Secured Target	Privileged users by Secured Target report

Stored Procedure Auditing



Stored Procedure Activity Overview	Digest of all audited operations on stored procedures for a specified period of time
Stored Procedure Modification History	Details of audited stored procedure modifications for a specified period of time
Created Stored Procedures	Stored procedures created within a specified period of time
Deleted Stored Procedures	Stored procedures deleted within a specified period of time
New Stored Procedures	Latest state of stored procedures created within a specified period of time

Compliance Reports



Payment Card Industry (PCI) Reports

Gramm-Leach-Bliley Act (GLBA) Reports

Health Insurance Portability and Accountability Act (HIPAA) Reports

Sarbanes-Oxley Act (SOX) Reports

To associate Secured Target(s) with this Compliance Category, click on the Go button

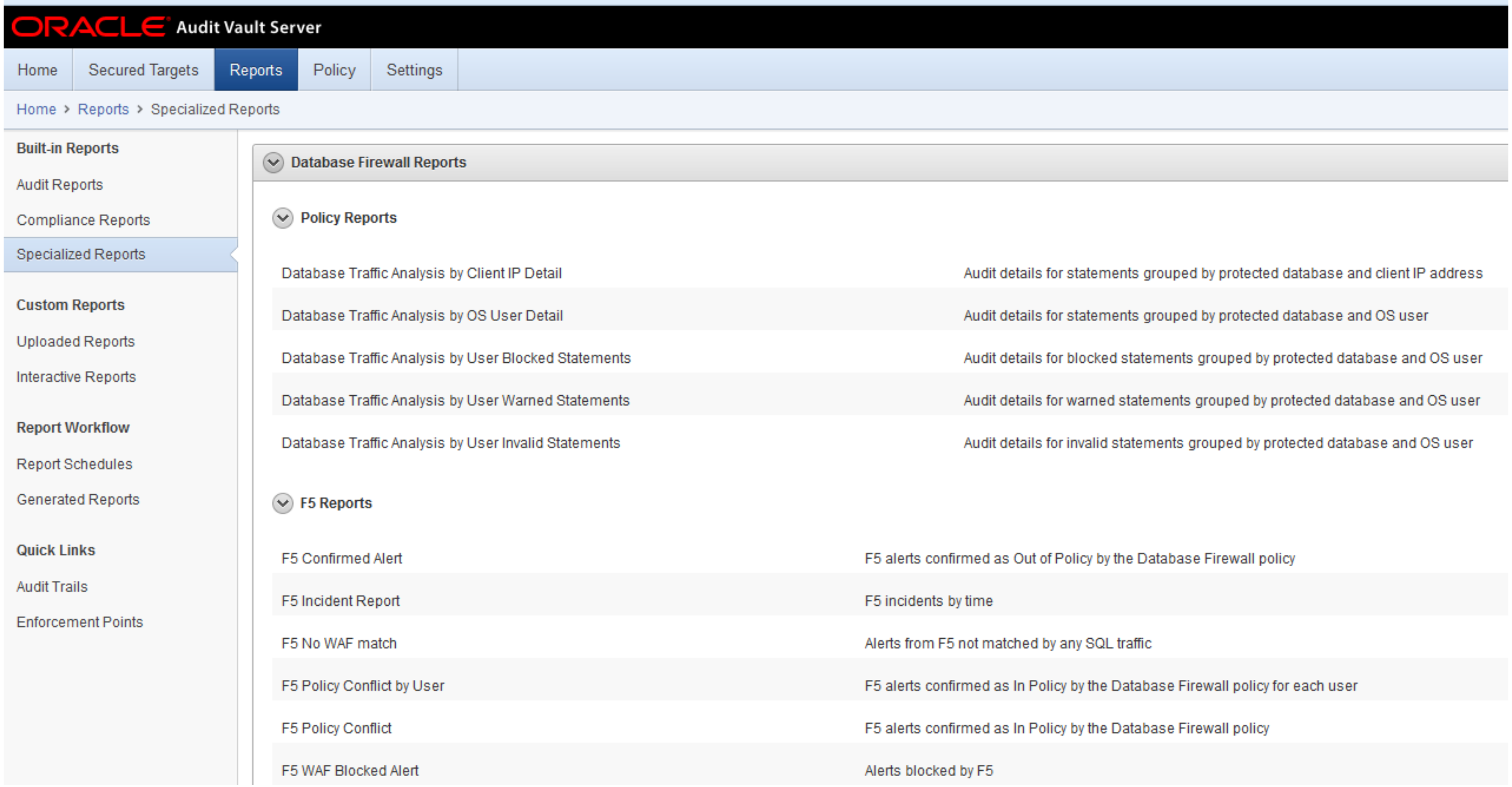
Activity Overview	Digest of all captured audit events for a specified period of time
Data Access	Details of audited read access to data for a specified period of time
Data Modification	Details of audited data modifications for a specified period of time
Database Schema Changes	Details of audited DDL activity for a specified period of time
All Activity	Details of all captured audit events for a specified period of time
Failed Logins	Details of audited failed user logins for a specified period of time
User Login and Logout	Details of audited successful user logins and logouts for a specified period of time
Entitlements Changes	Details of audited entitlement related activity for a specified period of time
Audit Settings Changes	Details of observed user activity targeting audit settings for a specified period of time
Secured Target Startup and Shutdown	Details of observed startup and shutdown events for a specified period of time
Stored Procedure Activity Overview	Digest of all audited operations on stored procedures for a specified period of time
Stored Procedure Modification History	Details of audited stored procedure modifications for a specified period of time
Created Stored Procedures	Stored procedures created within a specified period of time
Deleted Stored Procedures	Stored procedures deleted within a specified period of time
New Stored Procedures	Latest state of stored procedures created within a specified period of time

Data Protection Act (DPA) Reports

Out-of-the-box standard reports for:

