Implementing Data Integrity and Security (10%)

This assignment relates to the following Course Learning Requirements:

CLR 2 - Administer a DBMS using knowledge of SQL, database security features, globalization and database architecture (storage, memory and processes)

CLR 3 - Manage database system security and privacy controls

CLR 6 - Build database systems that directly support internationalization and globalization

CLR 7 - Explore and gain practical experience in current advanced database technology

Objectives of the Assignment

You will draft a procedure that adds SQL Server tables, restricts access to those tables, checks the tables data integrity, and monitors those tables using a database audit.

Requirements

This Assignment is designed to use ORACLE. Review the links below before starting this work.

- Creating ORACLE Virtual Private Database Policies -- https://docs.oracle.com/database/121/DBSEG/vpd.htm#DBSEG278
- Setting up Oracle's auditing features - Auditing CDB and PDB level in Oracle Multitenant (managescript.com)

1. **Create a new table – ASSIGNMENT1**. Includes steps to create this table.

a. The table has one column - COLUMNA and 100 rows.

```
SQL> CREATE TABLE ASSIGNMENT1 (
  2       COLUMNA VARCHAR(50)
  3  );

Table created.
```

b. Create a script to insert rows into ASSIGNMENT1 table. There needs to be several rows which have a text string beginning with the letter ‘A’, several rows beginning with the letter ‘M’ and several rows beginning with the letter ‘Z’.

SQL Plus

```
SQL> -- Insert rows beginning with 'A'
SQL>
SQL> INSERT INTO ASSIGNMENT1 (COLUMNA) VALUES ('Apple');

1 row created.

SQL> INSERT INTO ASSIGNMENT1 (COLUMNA) VALUES ('Airplane');

1 row created.

SQL> INSERT INTO ASSIGNMENT1 (COLUMNA) VALUES ('Ample');

1 row created.

SQL> INSERT INTO ASSIGNMENT1 (COLUMNA) VALUES ('Ape');

1 row created.

SQL> INSERT INTO ASSIGNMENT1 (COLUMNA) VALUES ('Apetizer');

1 row created.
```

SQL Plus

```
SQL> -- Insert rows beginning with 'M'
SQL>
SQL> INSERT INTO ASSIGNMENT1 (COLUMNA) VALUES ('Mango');

1 row created.

SQL> INSERT INTO ASSIGNMENT1 (COLUMNA) VALUES ('Monkey');

1 row created.

SQL> INSERT INTO ASSIGNMENT1 (COLUMNA) VALUES ('Monk');

1 row created.

SQL> INSERT INTO ASSIGNMENT1 (COLUMNA) VALUES ('Monker');

1 row created.

SQL> INSERT INTO ASSIGNMENT1 (COLUMNA) VALUES ('My');

1 row created.
```

SQL Plus

```
SQL> -- Insert rows beginning with 'Z'
SQL>
SQL> INSERT INTO ASSIGNMENT1 (COLUMNA) VALUES ('Zebra');

1 row created.

SQL> INSERT INTO ASSIGNMENT1 (COLUMNA) VALUES ('Zoo');

1 row created.

SQL> INSERT INTO ASSIGNMENT1 (COLUMNA) VALUES ('Zoology');

1 row created.

SQL> INSERT INTO ASSIGNMENT1 (COLUMNA) VALUES ('Zem');

1 row created.

SQL> INSERT INTO ASSIGNMENT1 (COLUMNA) VALUES ('Zooes');

1 row created.

SQL> -- Add more rows starting with 'A' until you have a total of 33 rows
SQL> -- Add more rows starting with 'M' until you have a total of 33 rows
SQL> -- Add more rows starting with 'Z' until you have a total of 34 rows
```

c. Provides a ‘select * from ASSIGNMENT1’ showing the contents of your new table

SELECT * FROM ASSIGNMENT1

2. **Create three new users**: USERA, USERB, USERC
   a. Include a screen shot of the scripts used to create this user.

SQL Plus

```
SQL> create user c##userA identified by 1234;

User created.

SQL> create user c##userB identified by 1234;

User created.

SQL> create user c##userC identified by 1234;

User created.

SQL>
```

3. **Create five roles**. RL_READONLY, RL_TBLACCESS, RL_ROWA_READ, RL_ROWM_READ and RL_ROWZ_READ.
   a. Include a screen shot of the scripts used to create these roles.
   b. When creating each role, give each ROLE their correct privileges. For example, RL_READONLY should only be granted the ‘select’ privilege on ASSIGNMENT1.

