

Stephen Dornu Dugbarney

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

Project: Database Access Control Audit

1.0 Background

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 determine existence and strength of controls to access, update and deletion of a bank loan customer database by officers of the loan department. 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 and Information Classification:

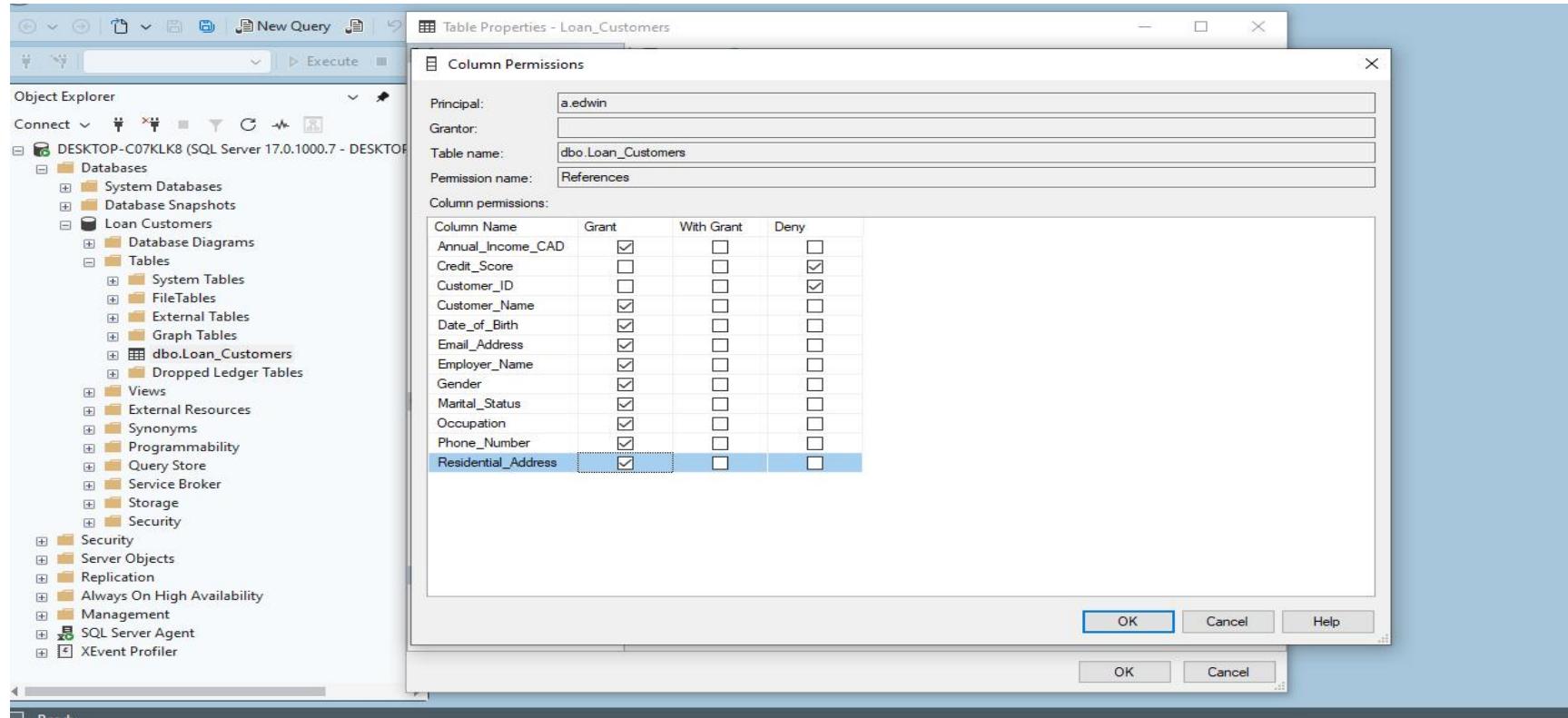
62 loan customers were used for this project. Their information is classified as below. The classification groups are: Internal, Confidential, or Highly Confidential