- PCI
- Gramm-Leach-Bliley
- HIPAA
- SOX
- DPA

Database Firewall and F5 Reports



Database Firewall Reports

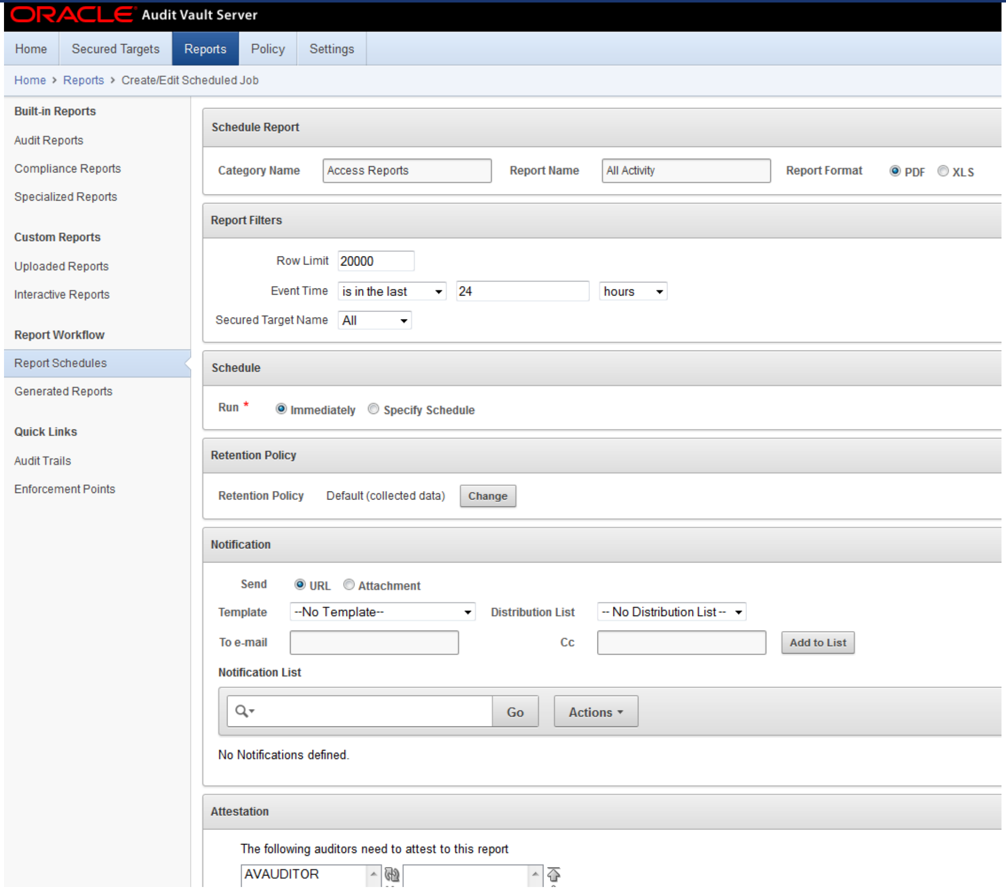
Policy Reports

Database Traffic Analysis by Client IP Detail	Audit details for statements grouped by protected database and client IP address
Database Traffic Analysis by OS User Detail	Audit details for statements grouped by protected database and OS user
Database Traffic Analysis by User Blocked Statements	Audit details for blocked statements grouped by protected database and OS user
Database Traffic Analysis by User Warned Statements	Audit details for warned statements grouped by protected database and OS user
Database Traffic Analysis by User Invalid Statements	Audit details for invalid statements grouped by protected database and OS user

F5 Reports

F5 Confirmed Alert	F5 alerts confirmed as Out of Policy by the Database Firewall policy
F5 Incident Report	F5 incidents by time
F5 No WAF match	Alerts from F5 not matched by any SQL traffic
F5 Policy Conflict by User	F5 alerts confirmed as In Policy by the Database Firewall policy for each user
F5 Policy Conflict	F5 alerts confirmed as In Policy by the Database Firewall policy
F5 WAF Blocked Alert	Alerts blocked by F5

Report Options



Schedule Report

Category Name: Access Reports
Report Name: All Activity
Report Format: ● PDF ○ XLS

Report Filters

Row Limit: 20000
Event Time: is in the last 24 hours
Secured Target Name: All

Schedule

Run *: ● Immediately ○ Specify Schedule

Retention Policy

Retention Policy: Default (collected data) Change

Notification

Send: ● URL ○ Attachment
Template: --No Template--
Distribution List: -- No Distribution List --
To e-mail:
Cc:
Add to List

Notification List

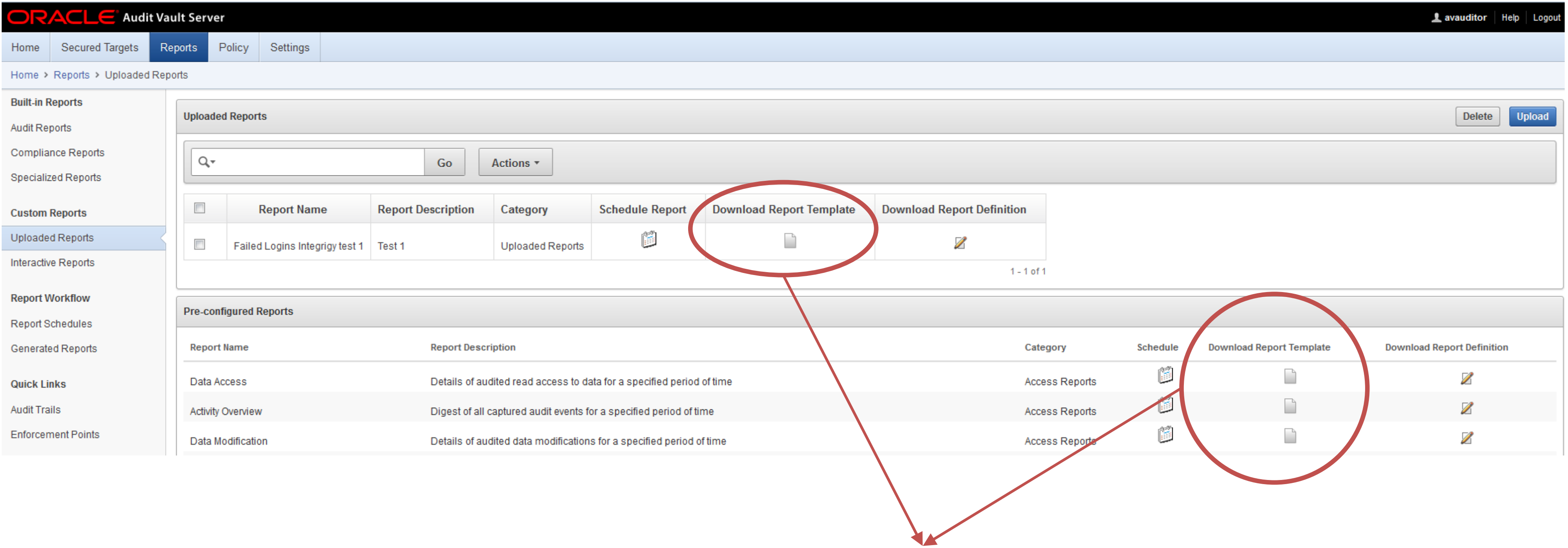
No Notifications defined.

