There are a variety of commercial security tools available to audit Oracle® databases. However, there are instances when their application is not practical:

• The cost may be prohibitive for smaller companies.
• Larger holding companies or geographically dispersed companies may not have full network connectivity between the centre and its subsidiaries.
• Consultancies performing external reviews may not be given permission to install or run tools that require full database administrator (DBA) privileges and, hence, the administrator password. Furthermore, the audited entity has no oversight of what the tool does or what effect it is likely to have on mission-critical databases.

One approach is to audit Oracle databases using computer-assisted audit techniques (CAATs) in conjunction with information taken directly from the Oracle database.

**ORACLE DATABASES**

Oracle databases contain metadata or data about data. This is contained in the data dictionary and database views.

The data dictionary provides information about every object in the database, including Oracle database users, their privileges, roles and auditing information.

The contents of the data dictionary can be queried through Oracle database views. These views display the underlying table data in a useful manner. Some views are accessible to all database users, whereas others are restricted to DBAs. These views (prefixed with ‘DBA_’) show all relevant information in the database, including the information stored in the data dictionary. A full list of DBA views, along with more detailed explanations, may be found in the Oracle Database Reference.

The Oracle database also maintains dynamic performance views. As their name suggests, they are continuously updated with performance information while a database is open and in use. Dynamic views are named beginning with ‘V$’. Again, a full list of V$ views, along with explanations, may be found in the Oracle database reference.

SQL*Plus is a query tool included in every Oracle database installation. It enables one to query the database using Structured Query Language (SQL), formatting the output as desired and writing the results to file (if required).

**OUTPUTTING ORACLE DATABASE VIEWS**

Using the formatting and configuration options in figure 1, Oracle query output, including those from views, can be directed to comma-separated values (CSV) text file(s).

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPOOL</td>
<td>SPOOL outputs query results to a file in a given location. SPOOL OFF stops the output.</td>
</tr>
<tr>
<td>SET LINES</td>
<td>Specifies the total number of characters that display on one line before beginning a new line</td>
</tr>
<tr>
<td>SET TRIMSPOOL ON</td>
<td>Removes trailing blanks at the end of each spooled line</td>
</tr>
<tr>
<td>SET PAGESIZE</td>
<td>Specifies the number of lines on each page of output. Headings will appear only once for each ‘page’.</td>
</tr>
<tr>
<td>SET TIMING OFF</td>
<td>Prevents timing information being output</td>
</tr>
<tr>
<td>SET ECHO OFF</td>
<td>Prevents output of commands in a script</td>
</tr>
<tr>
<td>SET FEEDBACK OFF</td>
<td>Prevents feedback messages (e.g., number of records returned by a query)</td>
</tr>
<tr>
<td>SET COLSEP</td>
<td>Sets the column separator character printed between columns in output. To generate a CSV type file, this will normally be a comma (‘,’). However, if the output contains a comma, this should be changed to a different character that does not appear in the output (e.g., ‘</td>
</tr>
<tr>
<td>SET UNDERLINE OFF</td>
<td>Prevents the column headings from being underlined</td>
</tr>
<tr>
<td>SET NEWPAGE</td>
<td>If set to zero, skips zero lines at the start of a page</td>
</tr>
</tbody>
</table>

Ian Cooke, CISA, CGEIT, COBIT-F, CFE, CPTS, DipFM, ITIL-F, Six Sigma Green Belt, is an IT audit manager based in Dublin, Ireland, with more than 25 years of experience in all aspects of information systems. Cooke is the topic leader for Oracle databases, SQL Server Databases and OS/400 in the ISACA Knowledge Center, and a member of ISACA’s Communities Committee. He welcomes comments or suggestions at ian.j.cooke@gmail.com or on the Oracle Database topic (www.isaca.org/Groups/Professional-English/oracle-database/Pages/Overview.aspx) in the ISACA Knowledge Center.
**Figure 2** gives an idea of what a script would look like (a full Oracle script can be downloaded from the ISACA® Knowledge Center). Once generated, these scripts can be handed over to the DBA to be run over the required database(s). One CSV file will be produced for each view.

```sql
SET LINES 10000
SET TRIMSPOOL ON
SET PAGESIZE 10000
SET TIMING OFF
SET ECHO OFF
SET FEEDBACK OFF
SET COLSEP ‘,’
SET UNDERLINE OFF
SET NEWPAGE 0

-- Get a list of profiles on the system
SPOOL dba_profiles.txt
SELECT * FROM dba_profiles;
SPOOL OFF

-- Get a list of all users on the database
SPOOL dba_users.txt
SELECT * FROM dba_users;
SPOOL OFF

-- Parameter file contains commas
SET COLSEP “!”

-- Get a list of parameters
SPOOL v$parameter.txt
SELECT * FROM v$parameter;
SPOOL OFF
```

**ANALYSING ORACLE DATABASE VIEWS**

These files can then be imported into CAATs tools, such as the following, for analysis and comparison.

