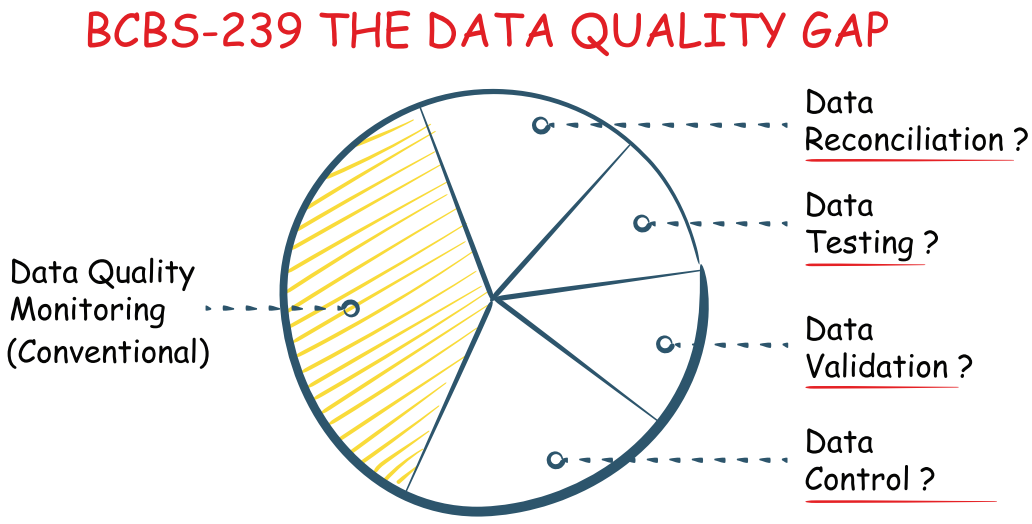
iCEDQ

TORANA INC.

BCBS 239- Data Quality Gaps

In this guide, while we will review BCBS 239 principles and discuss gaps in data quality that banks are facing. We will point out, that how banks are missing the crucial requirements for **data testing**, data validation, data reconciliation, and data controls. For data quality basics, please refer to the earlier **data quality guide.**



Torana Inc.
60 Long Ridge Road, Suite 303, Stamford CT 06902.
Phone: (203) 666-4442
contact@icedq.com

What is BCBS 239?

BCBS 239 is a regulatory act designed by Basel Committee on Banking Supervision, to ensure that large banks will have the right ***data infrastructure, data controls,*** *and* ***data reporting capabilities*** *on their risks and exposures. The* **BCBS 239***, is the first document to precisely define data management practices around implementation, management, and reporting of data.*

During the global financial crisis of 2007, the large banks (G-SIBs) were unable to provide "Aggregated Risk Exposure Data" from their systems. The regulations such as SOX, Dodd-Frank, CCAR, FINRA, Solvency and even BASEL were found inadequate as they had not clearly defined the **data quality** and the data management requirements.

BCBS 239 Principles

BCBS 239, Basel Committee on Banking Supervision published **14 Key Principles** for effective risk data aggregation and risk reporting under 4 categories (Data Governance and Infrastructure, Risk Data Aggregation Capabilities, BCBS Risk Reporting Practices, Supervisory).

Category	Principle	Description
A	1. Governance	A bank's risk data aggregation capabilities and risk reporting practices should be subject to strong governance arrangements.
	2. Data Arch & IT Infrastructure	A bank should design, build, and maintain data architecture and IT infrastructure which fully supports its risk data aggregation capabilities and risk reporting practices.