Attestation

The following auditors need to attest to this report

AVAUDITOR

BI Publisher for Custom Reports



Uploaded Reports

☐	Report Name	Report Description	Category	Schedule Report	Download Report Template	Download Report Definition
☐	Failed Logins Integrigy test 1	Test 1	Uploaded Reports	📋	📄	✎

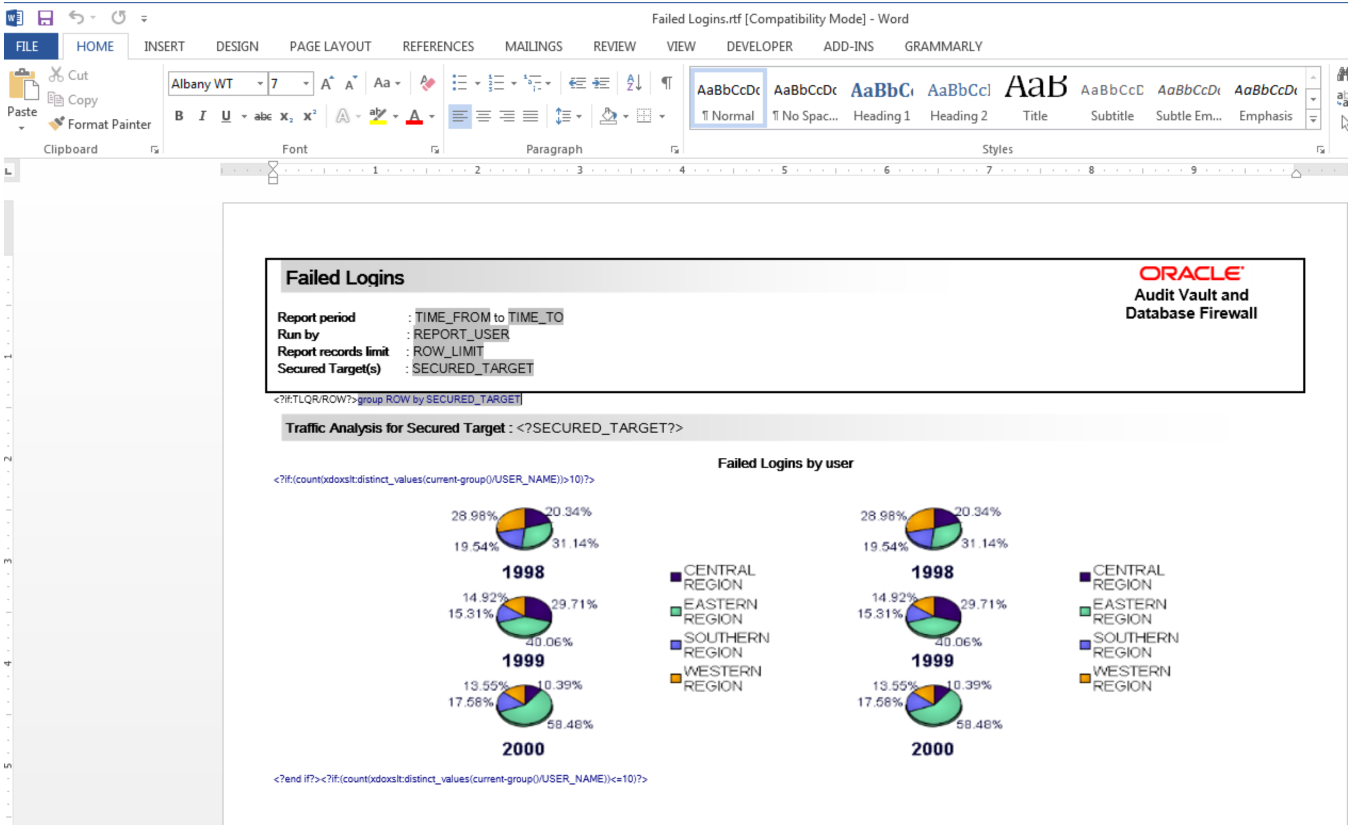
1 - 1 of 1

Pre-configured Reports

Report Name	Report Description	Category	Schedule	Download Report Template	Download Report Definition
Data Access	Details of audited read access to data for a specified period of time	Access Reports	📋	📄	✎
Activity Overview	Digest of all captured audit events for a specified period of time	Access Reports	📋	📄	✎
Data Modification	Details of audited data modifications for a specified period of time	Access Reports	📋	📄	✎

Download template to BI Publisher to edit

BI Publisher for Custom Reports



Failed Logins.rtf [Compatibility Mode] - Word

Failed Logins

ORACLE
Audit Vault and
Database Firewall

Report period	: TIME_FROM to TIME_TO
Run by	: REPORT_USER
Report records limit	: ROW_LIMIT
Secured Target(s)	: SECURED_TARGET

```
<?if:TLQR/ROW?>group ROW by SECURED_TARGET
```

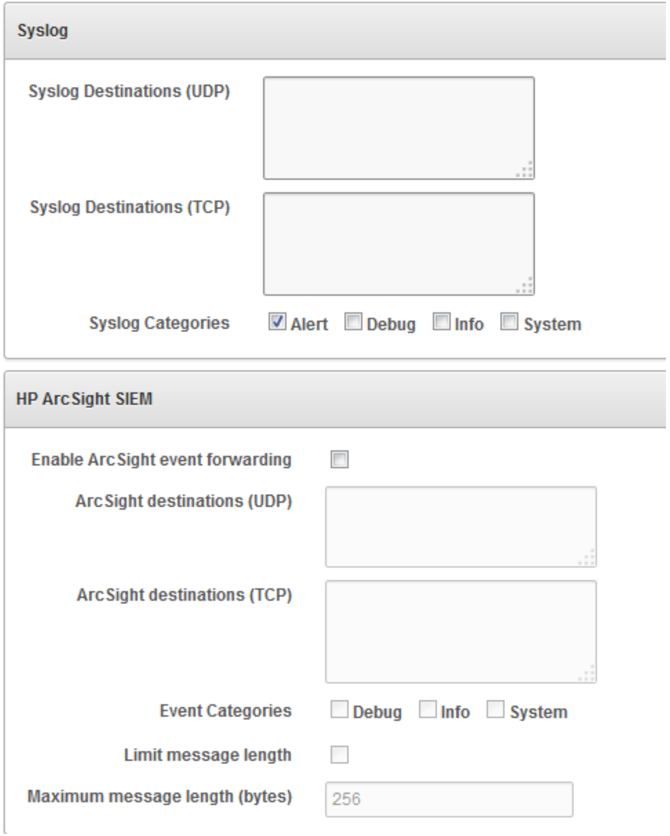
Traffic Analysis for Secured Target : <?SECURED_TARGET?>