SQL Plus

```
Connected.
SQL> -- Create role RL_READONLY
SQL> CREATE ROLE c##RL_READONLY not identified;

Role created.

SQL> -- Grant 'SELECT' privilege on ASSIGNMENT1 to RL_READONLY
SQL> GRANT SELECT ON ASSIGNMENT1 TO c##RL_READONLY;

Grant succeeded.

SQL> -- Create role RL_TBLACCESS
SQL> CREATE ROLE c##RL_TBLACCESS not identified;

Role created.

SQL> -- Grant 'SELECT', 'INSERT', 'UPDATE', and 'DELETE' privileges on ASSIGNMENT1 to RL_TBLACCESS
SQL> GRANT SELECT, INSERT, UPDATE, DELETE ON ASSIGNMENT1 TO c##RL_TBLACCESS;

Grant succeeded.

SQL> -- Create role RL_ROWA_READ
SQL> CREATE ROLE c##RL_ROWA_READ not identified;

Role created.

SQL> -- Grant 'SELECT' privilege on ASSIGNMENT1 to RL_ROWA_READ
SQL> GRANT SELECT ON ASSIGNMENT1 TO c##RL_ROWA_READ;

Grant succeeded.

SQL> -- Create role RL_ROWM_READ
SQL> CREATE ROLE c##RL_ROWM_READ not identified;

Role created.

SQL> -- Grant 'SELECT' privilege on ASSIGNMENT1 to RL_ROWM_READ
SQL> GRANT SELECT ON ASSIGNMENT1 TO c##RL_ROWM_READ;

Grant succeeded.

SQL> -- Create role RL_ROWZ_READ
SQL> CREATE ROLE c##RL_ROWZ_READ;

Role created.

SQL> -- Grant 'SELECT' privilege on ASSIGNMENT1 to RL_ROWZ_READ
SQL> GRANT SELECT ON ASSIGNMENT1 TO c##RL_ROWZ_READ;

Grant succeeded.
```

4. **Create the security access rules** for your new table (at **both** the ***table level*** and the ***row level*** access) -- **DO NOT** use views to implement this. This link will provide details on to set up the 'security policies' for row-level access -- https://docs.oracle.com/database/121/DBSEG/vpd.htm#DBSEG007

   Read through the details related to using Oracle's row level security options chose the one you feel supports the following business requirement. Be sure to indicate the 'choice' you have made (e.g., VPD, Label security or Data Redaction) -- Note, if you feel you need to 'alter' your table – ASSIGNMENT1 feel free to do so.

   a. Provide each of the three new users with the appropriate privileges that allow the following access:
      i. Read-only access to ASSIGNMENT1
      ii. USERA can only see rows in ASSIGNMENT1 which have values in **columnA** which begin with 'A'
      iii. USERB can only see rows in ASSIGNMENT1 which have values in **columnA** which begin with 'M'
      iv. USERC can only see rows in ASSIGNMENT1 which have values in **columnA** which begin with 'Z'

Step 1: Create Policy Functions

SQL Plus

```
Connected to:
Oracle Database 21c Express Edition Release 21.0.0.0.0 - Production
Version 21.3.0.0.0

SQL> conn / as sysdba
Connected.
SQL> --Connected as sysdba
SQL>
SQL> -- Create the policy function for USERA
SQL> CREATE OR REPLACE FUNCTION policy_function_usera (
  2    schema IN VARCHAR2,
  3    table_name IN VARCHAR2
  4  ) RETURN VARCHAR2 AS
  5  BEGIN
  6    RETURN 'SUBSTR(columnA, 1, 1) = ''A''';
  7  END;
  8  /

Function created.

SQL> -- Create the policy function for USERB
SQL> CREATE OR REPLACE FUNCTION policy_function_userb (
  2    schema IN VARCHAR2,
  3    table_name IN VARCHAR2
  4  ) RETURN VARCHAR2 AS
  5  BEGIN
  6    RETURN 'SUBSTR(columnA, 1, 1) = ''M''';
  7  END;
  8  /

Function created.

SQL> -- Create the policy function for USERC
SQL> CREATE OR REPLACE FUNCTION policy_function_userc (
  2    schema IN VARCHAR2,
  3    table_name IN VARCHAR2
  4  ) RETURN VARCHAR2 AS
  5  BEGIN
  6    RETURN 'SUBSTR(columnA, 1, 1) = ''Z''';
  7  END;
  8  /

Function created.
```