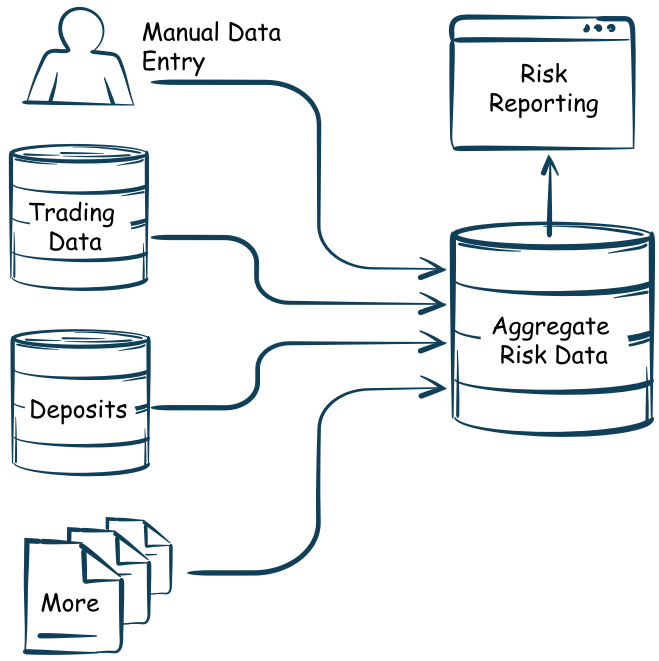
B	3. Accuracy & Integrity	A bank should be able to generate accurate and reliable risk data to meet normal and stress/crisis reporting accuracy requirements.
	4. Completeness	A bank should capture and aggregate all material risk data across the banking group by business line, legal entity, asset type, industry, region, and other groupings, as relevant.
	5. Timeliness	Provide aggregate and up-to-date risk data in a timely manner.
	6. Adaptability	Provide data on ad hoc requests during crisis situations or regular frequency.
C	7. Accuracy	Reports should be accurate, precise, and audited by reconciling and validated.
	8. Comprehensiveness	Reports should cover all material risk areas within the organization in depth and scope.
	9. Clarity & Usefulness	Reports should communicate information in a clear and concise manner.
	10. Frequency	The frequency of report production and distribution must be set appropriately.
	11. Distribution	Distribute reports to the relevant parties while ensuring confidentiality.
	12. Review	Supervisors should periodically review and evaluate a bank’s compliance with the eleven principles above.

D	13. Remedial Actions	Use the appropriate tools and resources to require effective and timely remedial action by a bank to address deficiencies.
	14. Home/host cooperation	Supervisors should cooperate.

All the BCBS 239 principles are parsed and grouped under the following 3 data requirements.

1. BCBS Reporting and data aggregation requirements.
2. BCBS 239 data governance.
3. BCBS 239 data quality requirements.

1. BCBS Reporting (Requirements)



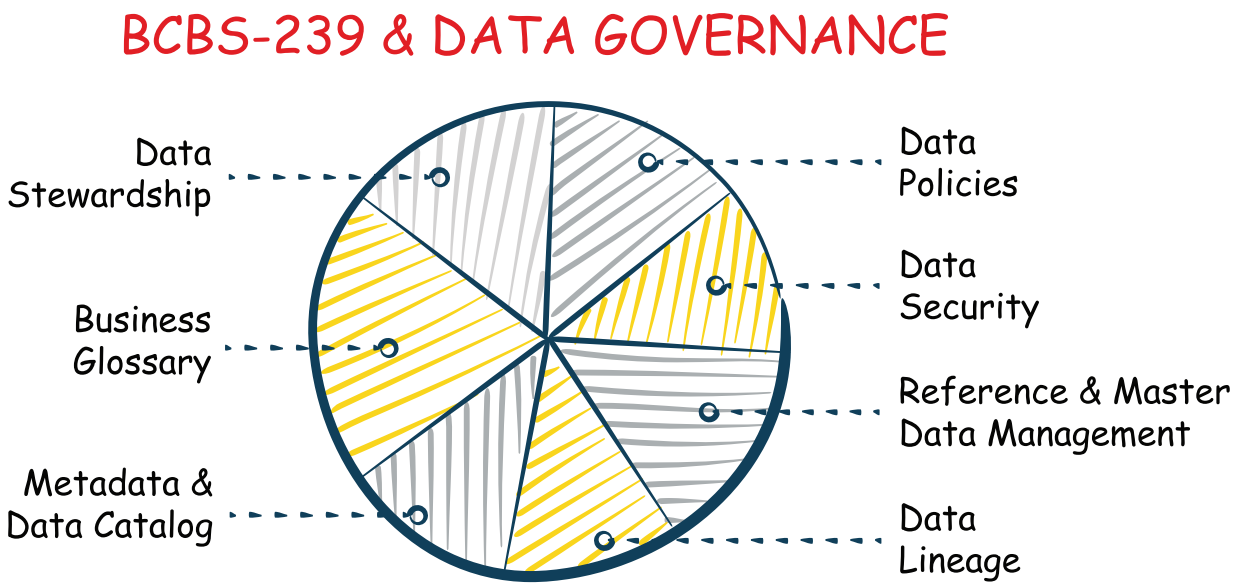
For BCBS reporting, banks collect all risk and exposure data from various data sources, divisions, and departments. This data is then integrated into a centralized database and can be made available to regulatory agencies and management in the form of reports.