Failed Logins by user

```
<?if:(count(xdoxslt:distinct_values(current-group()/USER_NAME))>10)?>
```

```
<?end if?><?if:(count(xdoxslt:distinct_values(current-group()/USER_NAME))<=10)?>
```

Forward Alerts to Syslog, ArcSight, or Remedy



Syslog

Syslog Destinations (UDP)

Syslog Destinations (TCP)

Syslog Categories ☑ Alert □ Debug □ Info □ System

HP ArcSight SIEM

Enable ArcSight event forwarding □

ArcSight destinations (UDP)

ArcSight destinations (TCP)

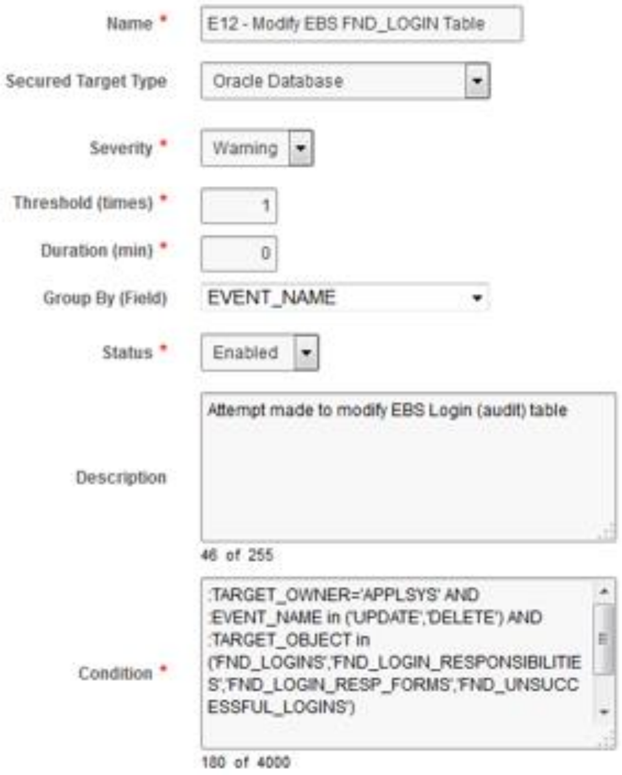
Event Categories □ Debug □ Info □ System

Limit message length □

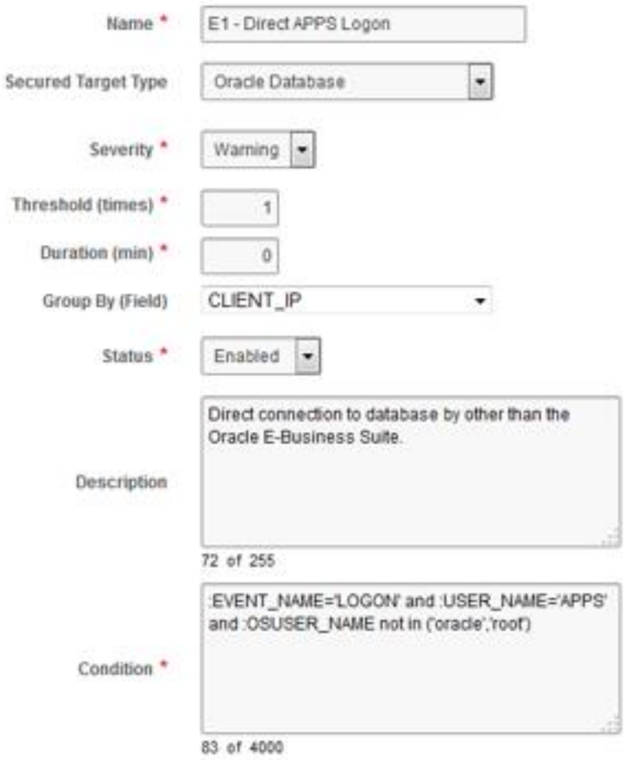
Maximum message length (bytes) 256

- Standard functionality to send alert to ArcSight and Syslog
- BMC Remedy Action Request Server integration through standard templates
  - Version 7.x and higher