**DBA_PROFILES**

The entity being audited should have a policy on how its passwords are configured. In Oracle databases, password configurations are reflected in the database profile (DBA_PROFILES) view. A profile is a named set of resource limits and password parameters that restricts database usage and instance resources for a user. That is, a given profile is attached to a user account, controlling, for example, the number of failed login attempts, password lifetime or password reuse for that user.

As noted previously, this view can be output to a CSV file (see **figure 2**). A sample output from the DBA_PROFILES CSV file can be seen in **figure 3**, in which the first line shows the Oracle field names. These field names relate to the defined layout for the DBA_PROFILES view (**figure 4**). The layout for this view and all Oracle database views is available in the Oracle Database Reference.

**Figure 3—DBA_PROFILES Sample Output**

<table>
<thead>
<tr>
<th>PROFILE</th>
<th>RESOURCE_NAME</th>
<th>RESOURCE_LIMIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFAULT</td>
<td>COMPOSITE_LIMIT</td>
<td>KERNEL,UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>SESSIONS_PER_USER</td>
<td>KERNEL,UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>CPU_PER_SESSION</td>
<td>KERNEL,UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>CPU_PER_CALL</td>
<td>KERNEL,UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>LOGICAL_READS_PER_SESSION</td>
<td>KERNEL,UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>IDLE_TIME</td>
<td>KERNEL,UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>CONNECT_TIME</td>
<td>KERNEL,UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>PRIVATE_SGA</td>
<td>KERNEL,UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>FAILED_LOGIN_ATTEMPTS</td>
<td>PASSWORD,5</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>PASSWORD_LIFE_TIME</td>
<td>PASSWORD,UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>PASSWORD_REUSE_TIME</td>
<td>PASSWORD,UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>PASSWORD_REUSE_MAX</td>
<td>PASSWORD,UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>PASSWORD_VERIFY_FUNCTION</td>
<td>PASSWORD,NULL</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>PASSWORD_LOCK_TIME</td>
<td>PASSWORD,UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>PASSWORD_GRACE_TIME</td>
<td>PASSWORD,UNLIMITED</td>
</tr>
</tbody>
</table>

**Figure 4—Fields in the DBA_PROFILES View**

<table>
<thead>
<tr>
<th>Column</th>
<th>Data Type</th>
<th>Null</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROFILE</td>
<td>VARCHAR2(30)</td>
<td>NOT NULL</td>
<td>Profile name</td>
</tr>
<tr>
<td>RESOURCE_NAME</td>
<td>VARCHAR2(32)</td>
<td>NOT NULL</td>
<td>Resource name</td>
</tr>
<tr>
<td>RESOURCE_TYPE</td>
<td>VARCHAR2(8)</td>
<td></td>
<td>Indicates whether the resource profile is a KERNEL or a PASSWORD parameter</td>
</tr>
<tr>
<td>LIMIT</td>
<td>VARCHAR2(40)</td>
<td></td>
<td>Indicates the limit placed on this resource for this profile</td>
</tr>
</tbody>
</table>

All common CAATs tools (and, indeed, Microsoft Excel and Microsoft Access) allow for importing CSV files. Once the DBA_PROFILES have been imported into the CAATs tool, they can be analysed for compliance to the entity’s standards. These standards could be based upon ISACA’s Oracle Audit/Assurance Program and ICQ, the Defense Information System Agency’s Security Technical Implementation Guide, the Center for Internet Security benchmarks, or a document developed by the entity.
The key concept is that once the entity has one database analysed and knows it to be compliant to relevant standards, it can use that as a master profile, configuring its CAATs tool to compare the profiles of interest across all of its Oracle databases. This can be done by joining on the fields profile and resource (or simply on resource), displaying all records where the limit is not equal. For example, the failed login attempts may differ across a sample of databases. In this manner, the entity can quickly flag noncompliant profiles for follow-up and review.

If required, the entity can also periodically repeat reviews of the Oracle profiles. This would allow it to track changes and could be used as part of a continuous monitoring audit programme.

**V$PARAMETER**

The entity being audited should also have a policy on how its Oracle databases are configured. Much of this configuration is reflected in Oracle initialisation parameters, which can be retrieved from the V$PARAMETER view. Examples of parameters include those for enabling the auditing of operations issued by privileged users, such as DBAs, or whether case-sensitive passwords are required.

There are approximately 260 Oracle initialisation parameters and a full list may be found in the *Oracle Database Reference*. However, a key concept of this approach is that not all the parameters of interest for all databases need to be reviewed. Again, once one database is known to be compliant to the standards, it can be used as a master in the CAATs tool to compare the parameters of interest across all of the databases. This can be done by joining on the field name (from the V$PARAMETER layout) and displaying all records where the value is not equal. As above, in this manner noncompliant configurations can be quickly flagged for follow up and review.