The principles (4, 5, 8.57) provide a guideline to the data architects for identifying data sources for all the risk related data and then building data pipelines to integrate all the risk data into a data repository.

BCBS 239 Guiding Principles Related to Risk Data Aggregation		
Risk Data Requirements	Principle 5	▪ Aggregate credit exposure data for all large corporate borrowers. ▪ Collect retail exposure data. ▪ Collect counterparty credit risk exposures data. ▪ Get data for trading exposures, positions, operating limits, and market concentrations by sector and by region. ▪ Calculate liquidity risk indicators such as cash flows/settlements and fundings. ▪ Aggregate risk data by country's credit exposures. ▪ Collect industry credit exposures data by industry types across all business lines and geographic areas.
	Principle 8, Rule 57	▪ Risk management reports should include exposure and position information for all significant risk areas (e.g., credit risk, market risk, liquidity risk, operational risk).
	Principle 4	▪ Data should be available by business line, legal entity, asset type, industry, region, and other groupings.
Data Infrastructure	Principle 4	▪ A bank should be able to capture and aggregate all material risk data across the banking group.

Beyond reporting data requirements, BCBS 239 also provides policies for data governance and **data quality** requirements for risk data aggregation and report generation.

2. BCBS 239 Data Governance (Requirements)



The regulation provides a series of guiding principles for data governance and data management. The categorization of the principles will provide you a quick guide related to the coverage of the BCBS 239 data governance requirements.

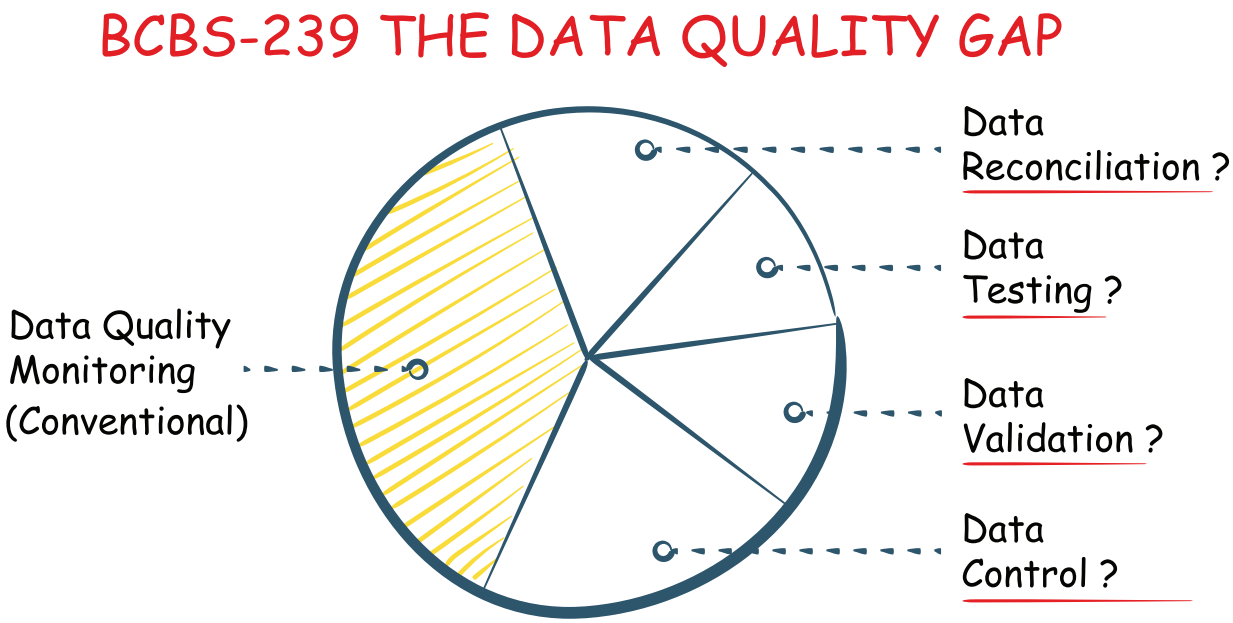
BCBS 239 Guidance for Data Governance		
Data Policies	Principle 1, Rule 27	▪ Create a framework to include agreed service level standards for both outsourced and in-house risk data.
	Principle 2, Rule 34	▪ Establish adequate controls throughout the lifecycle of the data.
	Principles 3, Rule 36, Rule 39	▪ A bank should strive towards a single authoritative source for risk data per each type of risk. ▪ Document and explain all their risk data aggregation processes whether automated or manual.