Custom Alerts for Key Security Events

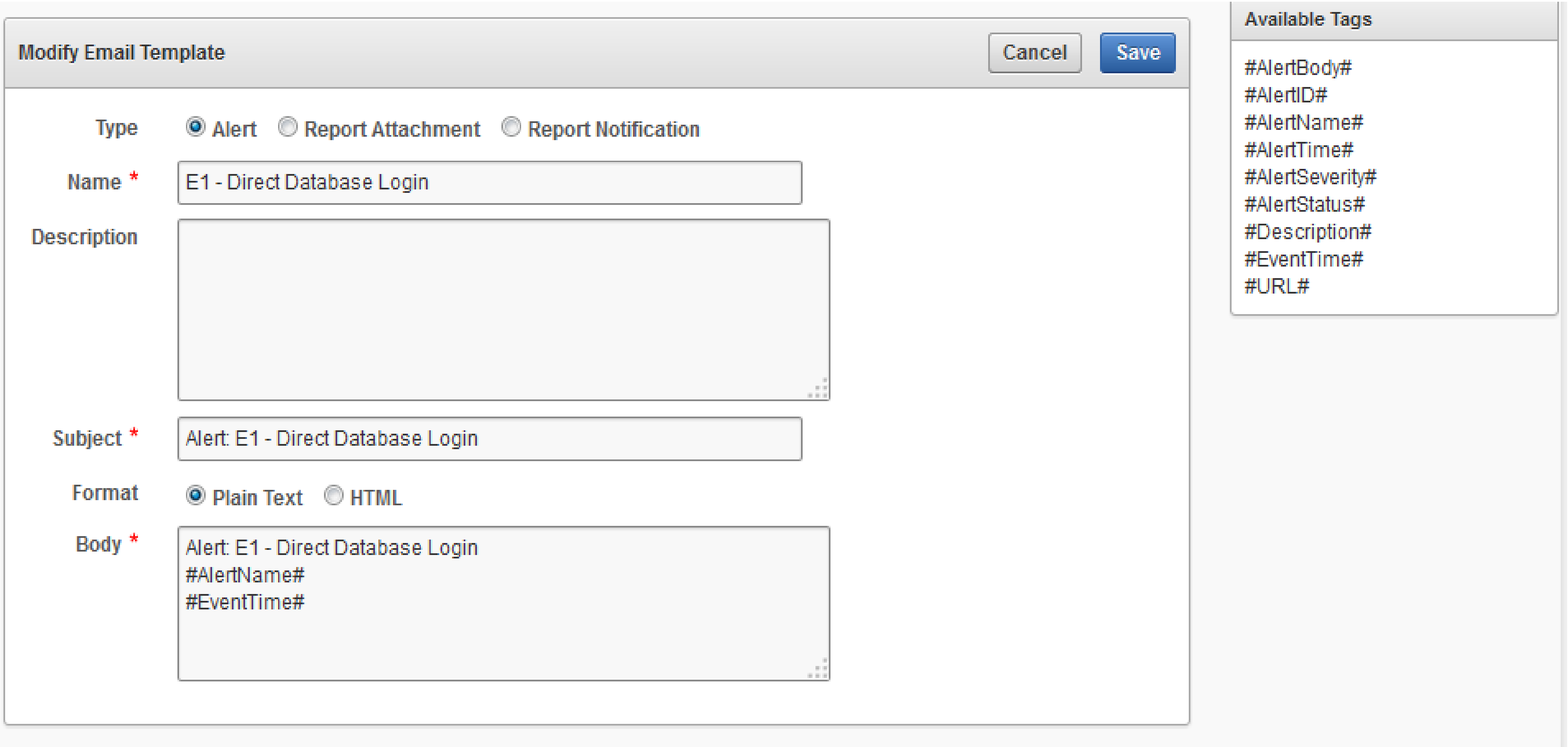


Name *	E12 - Modify EBS FND_LOGIN Table
Secured Target Type	Oracle Database
Severity *	Warning
Threshold (times) *	1
Duration (min) *	0
Group By (Field)	EVENT_NAME
Status *	Enabled
Description	Attempt made to modify EBS Login (audit) table 46 of 255
Condition *	:TARGET_OWNER='APPLSYS' AND :EVENT_NAME in ('UPDATE','DELETE') AND :TARGET_OBJECT in ('FND_LOGINS','FND_LOGIN_RESPONSIBILITIES','FND_LOGIN_RESP_FORMS','FND_UNSUCCESSFUL_LOGINS') 180 of 4000



Name *	E1 - Direct APPS Logon
Secured Target Type	Oracle Database
Severity *	Warning
Threshold (times) *	1
Duration (min) *	0
Group By (Field)	CLIENT_IP
Status *	Enabled
Description	Direct connection to database by other than the Oracle E-Business Suite. 72 of 255
Condition *	:EVENT_NAME='LOGON' and :USER_NAME='APPS' and :OSUSER_NAME not in ('oracle','root') 83 of 4000

Email Notifications



Modify Email Template

Type ● Alert ○ Report Attachment ○ Report Notification

Name * E1 - Direct Database Login

Description

Subject * Alert: E1 - Direct Database Login

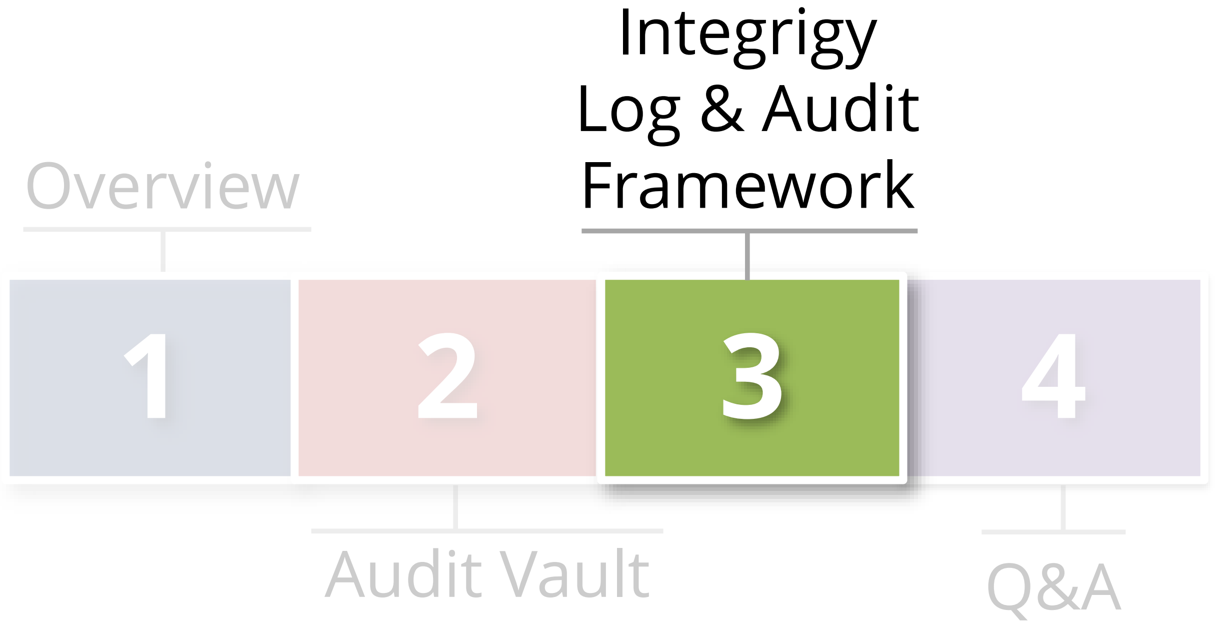
Format ● Plain Text ○ HTML

Body *
Alert: E1 - Direct Database Login
#AlertName#
#EventTime#

Available Tags

#AlertBody#
#AlertID#
#AlertName#
#AlertTime#
#AlertSeverity#
#AlertStatus#
#Description#
#EventTime#
#URL#

