**Auditing Database Activities**

**TASK:**

This project requires you to implement some security measures to protect your database. The scenario is as follows:

After intensive investigation, you found out that two (2) users (VPD\_CLERK1 and DBSEC\_CLERK) were abusing their privileges. Everyone else on their profile have no problems. You decided to implement a solution to prevent the two (2) users from creating any tables or other database objects and from updating CUSTOMER table. You are also going to monitor the activities by the two (2) users. Specifically, you need to:

1. To be safe, drop trigger named "trigger\_before\_change" at the beginning of your script.

2. Create a trigger named "trigger\_before\_change." (The period is not part of the trigger name.) The trigger will not allow the two (2) users, VPD\_CLERK1 and DBSEC\_CLERK, to change in CUSTOMER table such as insert, update, and delete. Exact spelling on the trigger name is required.

3. Raise an error message whenever the above two (2) users attempt to change records in CUSTOMER table. The message will read "You do not have the privilege to insert, update, or delete on CUSTOMER table. Please contact your manager for more details."

4. Revoke CREATE TABLE privilege from users VPD\_CLERK1 and DBSEC\_CLERK.

5. Use Oracle built-in audit function to set up the audit for the two (2) users' activities including CREATE and change in CUSTOMER table.

6. To be safe, connect to DBSEC account to grant insert, update, and delete privilege on CUSTOMER table to VPD\_CLERK1 and DBSEC\_CLERK.

7. Use one statement of your choice to test your trigger on each user on changing in CUSTOMER table. For example, each user can try to insert a new record.

8. Test the create table privilege for both VPD\_CLERK1 and DBSEC\_CLERK.

9. Show the audit results of the above attempts including operating system user name, database user name, date and action name.

10. Perform all the above functions in one SQL script file.