	Principle 9, Rule 69	▪ Confirm periodically with recipients that the information aggregated and reported is relevant and appropriate.
	Principle 11, Rule 73	▪ Supervisors expect a bank to confirm periodically that the relevant recipients receive timely reports.
Data Security	Principle 1, Rule 27	▪ Create policies on data confidentiality, integrity, and availability, as well as risk management.
Reference & Master Data Management	Principle 2, Rule 33	▪ Create single identifiers and/or unified naming conventions for data including legal entities, counterparties, customers, and accounts.
Data Lineage	Principle 1, Rule 29	▪ Fully document, subject to high standards of validation.
	Principle 3, Rule 39	▪ Document and explain all their risk data aggregation processes whether automated or manual.
Metadata & Data Catalog	Principle 2, Rule 33	▪ Create data taxonomies. ▪ Store information on the characteristics of the data (metadata).
Business Glossary	Principle 2, Rule 34	▪ Ensure data is aligned with the data definitions.
	Principle 3, Rule 37	▪ A bank should have a “dictionary” of the concepts used, such that data is defined consistently across an organization.
	Principle 9, Rule 67	▪ A bank should develop an inventory and classification of risk data items which includes a reference to the concepts used to elaborate the reports.

Data Stewardship	Principle 2, Rule 34	▪ Establish roles and responsibilities for the ownership and quality of risk data. ▪ Define the role of the business owner.