Agenda



1 Overview

2 Audit Vault

3 Integrigy Log & Audit Framework

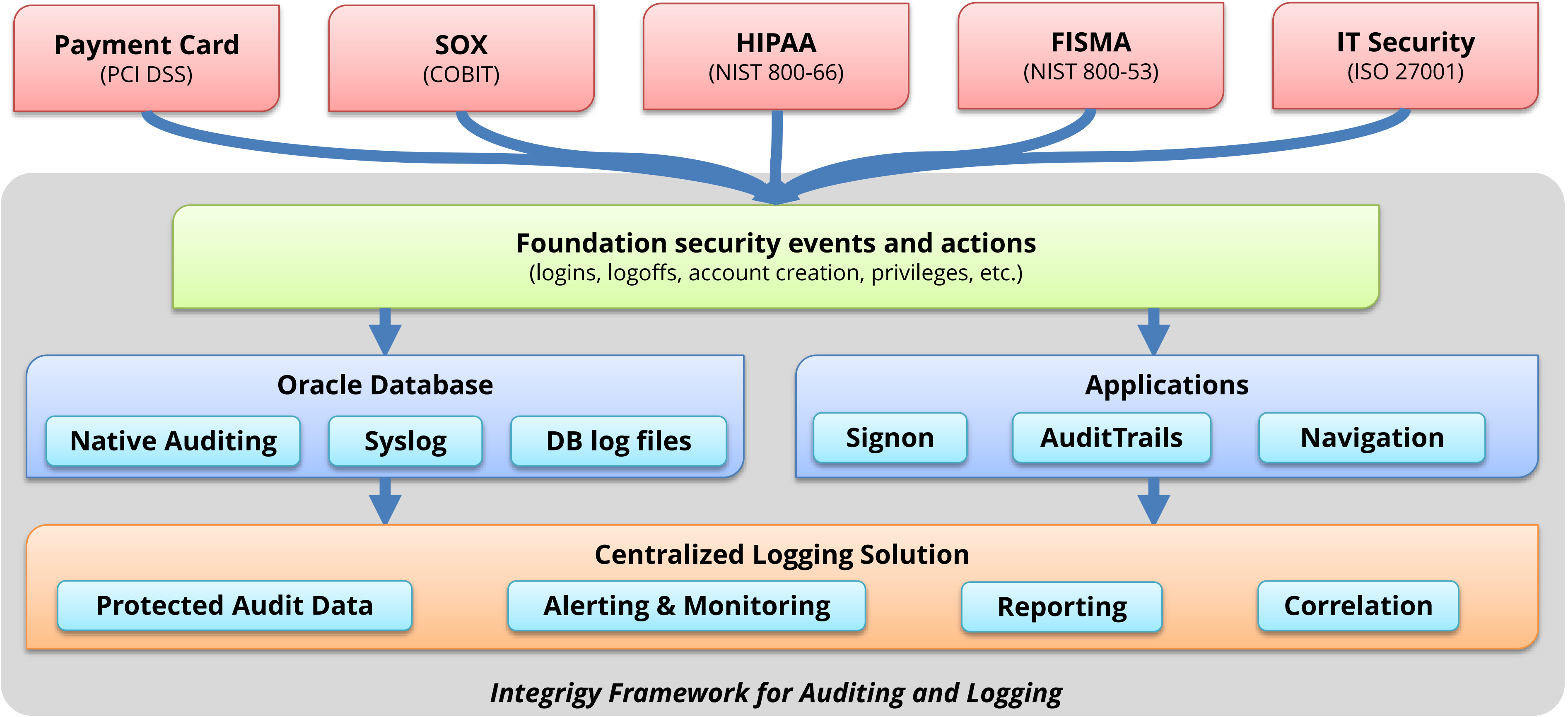
4 Q&A

Why Talk About the Framework?

- **Value is generated through data**
  - Audit Vault is only a data warehouse
  - Logs are generated by the source databases

- **Integrigy's Framework for Database Auditing defines content for the Oracle Audit Vault**
  - Defines what should be audited and alerted
  - Starting point and/or 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.)

Oracle Database

- **Native Auditing**
- **Syslog**
- **DB log files**

Applications

- **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**

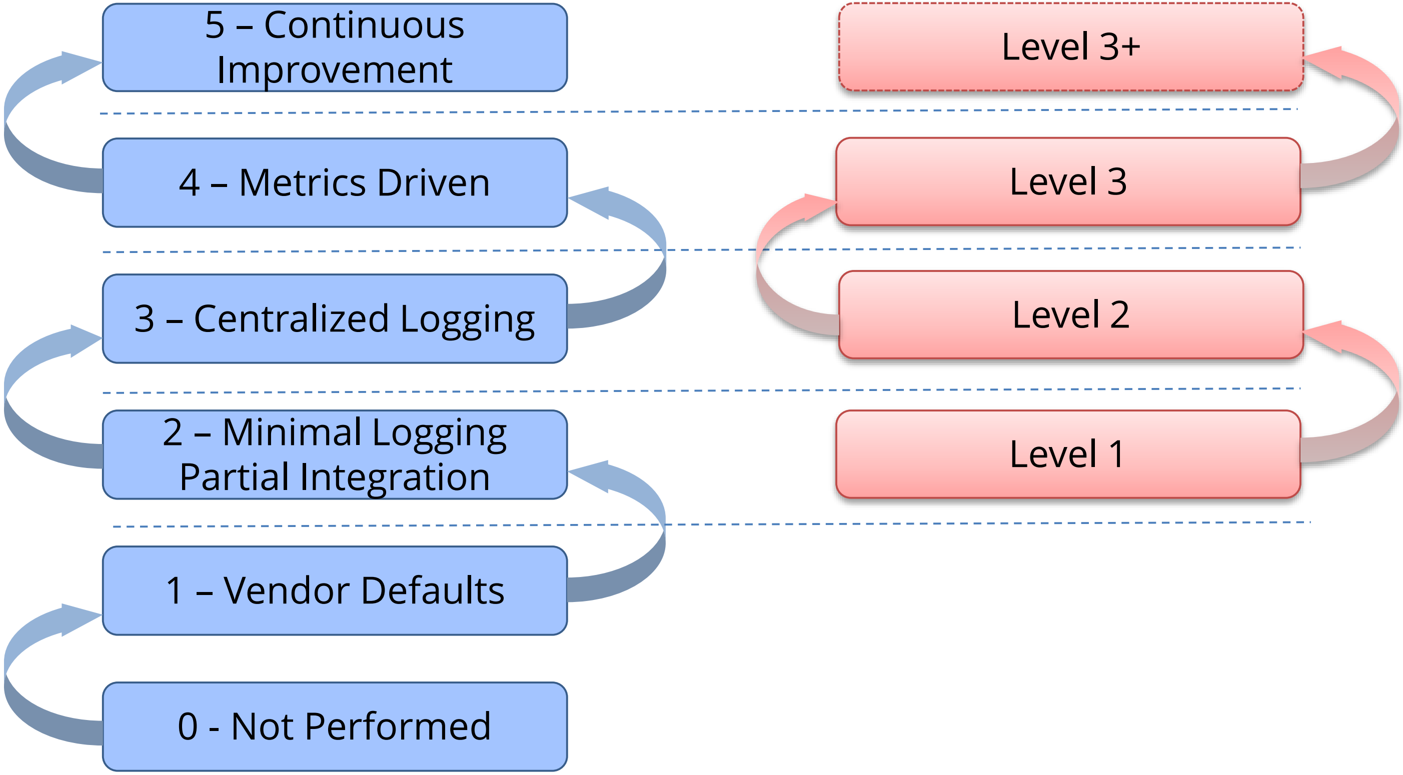
Foundation Security Events Mapping

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

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) such as the **Oracle Audit Vault**
Level 3	Extend logging to include **functional logging** and more complex alerting and monitoring

Logging Maturity Model



5 – Continuous Improvement

4 – Metrics Driven

3 – Centralized Logging

2 – Minimal Logging Partial Integration

1 – Vendor Defaults

0 - Not Performed

Level 3+

Level 3

Level 2

Level 1

Common Maturity Model (CMM)

