Agenda

1. Overview
2. Oracle Auditing
3. Integrigy Log & Audit Framework
4. Q&A
About Integrigy

Products

**AppSentry**
ERP Application and Database Security Auditing Tool

**AppDefend**
Enterprise Application Firewall for the Oracle E-Business Suite

Services

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

**Compliance Assistance**
SOX, PCI, HIPAA

**Security Design Services**
Auditing, Encryption, DMZ

Integrigy protects and validates Oracle E-Business Suite ERP Applications and databases.
Databases: Oracle, SQL Server, MySQL.
Agenda

1. Overview
2. Integrigy Log & Audit Framework
3. Oracle Auditing
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

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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
- DB Access Management Definition
- Implement Access Solution
- Access Controls/Policies
- Access Profiling
- Configuration Standard Auditing

### Access
- DAM Definition and Architecture
- DAM Selection and Implement
- Implement Configuration Std
- Baseline Database Auditing
- Key Application Auditing
- Database IDS
- Log Monitoring Integration

### Auditing
- Periodic Vulnerability Scans
- Implement Configuration Std
- Periodic Vulnerability Scans
- Data Encryption Process

### Monitoring
- 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

<table>
<thead>
<tr>
<th>Done Wrong</th>
<th>Done Right</th>
</tr>
</thead>
<tbody>
<tr>
<td>System performance impacted</td>
<td>No impact or system overhead</td>
</tr>
<tr>
<td>Too much or too little information</td>
<td>Generates actionable information</td>
</tr>
<tr>
<td>Ignored</td>
<td>Used</td>
</tr>
</tbody>
</table>

“If your database is a symphony orchestra, auditing done right will allow you to hear the kettle drums playing off key.”
Pre-Oracle 12c Database Auditing

Type of auditing and logging
1. Listener
   - LOGGING_name = ON

2. DB Alert Log
   - BG_DUMP_DEST dir

3. SYS Auditing
   - AUDIT_SYS_OPERATIONS

4. Standard Auditing
   - AUDIT_TRAIL

5. Fine Grained Auditing
   - DBMS_FGA.add_policy

Audit and logging parameters
- AUDIT_SYSLOG_LEVEL
- AUDIT_FILE_DEST
- AUDIT_TRAIL
- DB
- FGA_LOG$ table
- AUDIT_FILE_DEST dir
- AUD$ table
- AUDIT_FILE_DEST dir
- Syslog
- BG_DUMP_DEST dir
- TNS_ADMIN/log dir
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

<table>
<thead>
<tr>
<th>Other Oracle Logs</th>
<th>Outside Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Application Security (RAS)*</td>
<td>Operating System</td>
</tr>
<tr>
<td>Oracle Label Security (OLA)</td>
<td>Network</td>
</tr>
<tr>
<td>Oracle Data Pump</td>
<td>Load Balancer</td>
</tr>
<tr>
<td>Database Vault (DV)</td>
<td>Storage</td>
</tr>
<tr>
<td>Oracle RMAN</td>
<td>Backup Tools</td>
</tr>
<tr>
<td>SQL*Loader Direct Load</td>
<td>Application</td>
</tr>
</tbody>
</table>

*Oracle 12c only
Database Auditing Effort by Task

Effort

- Monitoring, Alerting, Reporting, Reviewing: 80%
- Archiving & Purging: 10%
- Enable: 5%
- Design: 5%

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

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.

<table>
<thead>
<tr>
<th>Event</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1</td>
<td>Login</td>
</tr>
<tr>
<td>E2</td>
<td>Logoff</td>
</tr>
<tr>
<td>E3</td>
<td>Unsuccessful login</td>
</tr>
<tr>
<td>E4</td>
<td>Modify auth mechanisms</td>
</tr>
<tr>
<td>E5</td>
<td>Create user account</td>
</tr>
<tr>
<td>E6</td>
<td>Modify user account</td>
</tr>
<tr>
<td>E7</td>
<td>Create role</td>
</tr>
<tr>
<td>E8</td>
<td>Modify role</td>
</tr>
<tr>
<td>E9</td>
<td>Grant/revoke user privileges</td>
</tr>
<tr>
<td>E10</td>
<td>Grant/revoke role privileges</td>
</tr>
<tr>
<td>E11</td>
<td>Privileged commands</td>
</tr>
<tr>
<td>E12</td>
<td>Modify audit and logging</td>
</tr>
<tr>
<td>E13</td>
<td>Create, Modify or Delete object</td>
</tr>
<tr>
<td>E14</td>
<td>Modify configuration settings</td>
</tr>
<tr>
<td>Security Events and Actions</td>
<td>PCI DSS 10.2</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>E1 - Login</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E2 - Logoff</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E3 - Unsuccessful login</td>
<td>10.2.4</td>
</tr>
<tr>
<td>E4 - Modify authentication mechanisms</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E5 – Create user account</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E6 - Modify user account</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E7 - Create role</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E8 - Modify role</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E9 - Grant/revoke user privileges</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E10 - Grant/revoke role privileges</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E11 - Privileged commands</td>
<td>10.2.2</td>
</tr>
<tr>
<td>E12 - Modify audit and logging</td>
<td>10.2.6</td>
</tr>
<tr>
<td>E13 - Objects Create/Modify/Delete</td>
<td>10.2.7</td>
</tr>
<tr>
<td>E14 - Modify configuration settings</td>
<td>10.2.2</td>
</tr>
</tbody>
</table>
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
<table>
<thead>
<tr>
<th>Level 1</th>
<th>Enable <strong>baseline auditing and logging</strong> for application/database and implement security monitoring and auditing alerts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 2</td>
<td>Send audit and log data to a <strong>centralized logging</strong> solution outside the Database and Application such as the <strong>Oracle Audit Vault</strong></td>
</tr>
<tr>
<td>Level 3</td>
<td>Extend logging to include <strong>FGA &amp; functional logging</strong> and more complex alerting and monitoring. Protect sensitive data.</td>
</tr>
</tbody>
</table>
Logging Maturity Model