3. BCBS 239 Data Quality (Requirements)

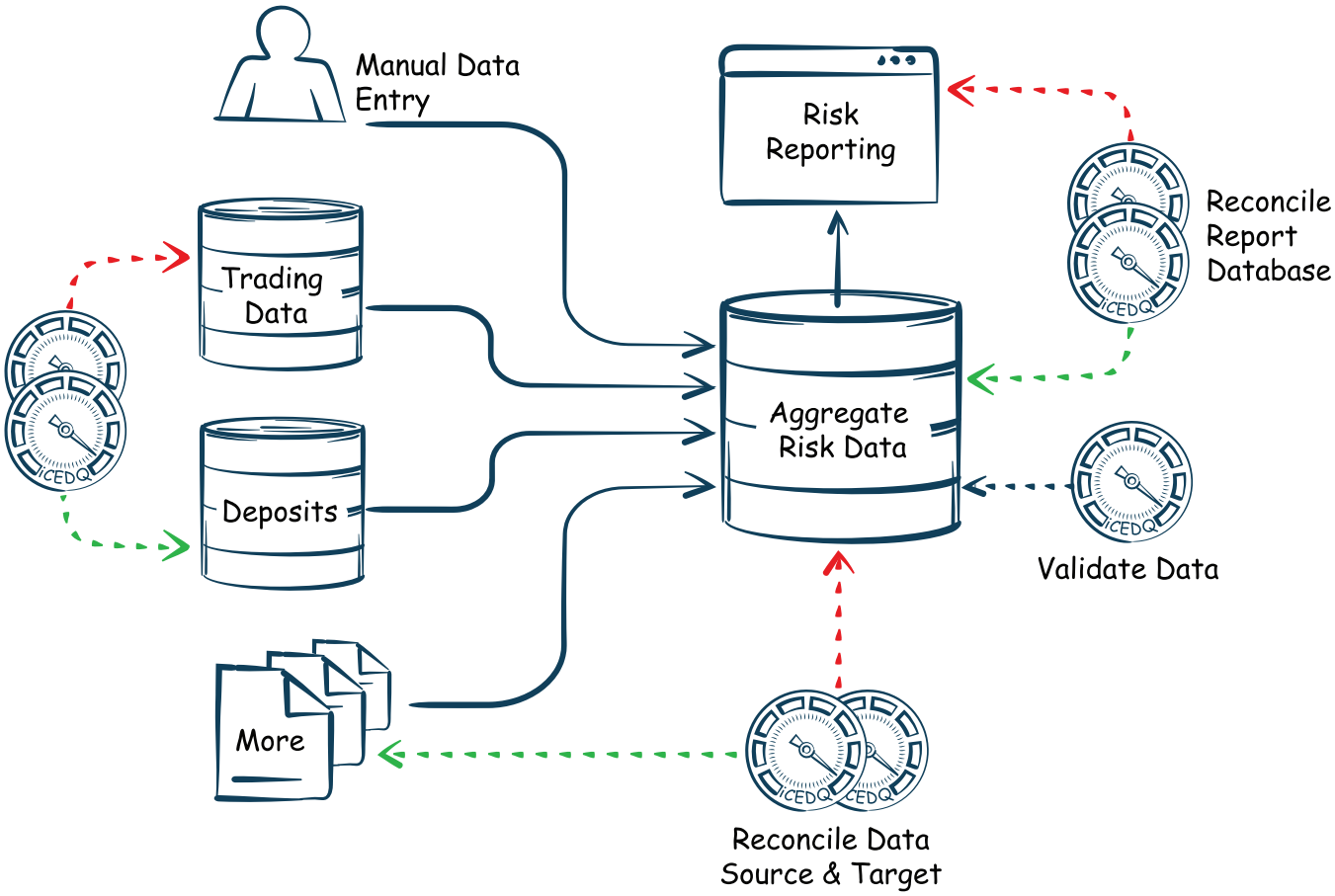
Despite the granular specifications outlined in the BCBS 239 requirements, organizations are limiting themselves to the conventional data quality ideas of reporting data quality metrices along the lines of the **six dimensions of data quality.**



However, a simple parsing of the principles, it becomes very clear that many of the key data quality requirements are not fulfilled by conventional data quality approach.

BCBS 239 Data Quality, Data Reconciliation, Validations, Testing and Controls Requirements.		
General Data Quality	Principle 1, Rule 27, Rule 30	▪ Identify data critical to risk data aggregation. ▪ Promote the identification, assessment, and management of data quality risks.
	Principle 7, Rule 54, Rule 55, Rule 56	▪ Establish expectations for the reliability of approximations (**accuracy**, **timeliness**, etc.) ▪ Establish accuracy and precision requirements. ▪ Supervisors expect banks to consider accuracy requirements analogous to accounting materiality.
Data Reconciliation	Principle 2, Rule 33	▪ Banks do not necessarily need to have one data model; rather, there should be robust automated reconciliation procedures where multiple models are in use.
	Principle 3, Rule 36	▪ Risk data should be reconciled with the bank's sources, including accounting data where appropriate, to ensure that the risk data is accurate. ▪ A bank's risk personnel should have sufficient access to risk data to ensure they can appropriately aggregate, validate and reconcile the data to risk reports.
	Principle 7, Rule 53	▪ Reports should be reconciled and validated. ▪ Defined requirements and processes to reconcile reports to risk data.
Data Validation	Principle 7, Rule 53, Rule 56	▪ Reports should be reconciled and validated.

		▪ Automated and manual edit and reasonableness checks, including an inventory of the validation rules that are applied to quantitative information. The inventory should include explanations of the conventions used to describe any mathematical or logical relationships that should be verified through these validations or checks. ▪ Expect a bank to consider precision requirements based on validation, testing or reconciliation processes and results.
Data Testing	Principle 7, Rule 56	▪ Expect a bank to consider precision requirements based on validation, testing or reconciliation processes and results.
Data Controls	Principle 3, Rule 36, Rule 40	▪ Controls surrounding risk data should be as robust as those applicable to accounting data. ▪ Monitor the accuracy of data and to develop appropriate escalation channels and action plans to be in place to rectify poor data quality.
	Principle 7, Rule 53, Rule 58	▪ Integrated procedures for identifying, reporting, and explaining data errors or weaknesses in data integrity via exceptions reports.
	Principle 4, Rule 42	▪ Process to rectify completeness issues.

