Stephen Dornu Dugbartey
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 Permision
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

2.0 Methodology

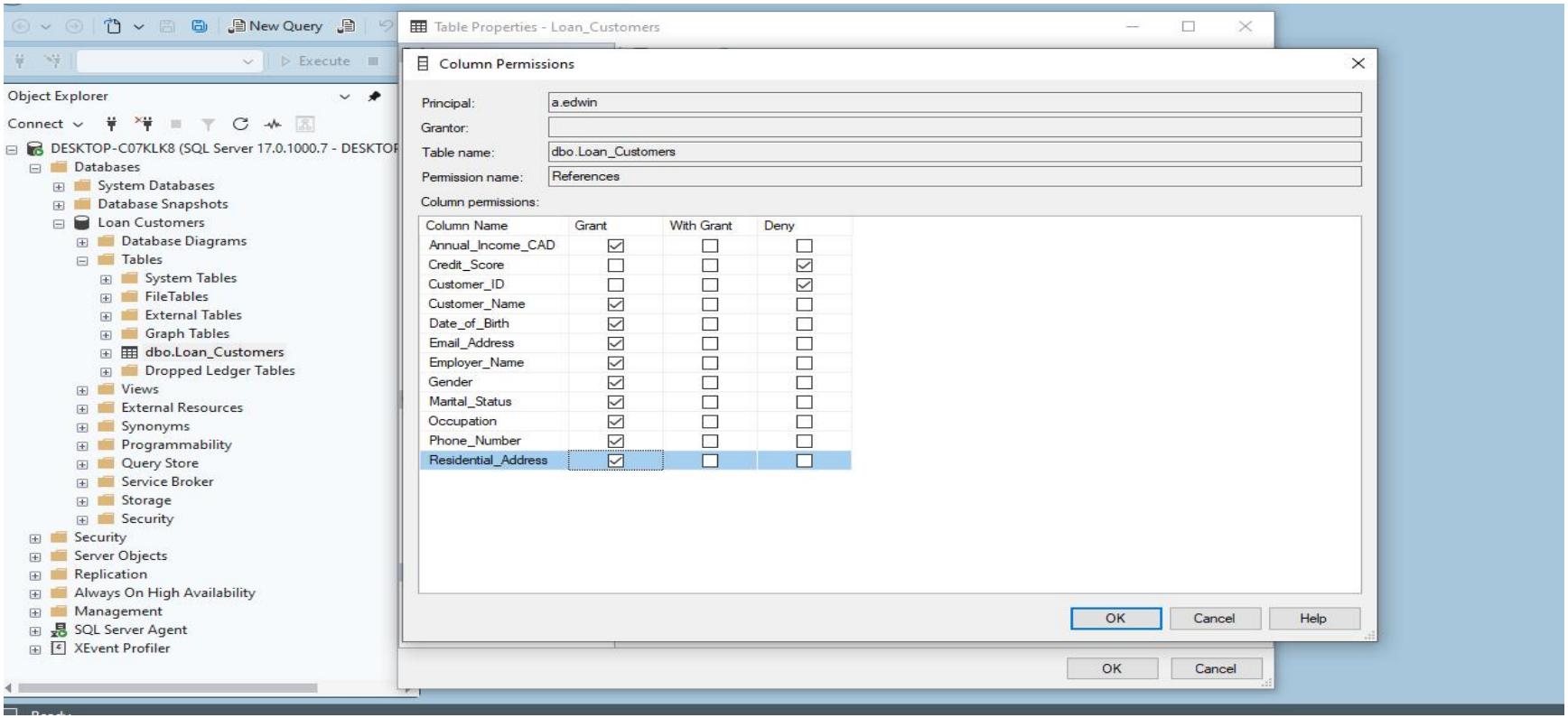
The following methods were deployed:

- 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.***

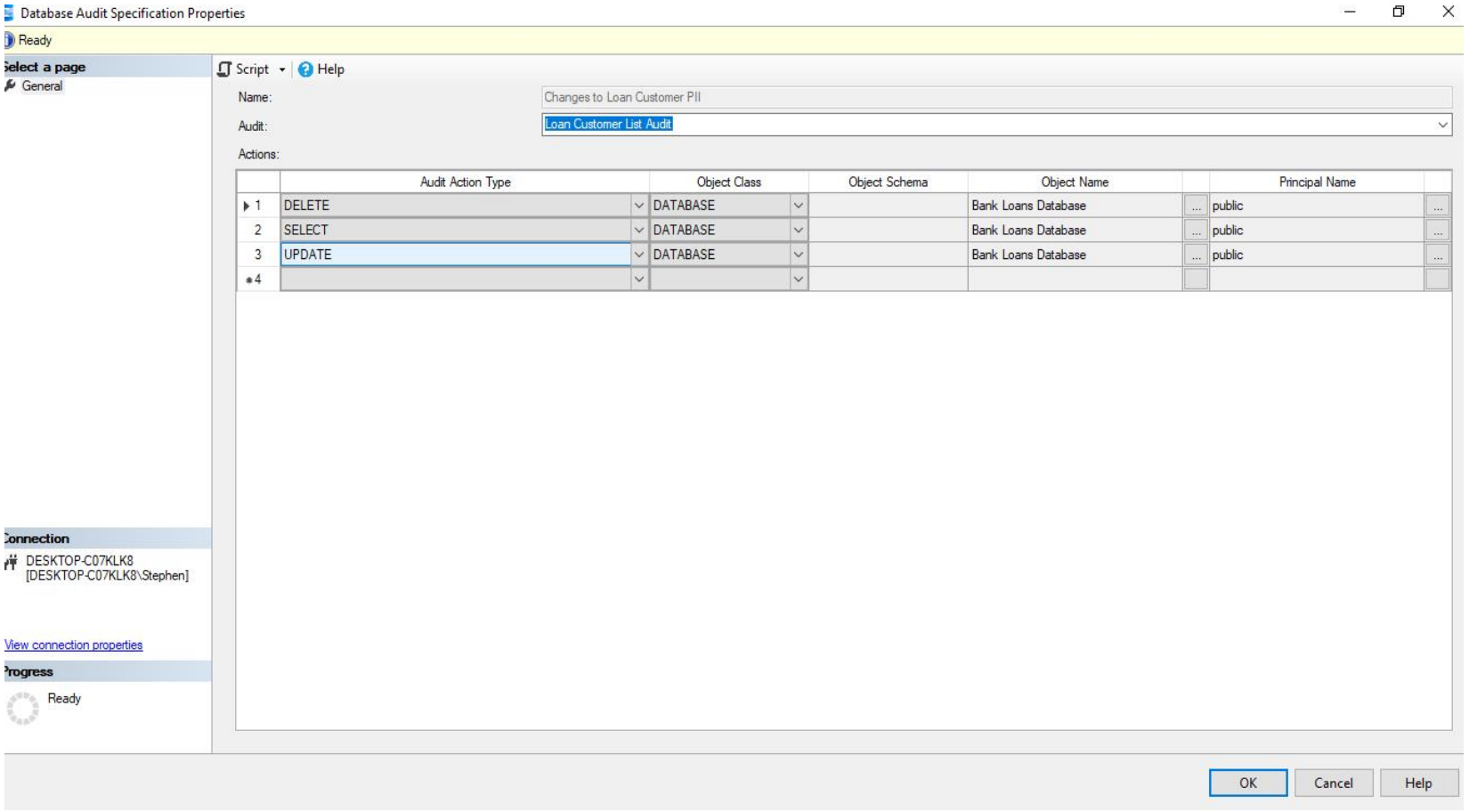
- The SQL Server Standard Development option was downloaded and installed together with the SQL Server Management Studio (SSMS).

- The **Loan Customer** database was created in SSMS and the bank loan customer list was uploaded.