0 - Not Performed
1 - Vendor Defaults
2 - Minimal Logging Partial Integration
3 - Centralized Logging
4 - Metrics Driven
5 - Continuous Improvement

Level 1
Level 2
Level 3
Level 3+

Common Maturity Model (CMM)  Integrigy Framework
## Level 1 – Recommended Alerts

<table>
<thead>
<tr>
<th>Framework</th>
<th>What to Monitor For</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1</td>
<td>Direct database logins (successful or unsuccessful) to EBS schema database accounts</td>
</tr>
<tr>
<td>E1, E11</td>
<td>User SYSADMIN successful logins</td>
</tr>
<tr>
<td>E1, E11</td>
<td>Generic seeded application account logins</td>
</tr>
<tr>
<td>E1, E11</td>
<td>Unlocking of generic seeded application accounts</td>
</tr>
<tr>
<td>E1, E2</td>
<td>Login/Logoff</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Framework</th>
<th>What to Monitor For</th>
</tr>
</thead>
<tbody>
<tr>
<td>E3</td>
<td>User SYSADMIN - unsuccessful login attempts</td>
</tr>
<tr>
<td>E4</td>
<td>Modify authentication configurations to database</td>
</tr>
<tr>
<td>E4</td>
<td>Modify authentication configurations to Oracle E-Business Suite</td>
</tr>
<tr>
<td>E6</td>
<td>New database accounts created</td>
</tr>
<tr>
<td>E9, E10, E12, E13, E14</td>
<td>Updates to AOL tables under AuditTrail</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Framework</th>
<th>What to Monitor For</th>
</tr>
</thead>
<tbody>
<tr>
<td>E12</td>
<td>Turning Sign-On Audit off</td>
</tr>
<tr>
<td>E12</td>
<td>Turning off AuditTrail</td>
</tr>
<tr>
<td>E12</td>
<td>Turning Page Access Tracking off</td>
</tr>
<tr>
<td>E12</td>
<td>Turning Audit Trail off</td>
</tr>
<tr>
<td>E12</td>
<td>Turning audit sys operations off</td>
</tr>
</tbody>
</table>
## Level 2 – Recommended Alerts

<table>
<thead>
<tr>
<th>Framework</th>
<th>What to Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>E1</strong></td>
<td>Successful or unsuccessful login attempts to E-Business without network or system login</td>
</tr>
<tr>
<td><strong>E1</strong></td>
<td>Successful or unsuccessful logins of named database user without network or system login</td>
</tr>
<tr>
<td><strong>E3</strong></td>
<td>Horizontal unsuccessful application attempts – more than 5 users more than 5 times within the hour</td>
</tr>
<tr>
<td><strong>E3</strong></td>
<td>Horizontal unsuccessful direct database attempts – more than 5 users more than 5 times within the hour</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Framework</th>
<th>What to Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>E9</strong></td>
<td>End-users granted System Administration Responsibility</td>
</tr>
<tr>
<td><strong>E9</strong></td>
<td>Addition or removal of privileges granted to user SYSADMIN</td>
</tr>
<tr>
<td><strong>N/A</strong></td>
<td>Monitor for database attacks</td>
</tr>
</tbody>
</table>
# Level 3 – Recommended Alerts

<table>
<thead>
<tr>
<th>Framework</th>
<th>What to Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1</td>
<td>Key functional setup and configuration activity</td>
</tr>
<tr>
<td>E1</td>
<td>SYSADMIN usage pattern</td>
</tr>
<tr>
<td>E6, E11</td>
<td>E-Business Suite Proxy user grants</td>
</tr>
<tr>
<td>E5, E11</td>
<td>Database account creation and privilege changes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Framework</th>
<th>What to Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>E13, E14</td>
<td>Reconcile creation and updates to Forms, Menus, Responsibilities, System Profiles and Concurrent Programs</td>
</tr>
<tr>
<td>E6</td>
<td>FND User email account changes</td>
</tr>
<tr>
<td>E14</td>
<td>Tables listed in APPLSYS.FND_AUDIT_TABLES</td>
</tr>
</tbody>
</table>
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
<table>
<thead>
<tr>
<th>Application</th>
<th>Example of how used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle E-Business Suite</td>
<td>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)</td>
</tr>
<tr>
<td>PeopleSoft</td>
<td>Starting with PeopleTools 8.50, the PSOPRID is now additionally set in the Oracle database CLIENT_IDENTIFIER attribute.</td>
</tr>
<tr>
<td>SAP</td>
<td>With SAP version 7.10 above, the SAP user name is stored in the CLIENT_IDENTIFIER.</td>
</tr>
<tr>
<td>Oracle Business Intelligence Enterprise Edition (OBIEE)</td>
<td>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)')</td>
</tr>
</tbody>
</table>
Overview

1. Oracle Auditing

2. Integrigy Log & Audit Framework

3. Oracle Auditing

4. Q&A
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