***Information regarding the scripts***

**i) Database script:**

EY consultants from around the world contributed to an Oracle 10g script that will interrogate the tables on the database using SELECT (read) statements. Only one script exists for both Windows and Unix/Linux operating systems. Thescript will write information to many text files, which may become quite large, so please request the database administrator (DBA) to zip them for you. You may then copy/extract the files to the specified directory (**C:\TextResults**) on your laptop before importing them into the Oracle Reporting Tool (see below). Please read the accompanying Oracle for Unix/Linux “Howto and legal requirements”-document of the script for detailed instructions.

**ii) Operating system script:**

The script was developed for an Oracle 10g environment in order to obtain information, not contained in the database itself. Versions are available for Windows and Unix/Linux operating systems. TheUnix/Linuxscript will create a tarball, called **EY\_<machine\_name>.tar**, while the Windows script will create several text files, called **WIN<item>.txt**. You may then extract the tarball to the C:\TextResults directory on your laptop. The Oracle Reporting Tool (see below) will import these files along with the database audit script results. Please read the accompanying Oracle for Unix/Linux “Howto and legal requirements”-document of the script for detailed instructions.

***Disclaimer when executing the Operating System and/or Database scripts:***A DBA from the client needs to execute these scripts using a user ID with the DBA\_ROLE allocated. You should never execute scripts or any statements on the client’s production, development or test environments.

Provide the script to the client via email and attach either the following disclaimer or your territories’ official “Hold Harmless letter/contract”:

It is the client’s responsibility to perform the following steps prior to execution of the script in the production environment:

1. Scrutinize the contents of the script to ensure that it does not contain any statements, commands or any other code that might negatively influence their environment(s) in either a security or operational way.
2. Test the script on the test environment to ensure that it does not contain any statements, commands or any other code that might negatively influence their environment(s) in either a security or operational way.
3. The final responsibility for executing this script lies with the client.
4. It is advised to execute the script during off-peak hours.
5. The client must remove all copies of the script as it is the property of Ernst & Young LLP. The client may retain the script results.

***Information regarding the Oracle Reporting Tool (ORT)***

The Microsoft Access-based front-end, provides an option to import the script result text files from C:\TextResults. You will be presented with a collection of menus that links to reports, which can be used to perform the reviews stated in the work program. Generally more information is provided than is required to perform the review, due to the fact that in certain circumstances more complex reviews needs to be performed by senior consultants and then this information are available.

Once both the Operating System, and Database audit script results have been copied/extracted to C:\TextResults, you may open a blank copy of the ORT, and select the “Import Script Results” option from the main menu.

After the import process has completed, you may select the Reports Menu, which will present you with the following sub-menus:

* General/System Related Reports
* Auditing Options Related Reports
* User Privileges Related Reports 1
* User Privileges Related Reports 2
* Unix crontabs
* Unix other
* Windows information -- ignore this menu for an Oracle for Unix/Linux review

All menu items will be discussed further down in this document, and references are made to the relevant reports in the work program.

The work program can be linked to the following script text results and to the Oracle Reporting Tool:

|  |  |
| --- | --- |
| **Text Result** | **Report Name** |
| DBPARMS  DBTRIG  oracle\_home\_dbs.tar | DB Parameters  DB Triggers  OS init<SID>.ora file |
| DBSYSAU | Auditing Options per User |
| DBPRVAD | Privileges Audited per User |
| DBSYSAU | Auditing Options per User |
| DBPRVAD | Privileges Audited per User |
| DBSYSAU  DBTRIG | Auditing Options per User  DB Triggers |
| DBSYSAU  DBTRIG | Auditing Options per User  DB Triggers |
| DBAUDPRV | DB Users with Audit privileges |
| DBPARMS | DB Parameters |
| OScron\*  OSvar\_spool\_cron | All reports under the Unix Crontabs menu |
| DBLOGFL | DB Redo Log Files |
| OScron\*  OSvar\_spool\_cron | All reports under the Unix Crontabs menu |
| DBCNTRF | DB Control Files |
| DBLOGFL  DBDATAF  DBPARMS  OSoracle\_file\_permissions | OS Oracle directory file permissions |
| OSoracle\_file\_permissions  OScron\*  OSvar\_spool\_cron | OS Oracle directory file permissions  All reports under the Unix Crontabs menu |
| N/A | N/A |
| DBDBLNK | DB Links (Trust relationships) |
| N/A | N/A |
| DBUDATA  DBUSROL  OSetc\_passwd  OSetc\_group | DB Active Users  DB User Role  OS etc\_passwd (OS user list)  OS etc\_group (OS groups and members) |
| DBUDATA | DB Active Users |
| N/A | N/A |
| DBUDATA (+standing data) | DB Default password results |
| DBRTPRIV  DBUDATA  DBUSROL  DBTABLP | DB User Table Privileges  DB Active Users  DB User Role  DB Table Privilege |
| DBTABLO  DBTABLE | DB Table Owners  DB User Tablespace |
| DBUDATA  OSps\_ef | DB Active Users  OS ps -ef (Process listing) |
| DBPROFI  DBPARMS  oracle\_home\_dbs.tar | DB User Profile  DB Parameters  OS init<SID>.ora file |
| DBPARMS  oracle\_home\_dbs.tar  OSetc\_passwd | DB Parameters  OS init<SID>.ora file  OS etc\_passwd (OS user list) |
| DBPUBTP | DB Public Table Grant |
| DBUDATA | DB Active Users |
| OSlistener\_file | OS Oracle listener file(s) |
| OSopatch | OS Installed Oracle patches |