Data controls for model data

Discussion paper

Building a better working world

Contents

1 Understanding data controls

Overview of data controls

What are data controls?

Data controls refer to the control activities embedded across the business data processes and underlying systems, from sourcing to consumption in risk/finance models. These controls, either process or data controls, can be preventive or detective in nature and can exist as manual or automated activities.
There are five (5) key data control categories:

- Data quality controls
- Data access & update controls
- Data entry controls
- Data attestation controls
- Data processing controls

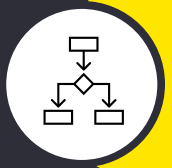
Why are data controls important?

- Robust data controls are crucial for compliant risk and finance processes, particularly in model data management domain to ensure data is fit for use and meets regulatory and management expectations.
- Key risk and finance regulations or guidelines, such as BCBS 239 Principles[1] for effective risk data aggregation, OSFI's E-23 Guidelines[2] on model risk management and AIRB's Data Maintenance Notes[5] on emphasize the need for effective data controls.
- Data capability frameworks such as DCAM (Data Management Capability Assessment Model) and DAMA (Data Management Association) provide industry best practices and emphasis the need to ensure managed and controlled data environments for business decision-making.

How can data controls be effectively designed?

Create a consistent data controls strategy aligned with the business goals and enterprise data capabilities

Develop a data controls operating model aligned with the three lines of defense



Evaluate the characteristics and complexity of business data procedures and systems to tailor controls at the appropriate magnitude and detail

Implement the controls and ensure the design corresponds to the identified risks and complies with second line review procedures

1 BCBS 239 Principles *2 E-23 Draft guideline* *3 Data Maintenance at IRB Institutions*

The need and expectations for effective data controls

Data controls help improve confidence in data while ensuring regulatory compliance. By implementing robust data controls, organizations can prevent data issues and subsequent loss of customer trust and regulatory fines. OSFI's E-23 guideline and BCBS's principles for risk data aggregation and reporting are some of the regulations that expect organizations to have effective data controls.

E-23 guideline

OSFI has issued guidelines on enterprise-wide model risk management. These guidelines touch upon the model risk arising from data and the need for effective controls to prevent data issues and ensure data used for model development satisfies the following properties1:

- Accurate and fit-for-use (e.g., free from material errors, bias is understood and managed)
- Relevant and representative (e.g., reflects the intended target population of the model)
- Adequately complete for its intended purpose
- Traceable (e.g., lineage and provenance are understood and documented)
- Timely (e.g., updated with a frequency aligned with its intended use).

BCBS 239 principles

BCBS 239 published by Basel Committee on Banking Supervision (BCBS) is a set of principles2 emphasizing improvements in financial institution's risk data aggregation and risk reporting capabilities. These principles set expectations on data quality and usability and ask organization to meet the following characteristics:

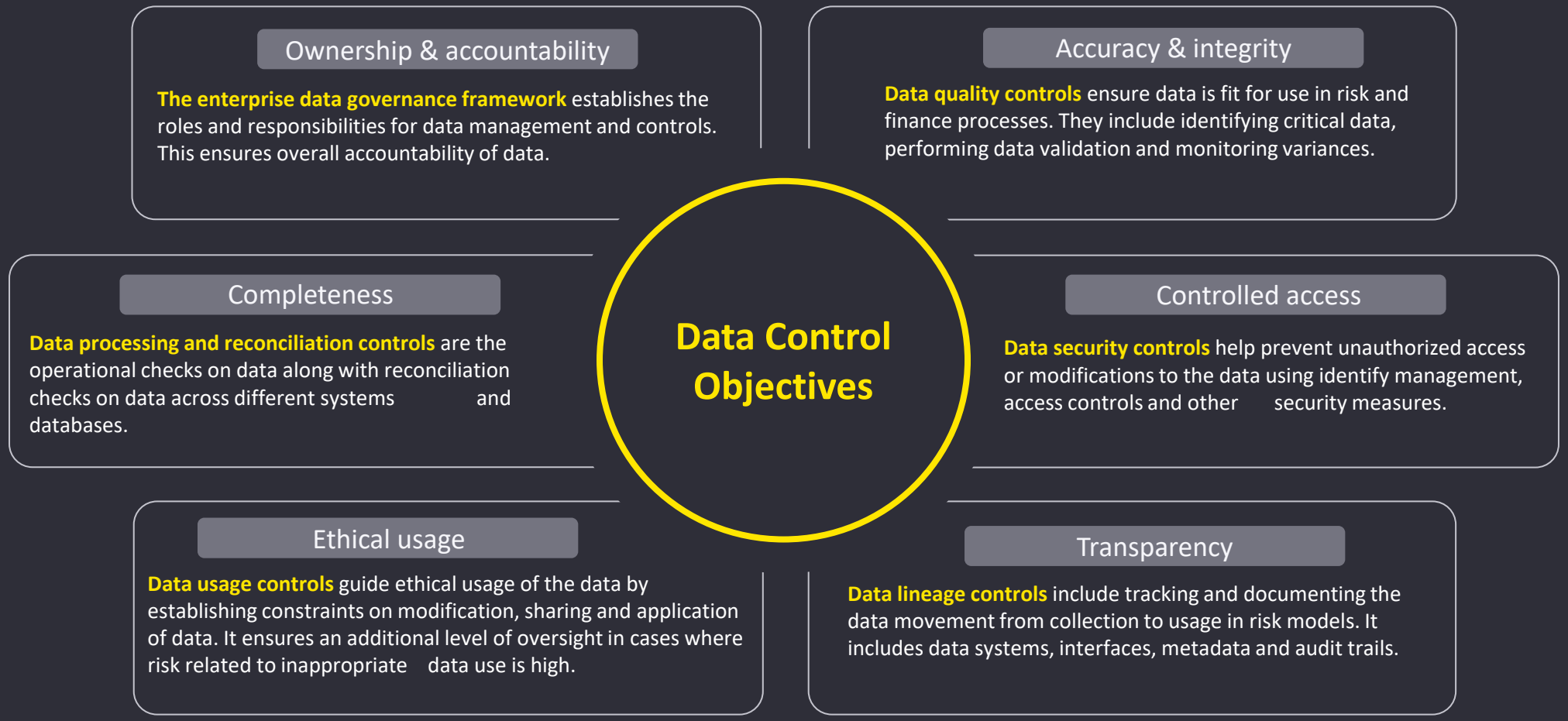
- Ensure accuracy and integrity through automation of data generation and risk report validation (Principles 3 & 7)
- Completeness of material risk data and comprehensiveness of risk reports to cover material risk domains (Principles 4, 8 & 9)
- Timeliness in producing risk information (Principle 5)
- Adaptability in data generation and creation of risk reports during times of crisis or to satisfy ad-hoc requests (Principle 6)

1 E-23 Draft guideline

2 BCBS 239 Principles

What objectives can be achieved through data controls?

Data controls are mechanisms and processes implemented to ensure data is accessible, trustworthy, well understood and fit for use for various risk management practices in an organization. They are critical to meet both business and regulatory objectives.

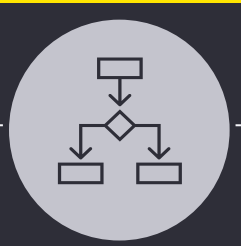


Key components of a controlled data environment

The below components help the organizations establish a data controls strategy and operationalize controls through a structured approach aligned with people, process and technology aspects.

Data control ownership & design authority

- Governing bodies and leadership roles should be created and assigned according to the policies and standards for data controls.
- Design authority is to be identified for working in collaboration with first line of defense to identify control requirements, design the controls and implement them.



Data management lifecycle and control points

- Data control functions must be in line with data management across the organization.
- Regular touchpoints and routines should be established to ensure ongoing collaboration across the organization.
- Any data being sourced should be subject to the data controls established in the organization across the different functions.

Data controls implementation

- Controls should be designed, implemented and tested for design and operational effectiveness.
- Continuous monitoring mechanisms must be in place to manage the data controls processes and to mitigate any issues with the controls.