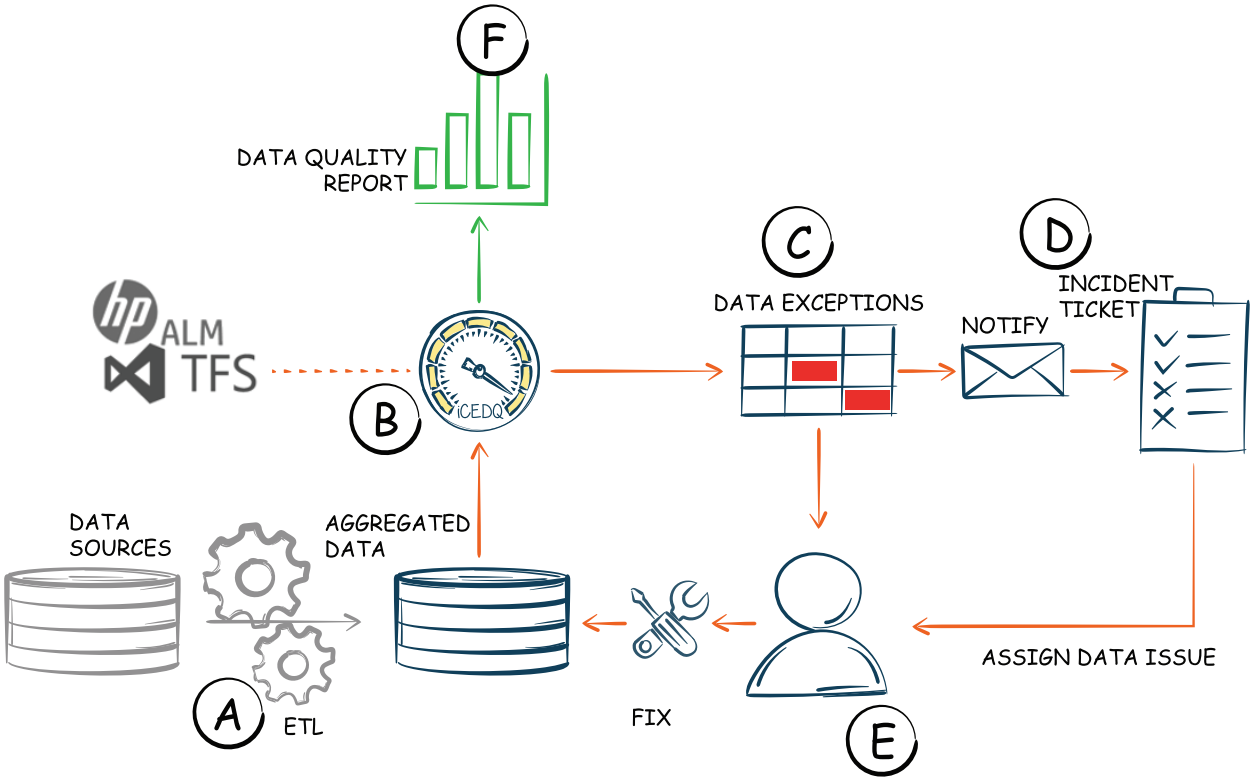


The DQ requirements are summarized below:

1. During the development of the data processing **data testing** is required.
2. Every time data is moved the from a source to destination then **source and target data reconciliation** is required.
3. There must be a process to report **data exceptions**, otherwise none can find and fix the data.
4. There must be a **workflow** to open and assign tickets for data issues and assign responsibilities.
5. A centralized data **rules repository** for all the data checks.
6. **Data quality reporting** for compliance.

BCBS 239 Compliance & iceDQ

iceDQ's was purpose-built for data pipeline testing, data validations, data reconciliations, and data controls.



A	Multiple data pipelines extract data from various systems all over the world, then transform and load data into a centralized risk database.
B	iceDQ rules the tests and monitor the data to find any discrepancies by executing multiple validation and reconciliation rules.
C	The data exceptions are identified and notified.
D	Tickets are created in incident management system.
E	The data stewards take the ticket along the data exception files, investigate, and fix the data issues.
F	DQ reports are generated for overall state of the data infrastructure.