Integrigy Framework

Integrigy Framework – Level 1

Objectives

- Enhance or start **baseline auditing and logging**
- Enhance or implement base security monitoring and auditing alerts
- Using standard database and EBS functionality

Tasks

1. **Database logging**
   - Enable AUDIT_SYS_OPERATIONS
   - Enable Standard auditing
2. **E-Business Suite logging**
   - Set Sign-on audit to log at the ‘Form’ level
   - Enable Page Access Tracking
   - Enable Audit Trail
3. **Create simple alerts**

Level 1 – Database Logging

- **Enable Standard Audit**
  - Log to sys.aud$
  - Define events
- **Purge per organizational policy**

Object	Oracle Audit Statement	Resulting Audited SQL Statements
Session	session	Database logons and failed logons
Users	user	create user alter user drop user
Roles	role	create role alter role drop role
Database Links **Public Database Links**	database link public database link	create database link drop database link create public database link drop public database link
System	alter system	alter system
Database	alter database	alter database
Grants (system privileges and roles)	system grant	grant revoke
Profiles	profile	create profile alter profile drop profile
SYSDBA and SYSOPER	sysdba sysoper	All SQL executed with sysdba and sysoper privileges

Note: table is not complete – see whitepaper for full table

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

Integrigy Framework – Level 2

Objectives

- Integrate Oracle Database and Oracle EBS with **Oracle Audit Vault** for protection and alerting
- Use Oracle Database Syslog auditing functionality
- Protect EBS logon and navigation activity

Tasks

1. **Implement Oracle Audit Vault**
   - Implement before Oracle Database Firewall
2. **Redirect database logs to Audit Vault**
   - Use either DB or OS collection agent
3. **Log and protect EBS audit data with Audit Vault**
4. **Transition level alerts and monitoring to logging solution**

Secure End-User Navigation Logs

Table	Description
APPLSYS.FND_USERS	This is the base table defining all users and their associated email address and links to HR records
APPLSYS.FND_LOGINS	Sign-On Audit table
APPLSYS.FND_LOGIN_RESPONSIBILITIES	Sign-On Audit table
APPLSYS.FND_LOGIN_RESP_FORMS	Sign-On Audit table
APPLSYS.FND_UNSUCCESSFUL_LOGINS	Unsuccessful logins via the Personal Home Page (Self Service/Web Interface) are stored in both the FND_UNSUCCESSFUL_LOGINS and ICX_FAILURES tables.
ICX.ICX_FAILURES	The ICX_FAILURES table contains more information than the FND_UNSUCCESSFUL_LOGINS. Failed logins to the Professional Interface (Forms) are only logged to the FND_UNSUCCESSFUL_LOGINS tables.
JTF.JTF_PF_SES_ACTIVITY	Page Access Tracking Table
JTF.JTF_PF_ANON_ACTIVITY	Page Access Tracking Table
JTF.JTF_PF_REPOSITORY	Page Access Tracking Table
JTF.JTF_PF_LOGICAL_FLOWS	Page Access Tracking Table
APPLSYS.WF_USER_ROLE_ASSIGNMENTS	Need for E-Business end-user entitlements and role assignments
APPLSYS.FND_USER_RESP_GROUPS	Need for E-Business end-user entitlements and role assignments

Framework:
E1, E2 & E3

Built alerts and report to monitor these tables

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

Integrigy Framework – Level 3

Objectives

- Extend logging to include **functional logging** and more complex alerting and monitoring
- Automate routine compliance activities
- Enhance and extend for continuous monitoring

Tasks

1. **Pass database logs and application server logs**
   - Use correlation to identify multi-layer incidents
2. **Extend to include EBS functional setups**
   - Focus on automating compliance activities
3. **Enhance and extend alerting, monitoring, and reporting for continuous monitoring**
   - Integrate people, processes, and technology

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

Level 3 is Continuous

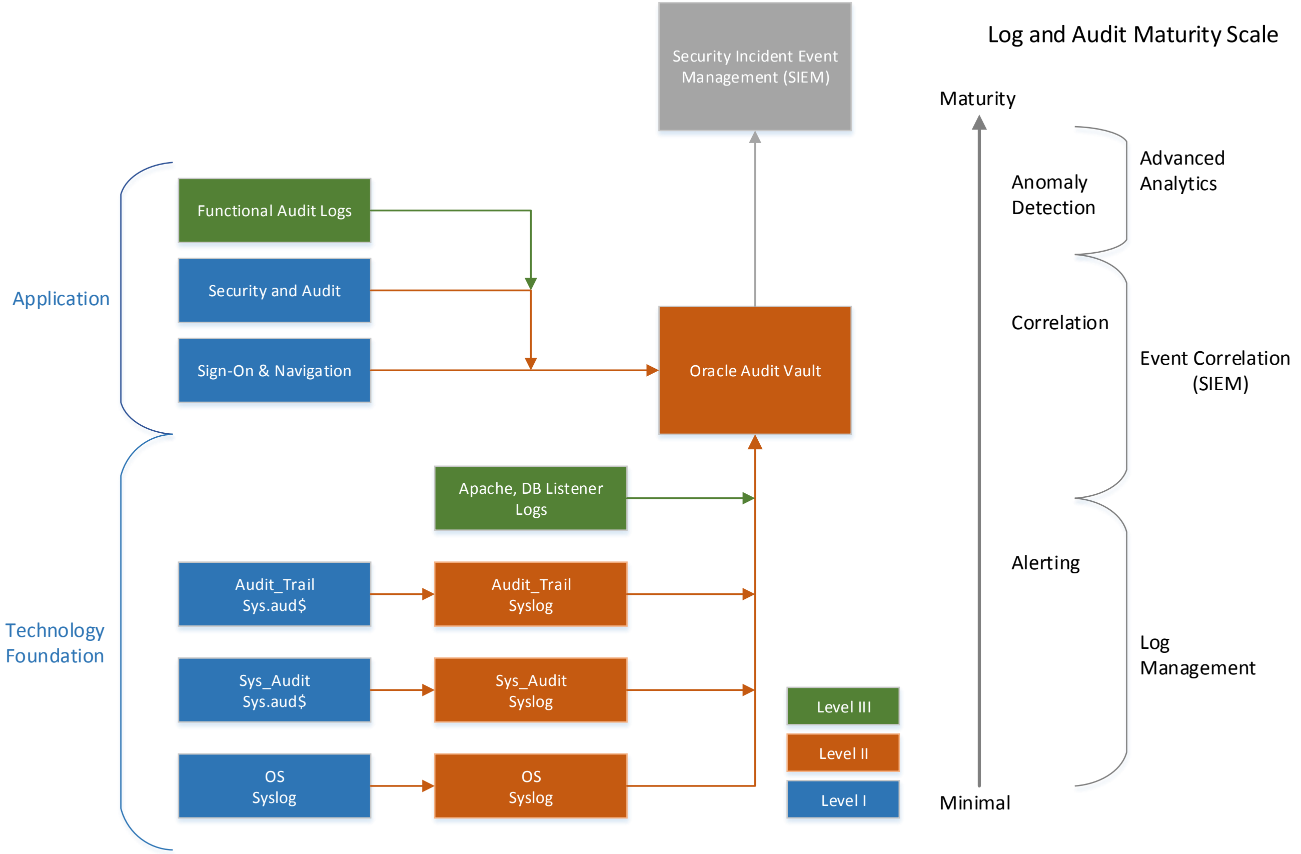
- **Continuous process**
  - Baseline expected activity
  - Define correlations
  - Build alerts and reports
  - Look for anomalies