2 Data controls ownership

3 Lines of Defense (3LoD) model for data controls

Data controls need to be implemented upstream at data capture and processing for various business operations, through to its usage in risk or finance models. The business data stewards in First Line of Defense (1LoD) are responsible for effective design of these controls, supported by the design authority and enterprise data office. The oversight and testing of data controls should be performed according to second line (2LOD) policies and procedures.

First Line of Defense (Controls design)	Second Line of Defense (Controls testing)	Third Line of Defense (Controls audit)
Data stewardship & design authority **1A (Data steward, Data custodian):** • Ownership of controls in respective business areas • Ensure appropriate controls are in place for data in respective business units • Identify, design, implement and maintain required controls based on associated risk and its severity • Monitor for any data control issues and exceptions and remediate promptly **1B (CDO):** • Provide oversight for controls design and ensure compliance with the Second Line of Defense's (2LoD's) governance requirements • The authority on matters pertaining to the data controls design and implementation	• Ensure roles and responsibilities for data controls management have been established • Establish metrics/risk tolerances to measure the performance of controls • Establish expectations and define frameworks related to data risk management and communicate to 1 LoD • Support 1 LoD with expertise to understand the controls testing criteria and approach • Periodically test the controls and monitor the operational effectiveness of implemented controls to mitigate the risk • Ensure compliance with policy, standards and guidelines and report to management as required by the frameworks and policy	• Review effectiveness of control testing • Perform an independent assessment of governance, risk management and internal controls and report on the gaps/findings identified in the internal control processes • Provide objective assurance to the management committee and the board of directors on the overall effectiveness of governance, risk management and controls • Provide recommendations for enhancing controls and improving overall data controls management • Monitor remediation of identified data control issues and exceptions

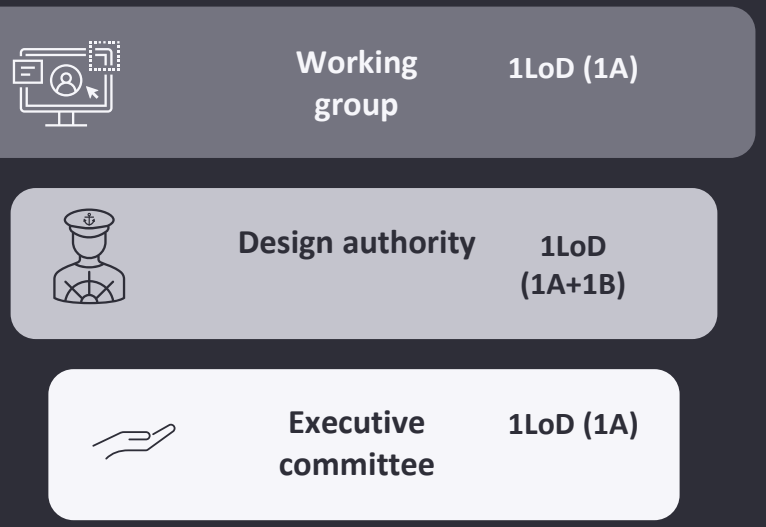
Ownership of data controls

Controls operating model – governing bodies

The controls working group and design authority work closely (1LOD) to design and operationalize controls in data processes and IT systems. Below is a summary of the roles and responsibilities of the governing bodies that are involved in controls implementation.

Working group

- Working group consists of data stewards, custodians and any technology support resources, as needed.
- It is responsible for designing and operationalizing the data controls within each business domain.
- Data stewards identify the data controls requirements and custodians are responsible for technical implementation of the controls and establishing monitoring mechanisms



Design authority

- Design authority includes data owners, data architects, process owners, data governance and business data leads.
- This authority is responsible to review and provide approvals for data controls design within the organization and define the best practices for designing these controls.
- The authority works closely with domain leads to ensure implemented controls mitigate the data risks identified.

Executive committee

- Executive committee comprises the CDO and the individual business unit heads.
- This committee oversees and supports the development and implementation of data controls and ensures alignment of these controls with the organization‘s strategic goals and internal risk and controls framework.
- The committee establishes requirements for periodic monitoring of controls, reviews effectiveness of controls and prioritizes remediation.