By following the above workflow iceDQ can fulfill multiple data quality gaps identified previously.

DQ Gap	DQ Requirements	iceDQ Solution
Data Reconciliation	The aggregated risk database must source data from multiple systems. It is brought there from many independent data sources. How do you know if the data in the risk database matches with the source systems?	Create data reconciliation between data sources and risk database.
	A typical bank will have multiple systems. Each system produces its own set of data and stores in its own database. This can also result in duplicate or redundant data in multiple systems. How does the bank know that the two systems have consistent data?	Create rules data reconciliation across systems. Implement data integrity reconciliations rules.
	Data integration is done by populating data from multiple sources and by multiple data pipelines. Even if the processes loaded data successfully it does not mean that the data integration is correct. Example, it is possible for two independent data processes to correctly load data in accounts and transactions but still be wrong. As it is possible that the account data process never received the complete account list and it processed whatever it got successfully. It is not possible to identify such data integrity issues with a simple data quality check.	Example, determine if there are any accounts in a transaction that don't exist in the account master.
Data Validation	Sometimes the data correctness can only be determined by digging into the business rules. Example: How to validate "Net Amount"?	Create a Data Validation Rule. For "Net Amount", it can be done by invoking the formula and calculating the value based on the underlying metrics.

Data Controls	Banks have thousands of data jobs running every day which are scheduled and monitored by the orchestration tools. When the data jobs fail, they stop the data flow. However, they don't monitor if the data processes have transformed the data correctly. As often happens, periodic checks of data might let you know there are data quality issues. But most of the time it is too late or too expensive to fix it. As the damage is already done. What kind of data controls and escalation are available to detect and escalate data processing errors?	Establish Data Controls on top of the data processing. Don't let the next process start before the upstream data process passes the control test.
	Regardless of all the checks, data issues will happen. In such cases, it is not enough to say there is an issue or a certain data element has an issue.	Make sure every data error generates an exception report to pinpoint the exact record and attribute where the error happened.
Data Testing	For the data processes to exist they must be developed, then the questions arise: How are the data processes being tested? How do you make sure that you don't have data introducing errors in your data? How are you doing **ETL Testing?**	Automate **ETL Testing** with iceDQ.

BCBS 239 Compliance Checklist

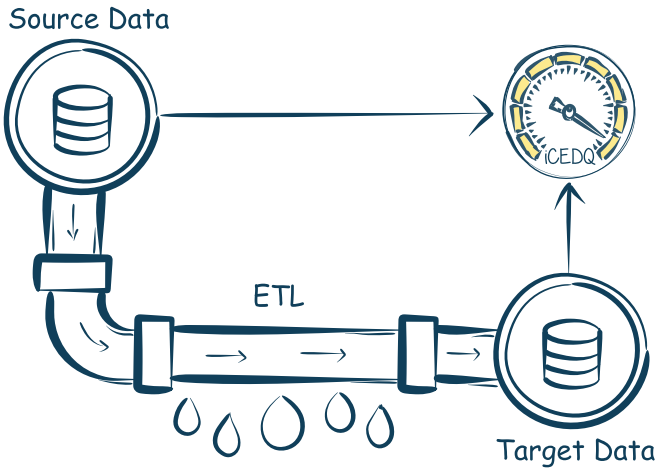
For BCBS 239 compliance report there is a rating system. For each of the 11 principles there is a rating of maximum 4 to a minimum of 1.

Rating	Comment
4	The principle fully complies within the existing architecture and processes.
3	The principle largely complies, and only minor actions are needed to fully comply.
2	The principle is materially non-complied and needs significant work.
1	The principle has not been implemented.

Conclusion

While considering data quality requirements for BCBS 239, it is essential to carefully review the 14 principles and sub-rules. This will ensure that banks don't leave gaps in their data quality compliance from the perspective of:

1. **Data Testing**
2. Data Validation
3. Data Reconciliation
4. Data Controls



"Integrated procedures for identifying, reporting and explaining data errors or weaknesses in data integrity via exceptions reports."

BCBS 239