Bristol County Savings Bank
Commitment. Stability. Community.
Business Intelligence & Data Analytics

BCSB – Data & Analytics Query Execution Procedure

Departmental Guide for Responding to Business Line Reporting Requests

---

Purpose

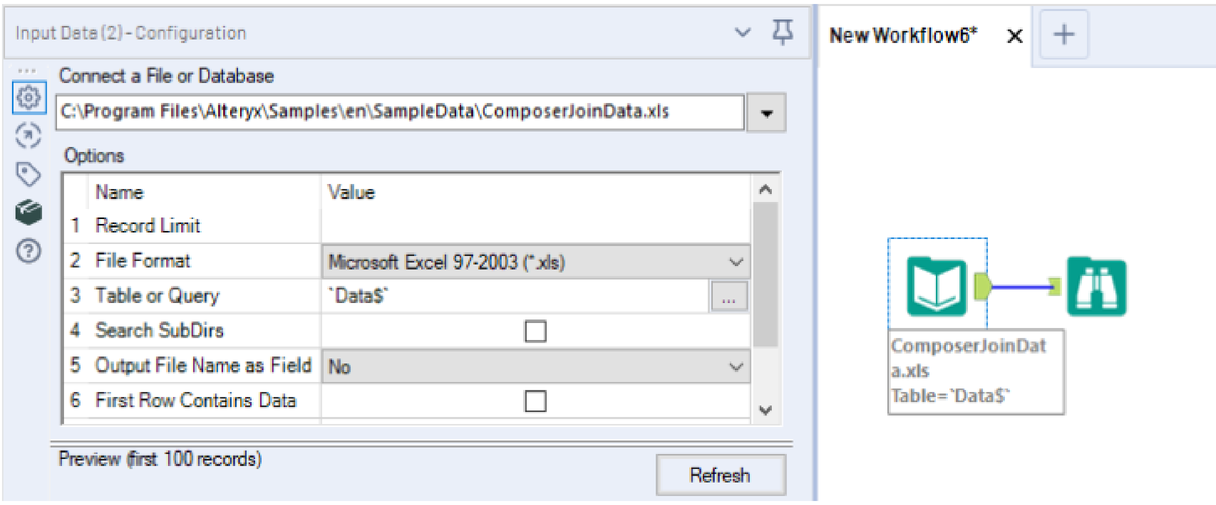
To define a standardized, secure, and auditable process for executing relational database queries in response to business line reporting requests. This ensures consistent procedures are followed across all tools and platforms, while maintaining compliance with internal controls and regulatory standards.

1. Tool Selection and Access Requirements

The Data & Analytics team may fulfill requests using one of the following approved query execution methods:

A. Alteryx (Input Data Tool)

- **Launch Alteryx Designer.**
- **Drag the "Input Data" tool onto the canvas.**
- **Navigate to 'Connect a File or Database' & click the down arrow to open the dropdown.**
  - **Select the appropriate Oracle database connection using the predefined connection string provided by IST.**
  - **Validate that the connection uses the approved driver and credentials configured by IST.**



Connect a File or Database

C:\Program Files\Alteryx\Samples\en\SampleData\ComposerJoinData.xls

Options

	Name	Value
1	Record Limit	
2	File Format	Microsoft Excel 97-2003 (*.xls)
3	Table or Query	`Data$`
4	Search SubDirs	□
5	Output File Name as Field	No
6	First Row Contains Data	□

Preview (first 100 records)

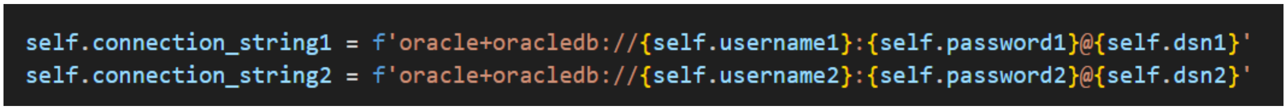
ComposerJoinData.xls
Table=`Data$`

- **Enter the SQL query directly into the tool or use the Visual Query Builder.**
- **Test query for accuracy and performance before continuing with the data pipeline.**