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

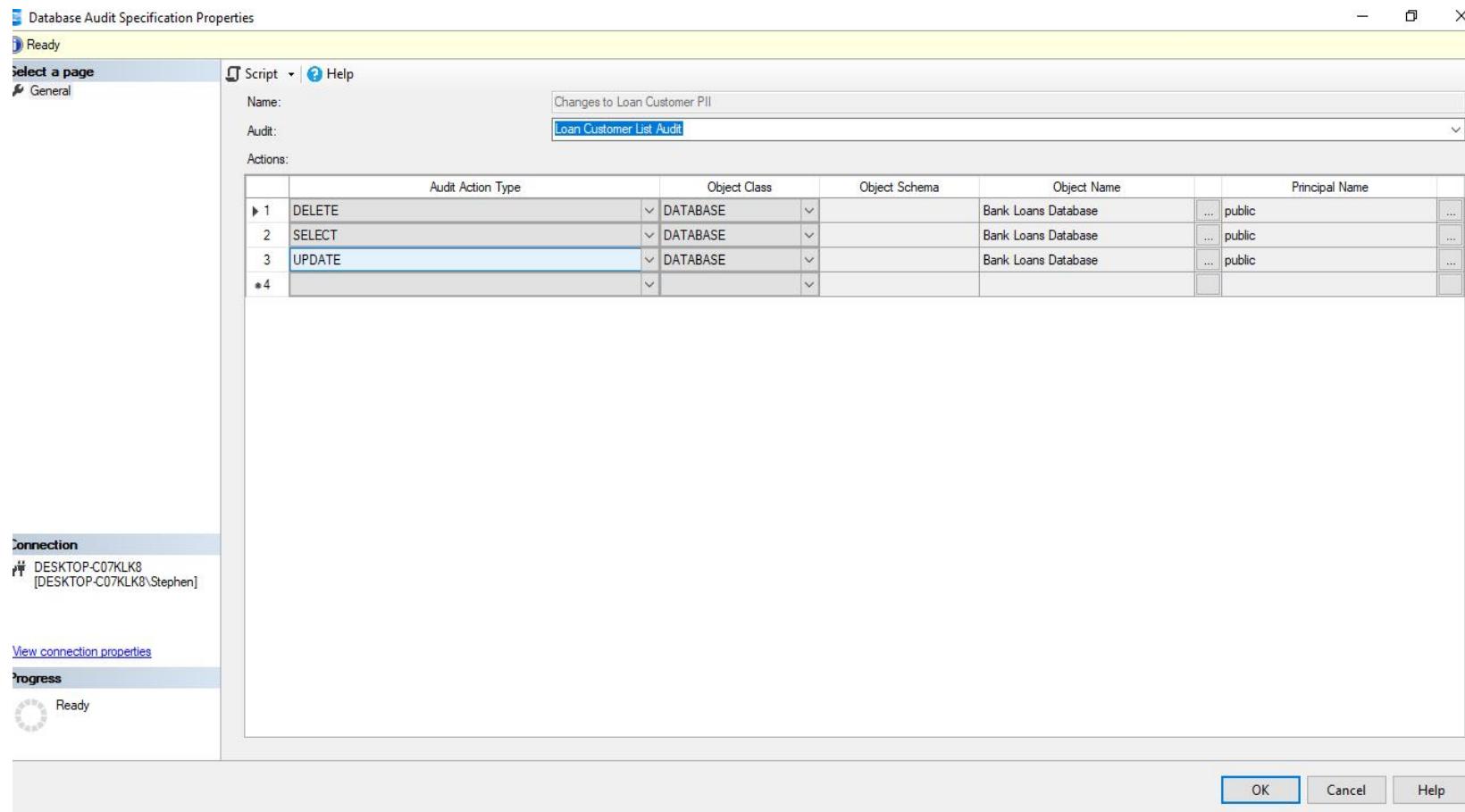
Methodology:

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 the loan customer database with required audit action type in the SSMS



- The user **a.edwin** was allowed to perform some activities on the Loan Customer List