3 Data management lifecycle and related controls

Data management lifecycle overview

Data controls need to be embedded in the various activities performed as part of the data management lifecycle. The data lifecycle refers to the movement of data in the system from creation to usage of the data in risk/ finance models. At each stage through the lifecycle the data goes through various processes or steps, supported by underlying technology systems.

Data usage

The stored data is now available for consumption within the organization in line with the data access definitions. Data usage principles are enforced to ensure data is utilized by the right set of roles and for the right purpose.

Data consolidation & aggregation

Once data has been collected from the varied sources, it needs to be consolidated into one single source of truth and aggregated at the appropriate granularity.

Data storage

The data is then stored in the designated databases to ensure easy accessibility and the storage is evaluated for security issues and performance capabilities. Additionally, appropriate data access measures are put in place.

Data creation

The first step in the data management lifecycle is creation of the data. This could include getting data from multiple sources such as automatic capture of data, manual data entry, external datasets, etc.

Data processing

The data is then processed to perform any data transformations, encryption or conversions to clean the data and ensure uniformity in the formats and to prepare the data to be stored and usable.

Common categories of data controls

The control categories outlined below help identify and define various data controls, as well as ensure robust coverage across the data management lifecycle.

Data Quality Controls (DQ)

These controls involve instituting activities for data quality governance, data retention and data validation in all source systems.

Data Attestation Controls (DA)

These controls set up an attestation framework that identified responsibilities and accountability for review and approval by management and board.

Data Access & Update Controls (DU)

These controls implement automated processes, edit checks, dual review processes and tiered approval systems in cases where risk of data access and alteration is high.

Data Entry Controls (DE)

These controls involve defining uniform business processes to create data during business transactions along with appropriate oversight procedures.

Data Processing Controls (DP)

These controls involve establishing well-defined reconciliation processes where comparing multiple sets of data aids in detection of data discrepancies.


4
Data Controls Implementation

Illustrative data controls and control activities – 1/2

Several controls need to be embedded throughout the business systems and technology architecture to reduce or mitigate risks. These control activities may be preventive or detective in nature and may exist as manual or automated procedures.

Control category	Identifier	Control activity	Description
Data Quality Controls (DQ)	DQ1	Data element identification and prioritization	Identify key data elements for the enterprise or critical inputs into the risk models used by different business units to implement robust governance practices.
	DQ2	Data quality checks	Implement data quality checks for upstream data sources to ensure high-quality data in the internal environment.
	DQ3	DQ certification of production data	Establish processes to certify production datasets on an ongoing basis by data owners or their delegates for consumption in AIRB production models.
Data Entry Controls (DE)	DE1	Trusted source designation	Designate trusted sources for all datasets to apply data entry controls and ensure reliable data sourcing. Trusted sources provide reliable, timely, verifiable, and authoritative data within an organization.
	DE2	Manual data input controls	Setup processes to apply controls on manual data entered into the system to check for datatype, range of the data being entered, and a completeness check to ensure all the fields have been entered.
Data Attestation Controls (DA)	DA1	Data lineage	Document the lineage (i.e., table, column, and element level lineage) for Critical Data Element (CDE) / Model Production Data Element (MPDE) / Model Analytics Data Element (MADE) in datasets such as portfolio sources, economic sources, etc. and periodically review and update the data flows and transformations applied to data.
	DA2	Metadata capture	Capture metadata in an enterprise tool, including a data dictionary and business glossary, and establish periodic monitoring/update processes for changes to metadata.
	DA3	DQ attestation of model data	Implement processes to attest model datasets for use in developing AIRB risk models.