- **Continuous audit and operations monitoring**
  - Automated compliance

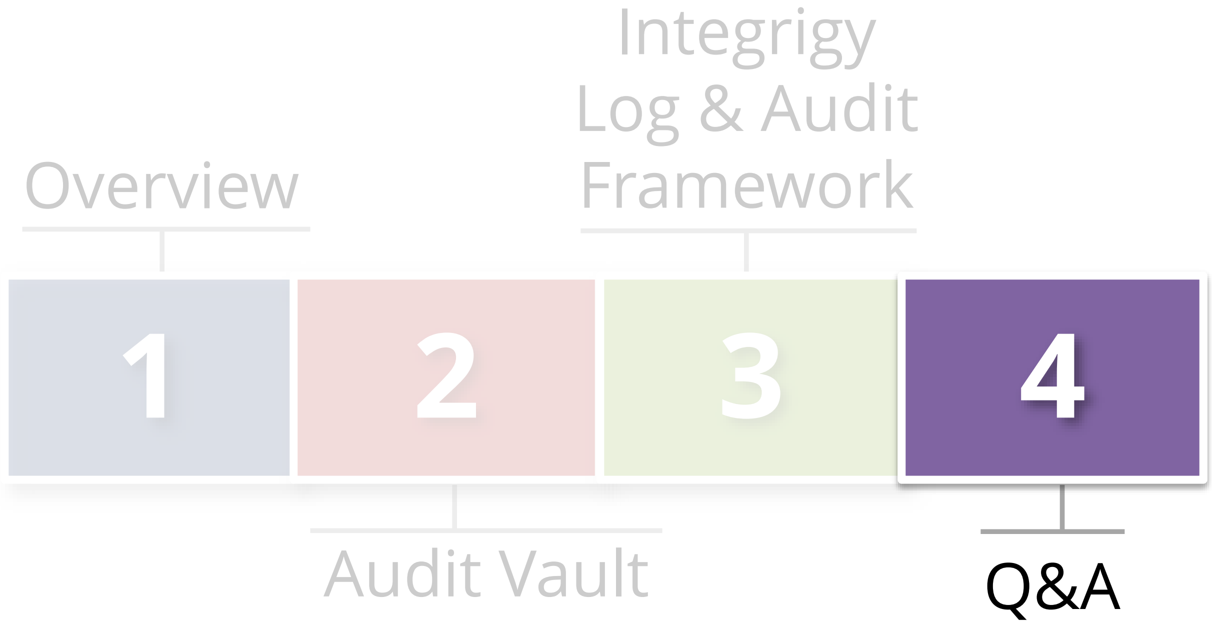
Oracle Client Identifier

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)')

Integrigy Framework for Database Auditing



Agenda



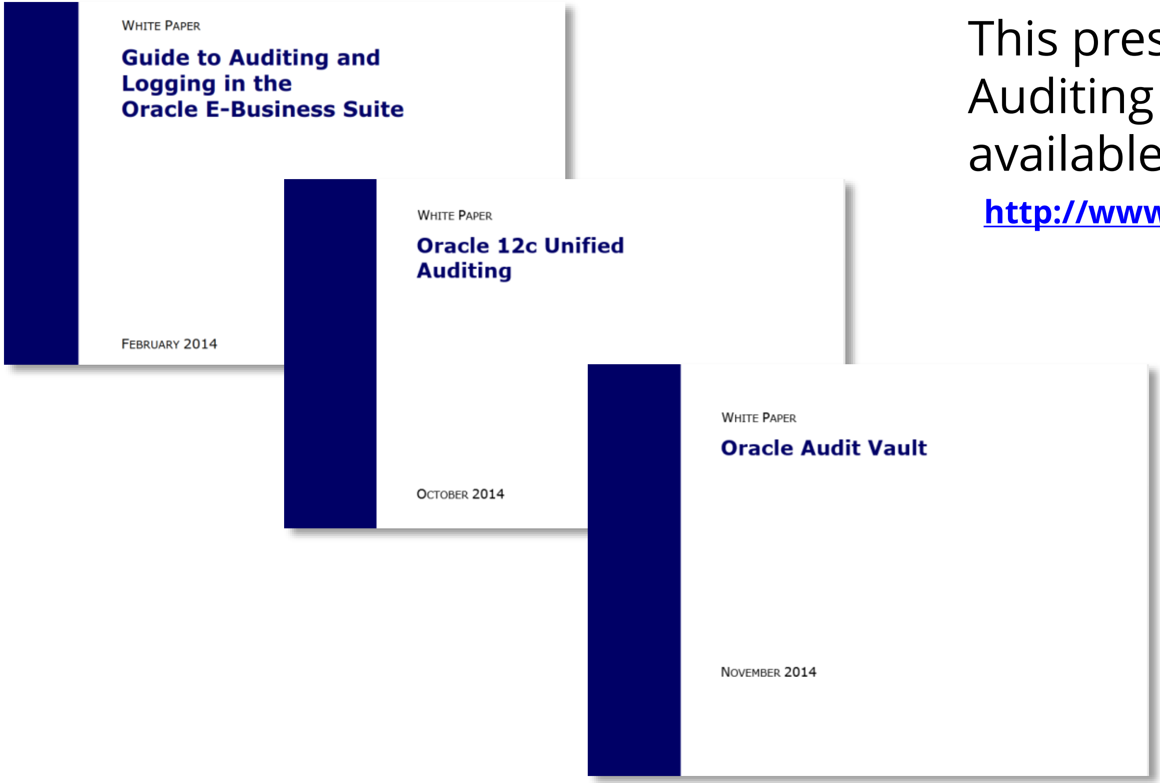
1 Overview

2 Audit Vault

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

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**