The screenshot shows the SQL Server Management Studio (SSMS) interface. In the Object Explorer, a connection to 'DESKTOP-C07KLK8 (SQL Server 17.0.1000.7 - a.edwin)' is selected. The 'Bank Loans Database' is chosen in the 'New Query' dropdown. The main window displays a query window titled 'SQLQuery1.s...ephen (51)*' containing 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

```

The results pane shows a table with 183 rows of data from the 'Loan Customer List' table. The columns are: Customer_ID, Customer_Name, Date_of_Birth, Gender, Marital_Status, Residential_Address, Phone_Number, Email_Address, and Annual_Income_CAD. The first few rows are:

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

The status bar at the bottom indicates 'Query executed successfully.' and provides system information.

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

Log File Viewer - DESKTOP-C07KLK8

Select logs

Audit Collection
 Loan Customer List Audit

Log file summary: No filter applied

Date	Server Instance Name	Action ID	Class Type	Sequence Number	Succeeded	Permission Bit Mask	Column Permission	Session ID	Server Principal ID	Database
1/3/2026 7:31:05 AM	DESKTOP-C07KLK8	SELECT	TABLE	1	True	0x0001	True	54	259	1
1/3/2026 7:31:05 AM	DESKTOP-C07KLK8	SELECT	TABLE	1	True	0x0001	True	54	259	1
1/3/2026 7:31:05 AM	DESKTOP-C07KLK8	UPDATE	TABLE	1	True	0x0002	True	54	259	1
1/3/2026 7:31:05 AM	DESKTOP-C07KLK8	SELECT	TABLE	1	True	0x0001	True	54	259	1
1/3/2026 7:31:05 AM	DESKTOP-C07KLK8	SELECT	TABLE	1	True	0x0001	True	54	259	1
1/3/2026 7:31:05 AM	DESKTOP-C07KLK8	DELETE	TABLE	1	True	0x0010	False	54	259	1
1/3/2026 7:31:05 AM	DESKTOP-C07KLK8	SELECT	TABLE	1	True	0x0001	True	54	259	1
1/3/2026 7:31:05 AM	DESKTOP-C07KLK8	UPDATE	TABLE	1	True	0x0002	True	54	259	1
1/3/2026 7:30:12 AM	DESKTOP-C07KLK8	SELECT	TABLE	1	True	0x0001	True	54	259	1
1/3/2026 7:30:12 AM	DESKTOP-C07KLK8	SELECT	TABLE	1	True	0x0001	True	54	259	1
1/3/2026 7:30:12 AM	DESKTOP-C07KLK8	SELECT	TABLE	1	True	0x0001	True	54	259	1
1/3/2026 7:30:12 AM	DESKTOP-C07KLK8	SELECT	TABLE	1	True	0x0001	True	54	259	1