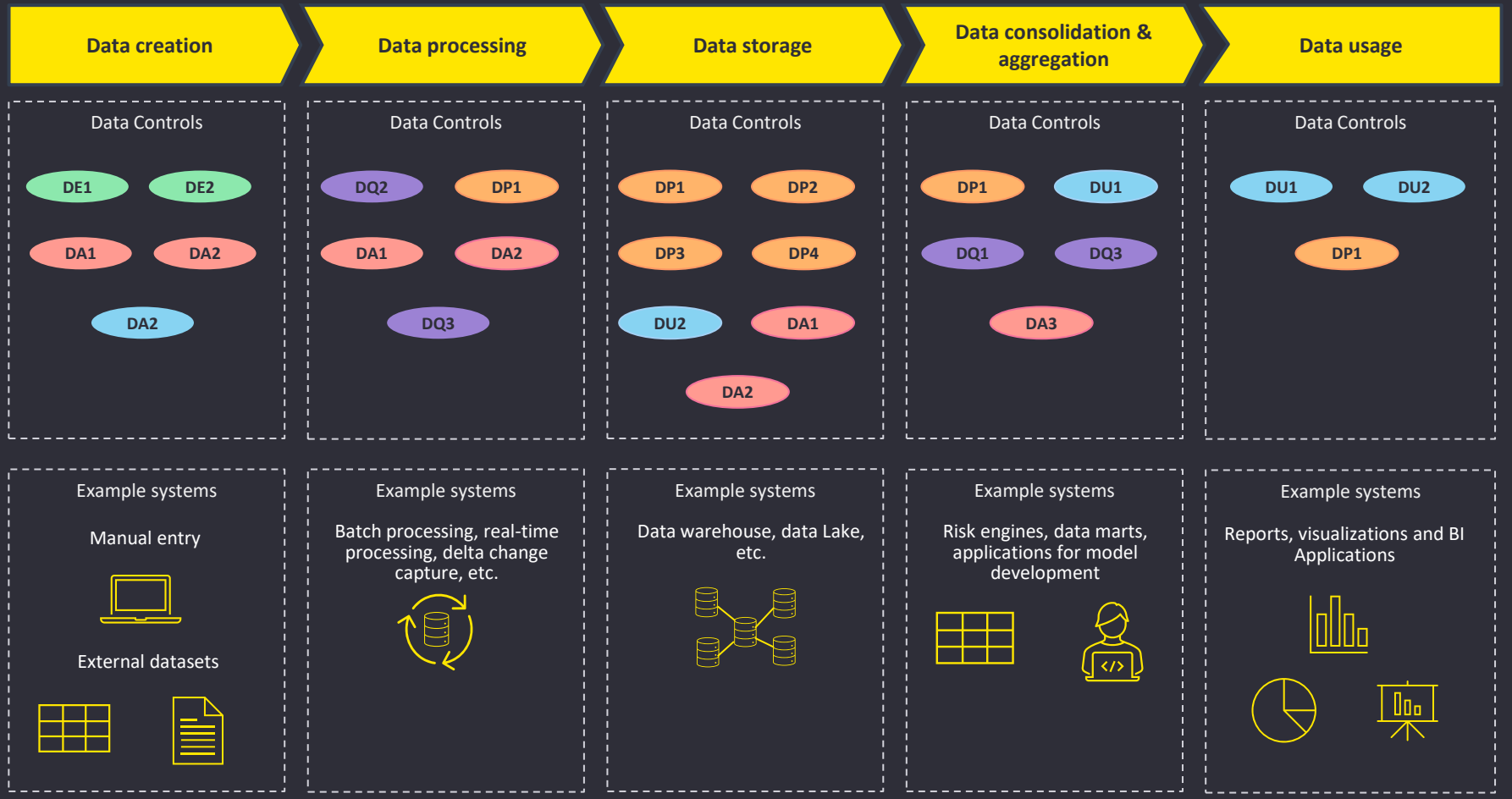
Illustrative data controls and control activities – 2/2

Control category	Identifier	Control activity	Description
Data Processing Controls (DP)	DP1	Data processing checks	Trigger alerts when the dataset fails data load checks with information such as job status, failed step, impact, remedial action, etc.
	DP2	Data feeds to EDW reconciliation with loan extract/product files.	Perform reconciliation of data feeds (i.e., internal or external) to Enterprise Data Warehouse (EDW) with data extracted from loan extract/files (e.g., third-party loans, macroeconomic, credit bureau data).
	DP3	Product balance in EDW reconciliation to accounting sub-ledger file	Perform reconciliation of product balance data consolidated in EDW to accounting balances received from the sub-ledger summary data file.
	DP4	Adjustment / Correction to data in EDW	Assign user roles to perform necessary manual adjustments/corrections to data in EDW to address operational scenarios based on documented procedures.
Data Access & Update Controls (DU)	DU1	EUC (End User Computing) Monitoring	Inventory and monitor EUCs used in data processes as per EUC industry best practices on its usage in risk data transformation or aggregation.
	DU2	Access control on data entry/updates	Implement access control based on user roles and activity mapping for data entry or modifications to prevent unauthorized data access, update, or deletion. Also, establish review and approval procedures for data updates.