Step 2: Create Security Policies:

1. **Create Security Policy for USERA (C##USERA):**

```
SQL> -- Create the security policy for USERA
SQL> BEGIN
  2    DBMS_RLS.ADD_POLICY(
  3      object_schema => 'C##CST',
  4      object_name => 'ASSIGNMENT1',
  5      policy_name => 'policy_usera',
  6      policy_function => 'policy_function_usera',
  7      statement_types => 'SELECT');
  8  END;
  9  /
```

2. Create Security Policy for USERB (C##USERB):

```
SQL> -- Create the security policy for USERB
SQL> BEGIN
  2    DBMS_RLS.ADD_POLICY(
  3      object_schema => 'C##CST',
  4      object_name => 'ASSIGNMENT1',
  5      policy_name => 'policy_userb',
  6      policy_function => 'policy_function_userb',
  7      statement_types => 'SELECT');
  8  END;
  9  /
```

3. Create Security Policy for USERC (C##USERC):

```
SQL> -- Create the security policy for USERC
SQL> BEGIN
  2    DBMS_RLS.ADD_POLICY(
  3      object_schema => 'C##CST',
  4      object_name => 'ASSIGNMENT1',
  5      policy_name => 'policy_userc',
  6      policy_function => 'policy_function_userc',
  7      statement_types => 'SELECT');
  8  END;
  9  /
```

5. **Setup Database Audit**. Includes the steps to setup the database audit in Oracle (refer to link in the resource section above).
    a. Use scripts to implement the audit. DO NOT use the menu options.
    b. You will test to make sure changes are being added to the log.
    c. Create a new table with one or two columns
    d. Insert five rows into the table.
    e. Delete one row from the table.
    f. Update one row.
    g. Select one row.
    h. Use a different row for each of the statements (e, f and g)
    i. Query the log showing the transactions and screenshot/paste the audio log

Select SQL Plus

```
SQL> conn sys as sysdba
Enter password:
Connected.
SQL> AUDIT INSERT, DELETE, UPDATE, SELECT ON sys.ASSIGNMENT1;

Audit succeeded.

SQL> CREATE TABLE sys.audit_test(
  2  id NUMBER,
  3      description VARCHAR2(50)
  4  );

Table created.

SQL>
SQL> -- Insert rows
SQL> INSERT INTO sys.audit_test VALUES (1, 'Row 1');

1 row created.

SQL> INSERT INTO sys.audit_test VALUES (2, 'Row 2');

1 row created.

SQL> INSERT INTO sys.audit_test VALUES (3, 'Row 3');

1 row created.

SQL> INSERT INTO sys.audit_test VALUES (4, 'Row 4');

1 row created.

SQL> INSERT INTO sys.audit_test VALUES (5, 'Row 5');

1 row created.
```

```
Select SQL Plus
SQL>
SQL> -- Delete a row
SQL> DELETE FROM sys.audit_test WHERE id = 3;

1 row deleted.

SQL>
SQL> -- Update a row
SQL> UPDATE sys.audit_test SET description = 'Updated Row 2' WHERE id = 2;

1 row updated.

SQL>
SQL> -- Select a row
SQL> SELECT * FROM sys.audit_test WHERE id = 1;

        ID DESCRIPTION
---------- --------------------------------------------------
         1 Row 1

SQL> SELECT OS_USERNAME, USERNAME, OBJ_NAME, ACTION_NAME, SQL_TEXT, TIMESTAMP
  2  FROM DBA_AUDIT_TRAIL
  3  WHERE OBJ_NAME = 'ASSIGNMENT1'
  4  ORDER BY TIMESTAMP DESC;

no rows selected
```

Submission Requirements

To submit this assignment, submit your file as a ***WORD File***, using the assignment upload tool in Brightspace. To access this, navigate to the Activities/Assignments link in the left-hand sidebar, and select Assignment 3 - Implementing Data Integrity and Security.