

Stephen Dornu Dugbarte
Edmonton, Alberta – Canada | +1 (825) 777-0501 | ddstephen07@gmail.com

Project: Database Access Control Audit

1.0 Executive Summary

Every modern organisation segregates duties performed by roles within a defined process. Segregation of duties ensures accountability and reporting that promotes good corporate governance. The duties performed by each role are predefined with assigned authority and access privileges. Continuous monitoring and audit are required to keep the assigned authority in check and the privileges within allowed limits.

Objective:

The objective of this project is to:

- Define customer loan data classifications based on their level of impact to breach
- Identify the existence of a defined user access rights to select, update or delete over the customer loan database
- Determine the functioning of existing controls inline to defined user rights
- Recommend controls based on NIST Cybersecurity Framework 2.0

It is expected that most of the Personally Identifiable Information (PII) of the customers which form this database should be relatively permanent and highly confidential. Any user requires appropriate access and the required permission to update or delete with supporting documents.

Scope:

- 62 loan customers were used for this project.
- The focus of users is limited to their rights to access, update and delete data on the loan customer database

Expected Results

After auditing the loan customer list database, its is expected that the:

- Users restricted from selecting, updating or deleting data on the loan customer database will not be able to do so

2.0 Background

Information Classification:

The customer data on the loan database is classified as Internal, Confidential, or Highly Confidential.

The classification of customer data on the loan database is defined by the level of risk the data can be exposed to. The risks were also defined by two impact criteria - **reputation loss and financial impact**:

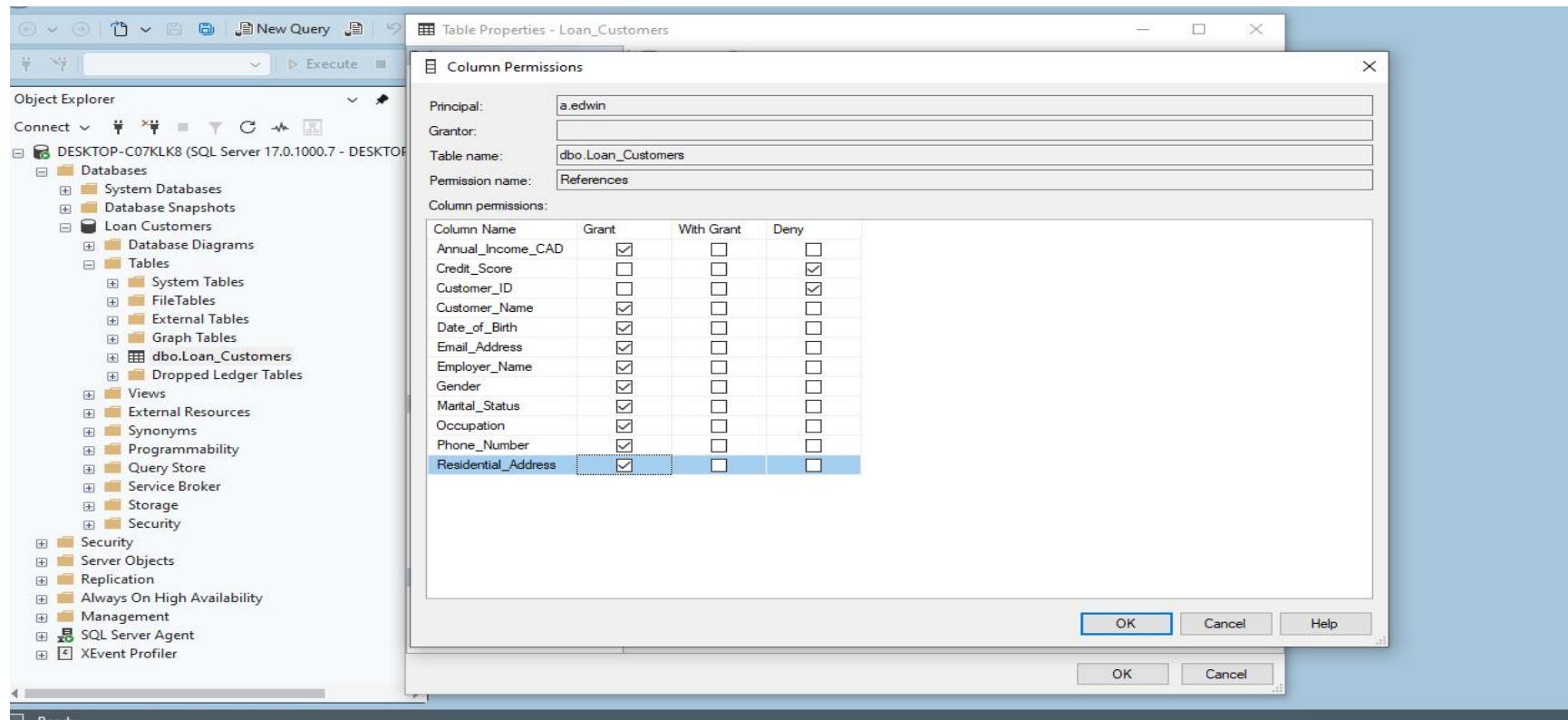
- **Low** - minimal reputation loss and minimal financial impact
- **Medium** - minimal or moderate reputation loss and minimal or moderate financial impact
- **High** - moderate or material reputation loss and moderate or high financial impact