1/3/2026 7:30:12 AM	DESKTOP-C07KLK8	SELECT	TABLE	1	True	0x0001	True	54	259	1
1/3/2026 7:30:12 AM	DESKTOP-C07KLK8	DELETE	TABLE	1	True	0x0010	False	54	259	1
1/3/2026 7:30:12 AM	DESKTOP-C07KLK8	SELECT	TABLE	1	True	0x0001	True	54	259	1
1/3/2026 7:29:10 AM	DESKTOP-C07KLK8	SELECT	VIEW	1	True	0x0001	True	91	259	1
1/3/2026 7:29:03 AM	DESKTOP-C07KLK8	SELECT	VIEW	1	True	0x0001	True	91	259	1
1/3/2026 7:29:03 AM	DESKTOP-C07KLK8	SELECT	VIEW	1	True	0x0001	True	91	259	1
1/3/2026 7:29:03 AM	DESKTOP-C07KLK8	SELECT	VIEW	1	True	0x0001	True	91	259	1
1/3/2026 7:29:03 AM	DESKTOP-C07KLK8	SELECT	VIEW	1	True	0x0001	True	91	259	1
1/3/2026 7:23:07 AM	DESKTOP-C07KLK8	SELECT	TABLE	1	True	0x0001	True	54	259	1
1/3/2026 7:23:07 AM	DESKTOP-C07KLK8	SELECT	TABLE	1	True	0x0001	True	54	259	1
1/3/2026 7:23:07 AM	DESKTOP-C07KLK8	DELETE	TABLE	1	True	0x0010	False	54	259	1
1/3/2026 7:23:07 AM	DESKTOP-C07KLK8	SELECT	TABLE	1	True	0x0001	True	54	259	1
1/3/2026 7:22:44 AM	DESKTOP-C07KLK8	SELECT	TABLE	1	True	0x0001	True	54	259	1
1/3/2026 7:22:44 AM	DESKTOP-C07KLK8	DELETE	TABLE	1	True	0x0010	False	54	259	1

Status

Last Refresh:
1/3/2026 12:31:50 AM

Filter: None

View filter settings

Progress

Done (411 records).

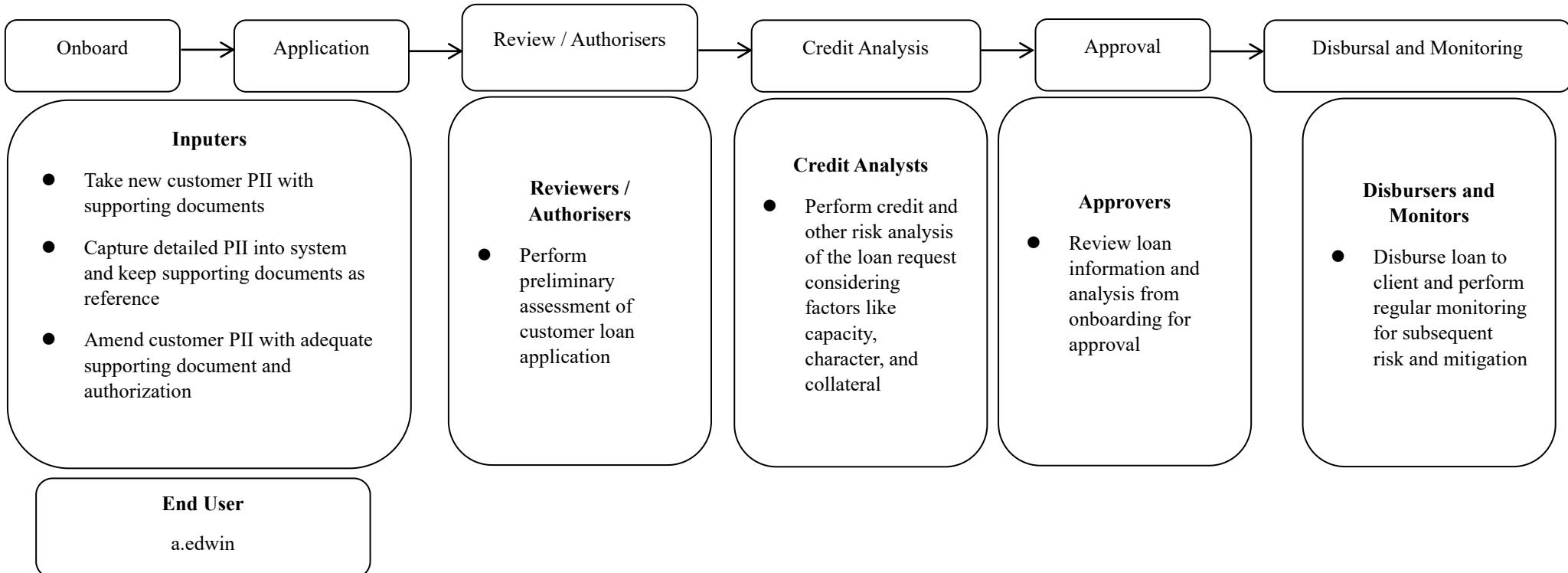
Selected row details:

Date	1/3/2026 7:31:05 AM
Log	Audit Collection (Loan Customer List Audit)
Event Time	07:31:05.9489968
Server Instance Name	DESKTOP-C07KLK8
Action ID	SELECT TABLE

Close

2.0 Loan Process and End Users

The loan process cycle is broken into six (6) stages as illustrated below and supported by the function of five (5) end users.



3.0 Audit Outcomes

The user **a.edwin** was able to perform all three actions 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 risk exposure should be assessed immediately with appropriate primary or supplementary controls put in place.

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
Update	Yes	No	GV.PO: Policy ID.RA: Risk Assessment ID.IM: Improvement
Delete	Yes	No	PR.AA: Identity Management, Authentication and Access Control PR.AT: Awareness and Training PR.DS: Data Security PR.PS: Platform Security