**DBA_USERS**

DBA_USERS describes all users of the Oracle database. This includes username, account status and, in Oracle databases up to and including 10.2.0.5, the password hash. The password is up to 30-characters long with all characters converted to uppercase before the hashing is performed. Furthermore there is no real “salt”—the algorithm simply uses the username. This means that the username password combinations sys/temp1 and system/p1 have the same password hash. Furthermore, a username installed with the same password on different Oracle databases will have the same password hash. This is often the case when the default value is accepted during database installation. Default passwords pose a real and common risk to Oracle database installations.

The threat is so common that a list of default Oracle password hashes is maintained online. This is maintained in various formats, including CSV and Excel, that can be imported easily into the CAATs tool. This list of default password hashes can then be compared against DBA_USERS (joining on the field password) across all of the entity’s databases—anywhere the password hashes match indicates the use of a default password. These should be reviewed immediately. DBA_USERS can also be compared to other sources of information, for example, the entity’s payroll to flag leavers and movers. (Note: From Oracle 11g, the new view DBA_USERS_WITH_DEFPWD displays all users who are still using their default passwords.)

**Default passwords pose a real and common risk to Oracle database installations**

**Other Views**

As there are hundreds of Oracle views, it is not possible to discuss them all in this article. Those mentioned are for illustrative purposes. The view(s) used depends on the purpose of the audit, but could also include:

- Any of the views described in ISACA’s Oracle Audit/Assurance Program and ICO
- DBA_ROLES, which lists all the roles that have been defined in the database. It could be reviewed to ensure that the roles are appropriate and password-protected, where applicable.
- DBA_ROLE_PRIVS, which identifies the roles granted to users or other roles. This could be reviewed to ensure that the role privileges granted to users are appropriate and under the principle of least privilege.
- DBA_SYS_PRIVS, which lists all systems privileges granted to users or roles. This could be reviewed to ensure that the system privileges granted to users are appropriate and under the principle of least privilege.
- DBA_TAB_PRIVS, which lists all table privileges granted to users or roles. This could be reviewed to ensure that the table privileges granted to users are appropriate and under the principle of least privilege.
DBA_OBJ_AUDIT_OPTS, which lists the auditing options on all objects. This could be reviewed to ensure that the auditing enabled is appropriate for the sensitivity of the data in the database.

DBA_PRIV_AUDIT_OPTS, which captures granting of system privileges. This could be reviewed to ensure that system privileges are only granted to appropriate users under the principle of least privilege.

DBA_STMT_AUDIT_OPTS, which captures issued statements. This could be reviewed to ensure that statements were issued by appropriate users and under the principle of least privilege.

DBA_DB_LINKS, which lists information about connections to other databases. This could be reviewed to ensure that connections to other databases are private and granted under the principle of least privilege.

V$VERSION, which lists version and status information for component Oracle products. This could be reviewed to ensure that the current version installed is fully supported.

V$LICENSE, which lists database licence information. This could be reviewed to ensure that the audited entity is in compliance with all Oracle licensing requirements.

A full list of Oracle views along with more detailed explanations may be found in the Oracle Database Reference. However, the key point is that any of the views may be output to CSV files and imported into a CAATs tool. These may then be:

- Compared to other Oracle databases, including a master that is known to be compliant to the standards
- Compared to development, test or quality assurance versions of the production database (useful for change control)
- Compared to other sources of data. This can include data from internal or external entities.

CONCLUSION
CAATs are a valuable tool for auditing Oracle databases. With the proposed CAATs, there are little or no set-up costs, because frequently the organisation is already using CAATs software. Furthermore, the approach allows external consultants and geographically dispersed companies to request that queries be run by the local DBA without the need to compromise the administrator password. The DBA of the audited entity can also review the SQL being run over the database to ensure that it will have no effect on the production environment.

Once the queries are run, they can be securely emailed or otherwise transferred for analysis. Query results can be compared against known compliant databases to highlight areas of audit concern. Query results can also be compared against preproduction databases and other sources of data, such as the company payroll. Finally, the entire process can be repeated and used as part of a continuous monitoring and/or audit.

ENDNOTES

2 Oracle, Oracle Database Reference 11g Release 2 (11.2), http://docs.oracle.com/cd/E11882_01/server.112/e25515.pdf
3 ISACA, Knowledge Center, www.isaca.org/Groups/Professional-English/oracle-database/GroupDocuments/Oracle.SQL
4 Op cit, Oracle, p. 17-3
8 Op cit, Oracle, p. 1-4
9 Op cit, Oracle, p. 8-52
12 Op cit, Oracle, p. 5-49
13 Op cit, ISACA, 2009
14 Op cit, Oracle