Information Type	Risk Level	Classification	Amendment Permission
Customer ID	Low	Internal	No
Customer name	Medium	Confidential	Yes
Gender	Low	Internal	Yes
Marital Status	Low	Internal	Yes
Residential address	High	Confidential	Yes
Phone number	High	Confidential	Yes
Email address	High	Confidential	Yes
Annual income	Medium	Highly Confidential	Yes
Employer	Medium	Highly Confidential	Yes
Credit score	High	Highly Confidential	No

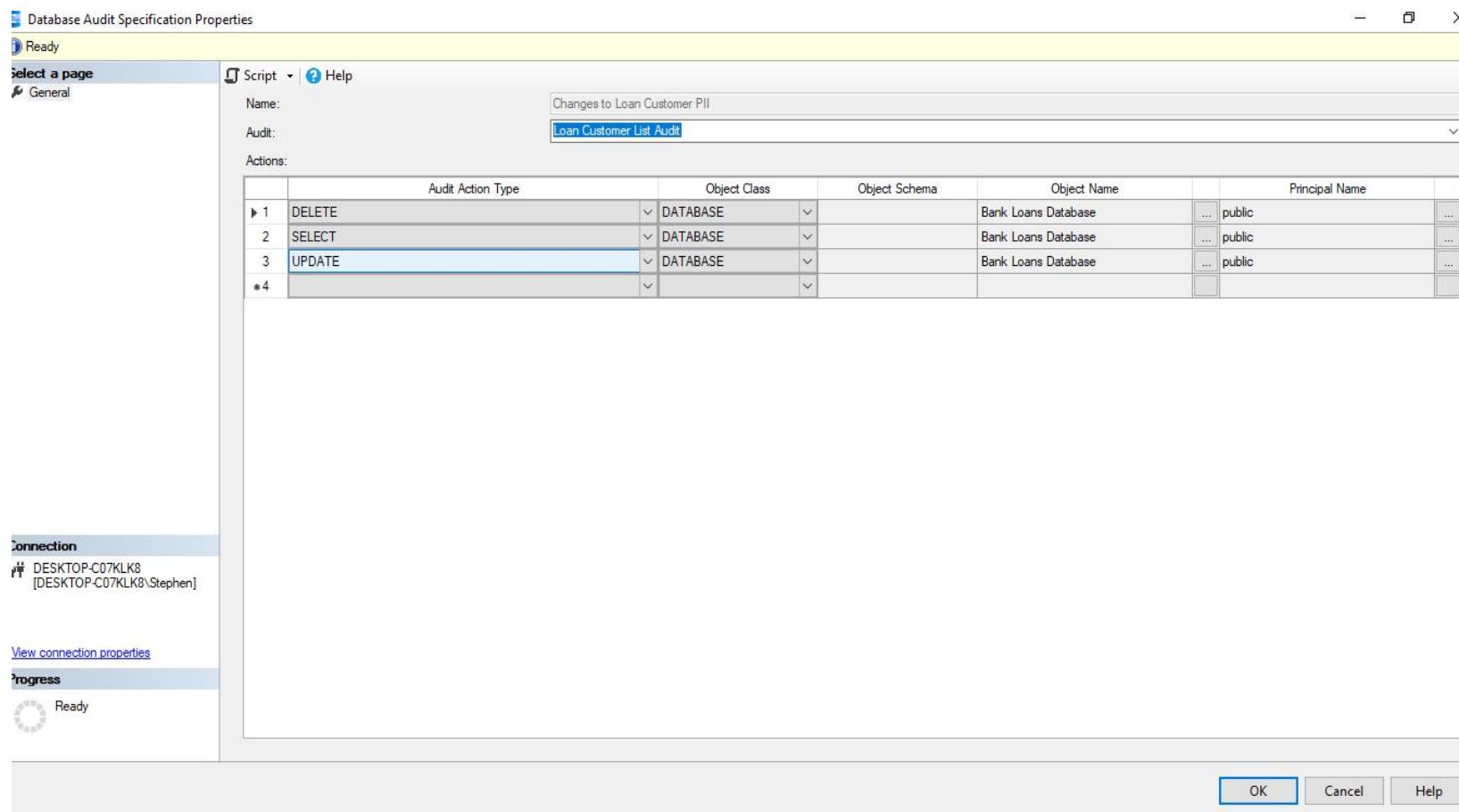
Methodology:

The following methods were deployed:

- Acquired sample datasets relating to 62 bank loan customers with their personal identifiable information (PII). *The PII of the loan includes information relating to their: Customer ID, Customer name, Gender, Marital Status, Residential address, Phone number, Email address, Annual income, Employer, Credit score.*
- The SQL Server Standard Development option was downloaded and installed together with the SQL Server Management Studio (SSMS).
- The **Loan Customer** database was created in SSMS and the bank loan customer list was uploaded.
- An identity and access login was created for **a.edwin** with appropriate permission as an inputer per the loan process cycle. A screenshot is captured below:



- The audit and the server audit specification were created for **a.edwin** over loan customer database with required audit action type in the SSMS. The user is permitted to access the database but not to update or delete



- The user **a.edwin** perform some activities relating to accessing, updating or deleting data on the database on the Loan Customer List

The screenshot shows the SSMS interface with the following details:

- Object Explorer:** Shows the connection to **DESKTOP-C07KLK8 (SQL Server 17.0.1000.7 - a.edwin)** and the **Bank Loans Database**.
- SQLQuery1.s...ephen (51)*:** The current query window contains the following T-SQL code:


```

1 select * from dbo.[Loan Customer List]
2
3 update dbo.[Loan Customer List]
4 set Customer_ID = 1000
5 where Customer_ID = 1001;
6
7 select * from dbo.[Loan Customer List]
8
9 delete from dbo.[Loan Customer List] where Customer_ID = 1000;
10
11 select * from dbo.[Loan Customer List]
12
      
```
- Results Grid:** Displays the data from the **[Loan Customer List]** table. The first eight rows are shown in detail:

	Customer_ID	Customer_Name	Date_of_Birth	Gender	Marital_Status	Residential_Address	Phone_Number	Email_Address	Annual_Income_CAD
1	1002	Robert Sinclair	2002-06-04	Female	Divorced	763 Main St, Laval, QC	747-555-1613	robert.sinclair88@email.com	46456
2	1003	Kevin Park	1990-05-30	Male	Single	329 Main St, Toronto, ON	705-555-3326	kevin.park3@email.com	97982
3	1004	Jean Tremblay	1999-09-11	Female	Divorced	961 Main St, Surrey, BC	710-555-6839	jean.tremblay58@email.com	68207
4	1005	Victor Ivanov	1998-01-02	Male	Single	392 Main St, Red Deer, AB	748-555-1390	victor.ivanov80@email.com	63664
5	1006	Priya Patel	2011-08-18	Male	Divorced	650 Main St, Brampton, ON	454-555-8890	priya.patel87@email.com	99000
6	1007	Grace O'Neill	2018-09-19	Male	Divorced	659 Main St, Montreal, QC	571-555-7072	grace.o'neill73@email.com	68828
7	1008	Lucas Martin	1993-01-03	Female	Single	216 Main St, Laval, QC	406-555-4361	lucas.martin92@email.com	52230
8	1009	Noah Peterson	2012-10-28	Male	Divorced	480 Main St, Laval, QC	518-555-5175	noah.peterson46@email.com	115697

 A second grid below shows the same data with different column headers:

	Customer_ID	Customer_Name	Date_of_Birth	Gender	Marital_Status	Residential_Address	Phone_Number	Email_Address	Annual_Income_CAD	Occupation
1	1002	Robert Sinclair	2002-06-04	Female	Divorced	763 Main St, Laval, QC	747-555-1613	robert.sinclair88@email.com	46456	Operations
- Status Bar:** Shows the message **Query executed successfully.** and other status information like the session ID and row count.
- Ready:** Status bar at the bottom left.

- The activities of the user *a.edwin* was audited over the the “Loan Customers List” to determine appropriate access, update or deletion permissions.

2.0 Audit Outcomes

The user **a.edwin** was able to perform all three actions of **access, update and delete** even though the granted access does not permit the user to either update or delete any customer information on the Loan Customer database.

- The capability of users performing all restricted actions even though there is adequate and detailed audit log records shows weak database access controls and introduces high access risks. The user's ability to update and delete highly confidential and risky data on the database adds extra layer of risks too

The risk exposure should be assessed immediately with appropriate primary or supplementary controls put in place. The NIST Cybersecurity Framework 2.0 was used to recommend controls for the database access control weaknesses.

Action	Action Success	Action Permission	Recommended Controls based on NIST CSF 2.0
Select	Yes	Yes	GV.RM: Risk Management Strategy GV.RR: Roles, Responsibilities and Authorities GV.PO: Policy ID.RA: Risk Assessment ID.IM: Improvement PR.AA: Identity Management, Authentication and Access Control PR.AT: Awareness and Training PR.DS: Data Security PR.PS: Platform Security
Update	Yes	No	
Delete	Yes	No	

Control ID	Control Description	Inherent Risk	Residual Risk	Responsibility	Frequency
GV.RM	Risk Management Strategy	High	Low	Chief Risk Officer	Annually
GV.RR	Roles, Responsibilities and Authorities	High	Low	Human Resource Director	Annually
GV.PO	Policy	Medium	Low	Chief Information Officer	Biennial
ID.RA	Risk Assessment	High	Medium	Chief Risk Officer	Quarterly
ID.IM	Improvement	Medium	Low	Chief Risk Officer	Annually
PR.AA	Identity Management, Authentication and Access Control	High	Medium	IT Manager	Bi-annual
PR.AT	Awareness and Training	Medium	Low	Human Resource Manager	Monthly
PR.DS	Data Security	High	Medium	Chief Information Security Officer	Daily
PR.PS	Platform Security	High	Medium	Chief Information Security Officer	Daily