- **Save workflows to the secure shared repository with appropriate naming and version control.**

B. Python (with Encrypted Credential Management)

- **Open the designated Python script or notebook template.**
- **Load the Oracle database connection string, which references credentials stored in an encrypted .env file (never hardcoding credentials)**

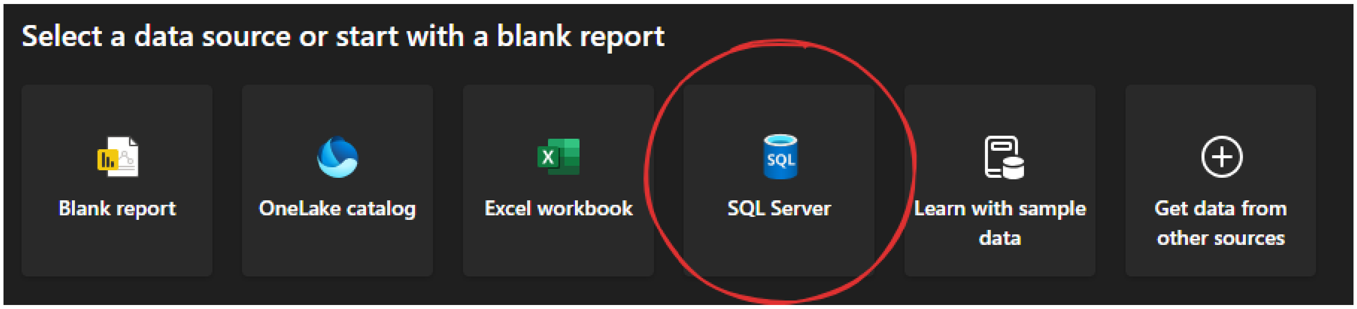


```
self.connection_string1 = f'oracle+oracledb://{self.username1}:{self.password1}@{self.dsn1}'
self.connection_string2 = f'oracle+oracledb://{self.username2}:{self.password2}@{self.dsn2}'
```

- **The .env file remains encrypted at rest and is decrypted at runtime only.**
- **Establish a connection to the Oracle database using the connection string**
- **Write and execute SQL queries as needed to fulfill the business request.**
- **Ensure that all access to the database is logged appropriately, including query context, execution time, and user.**
- **Store all scripts and output files in secure locations.**

C. Power BI (Direct Database Connection)

- **Open Power BI Desktop.**
- **Select "Get Data" → "SQL Server."**



Select a data source or start with a blank report

- **Enter the server and database names, and authenticate using credentials supplied by IST.**
- **Use either DirectQuery or Import mode, as appropriate to the request.**
- **Ensure any transformations or query modifications are documented in the Query Editor.**
- **Save Power BI files to the secure workspace and notify relevant stakeholders when the report is ready.**

---

2. Data Security and Compliance Controls

- **Credential Handling: Only use credentials provisioned by IST. Credentials must never be hardcoded or shared externally.**
- **Data Minimization: Retrieve only the data necessary to fulfill the request.**
- **Storage: Store outputs in approved directories with appropriate access controls. Sensitive data must be encrypted at rest.**

3. Review and Validation

- Before delivering any dataset or report, the output must be reviewed for completeness and accuracy.
- Confirm that data pipeline logic is traceable and reproducible.

4. Delivery and Documentation

- Deliver results through secure channels
- Document the request, query logic, tool used, and delivery method in the technical documentation in the request's repository ('Documentation' folder).
- Mark the request as completed only after confirmation of delivery and business line acknowledgment.

5. Ongoing Monitoring and Improvements

- Conduct periodic reviews of query practices and update this procedure as necessary.
- Revalidate connection strings and access credentials quarterly in coordination with IST.
- Participate in compliance audits and respond promptly to any remediation requests.

6. Ownership

This procedure is owned by the Chief Information Officer and maintained by the Data & Analytics team & the IST department. Any deviations must be approved in writing.

7. Review Cycle

This document is to be reviewed annually or upon significant changes to tools, security protocols, or regulatory requirements.