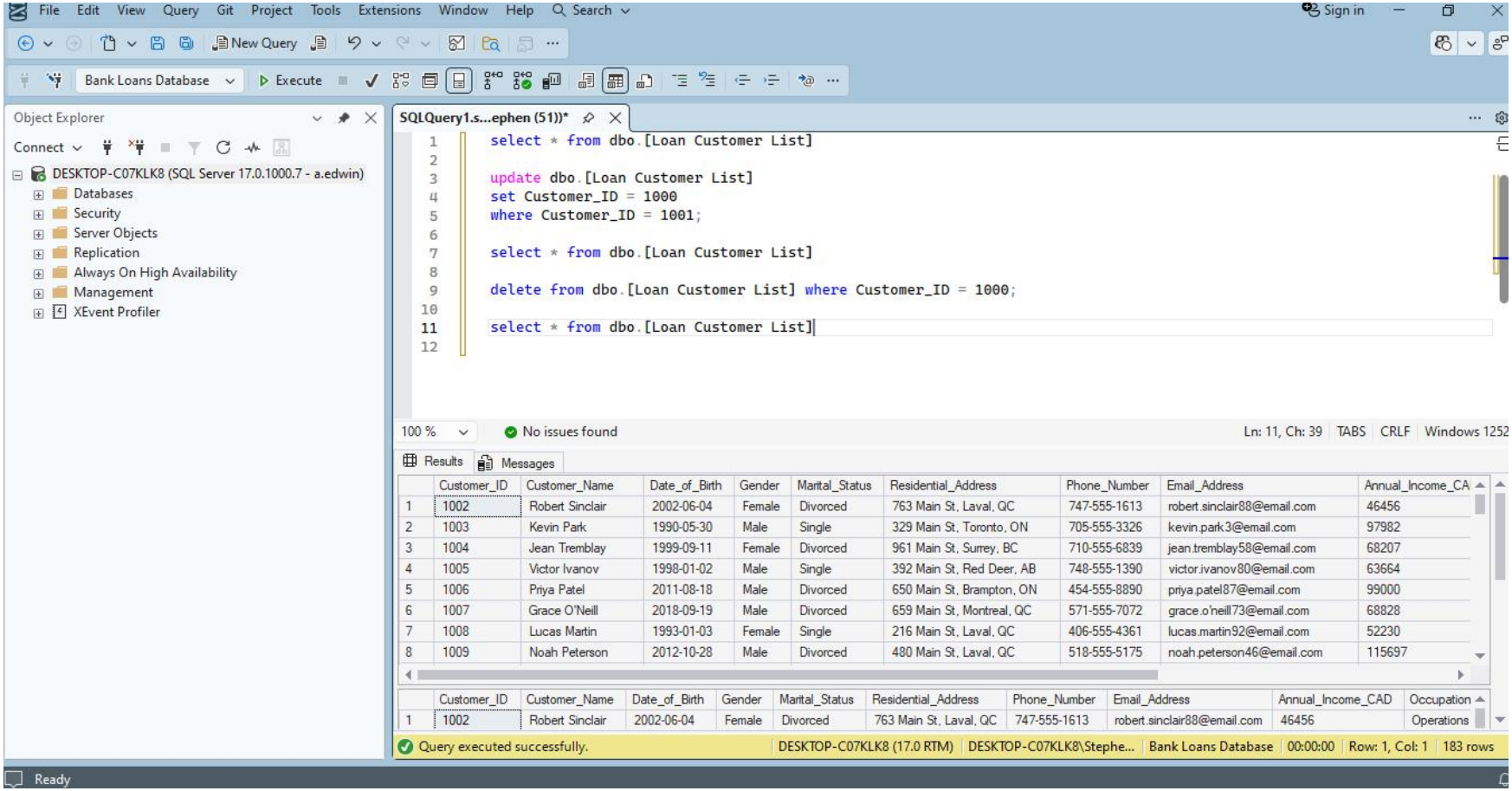
- An identity and access login was created for ***a.edwin*** with appropriate permission as an inputer per the loan process cycle. A screenshot is captured below:



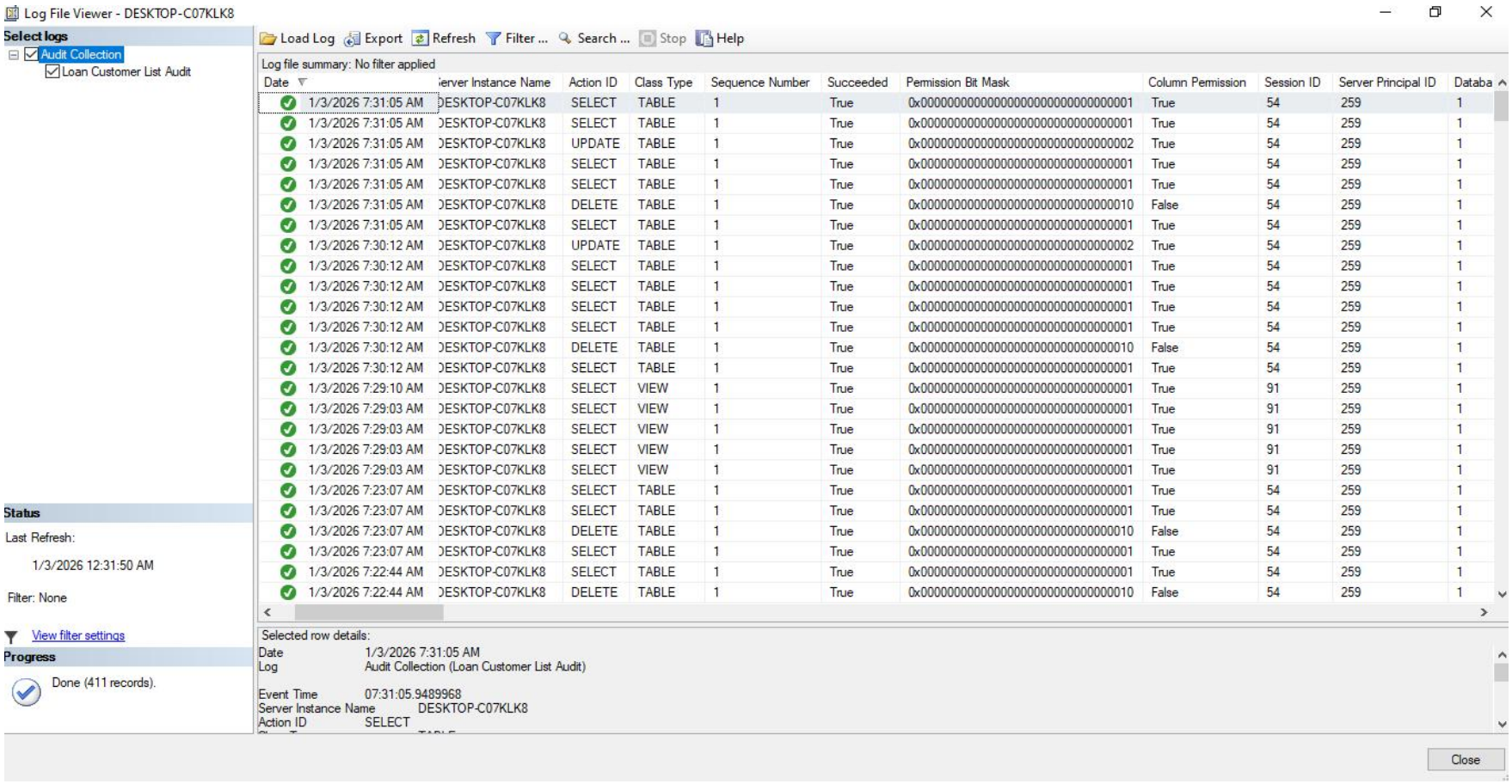
- The audit and the server audit specification were created for ***a.edwin*** over loan customer database with required audit action type in the SSMS. The user is permitted to access the database but not to update or delete



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



- The 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 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	