Illustrative controls implementation across data management lifecycle

The view below illustrates the data controls embedded into the various data lifecycle stages from creation to the usage in risk data models, along with the examples of underlying data systems or technology applications.

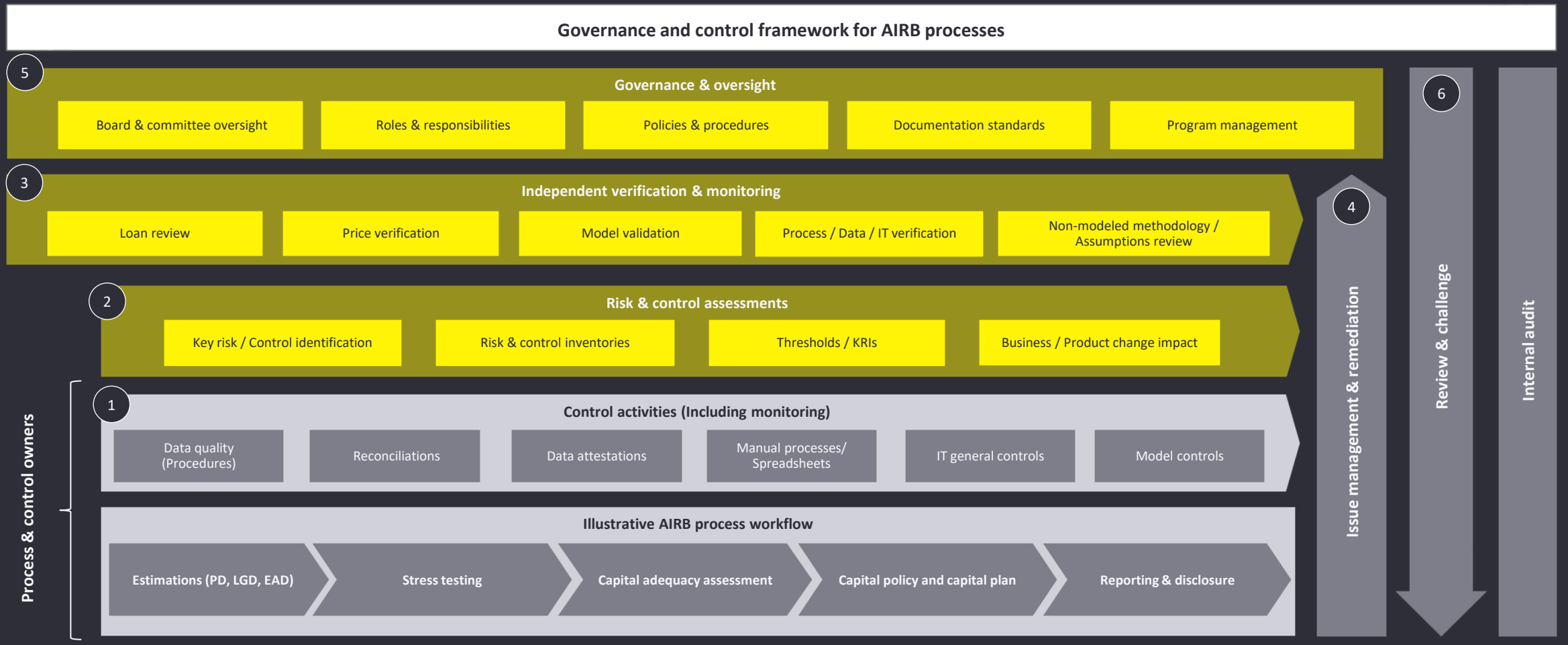
Controls Legend	
DQ1	Data element identification and prioritization
DQ2	Data quality checks
DQ3	DQ certification of production data
DE1	Trusted source designation
DE2	Manual data input controls
DA1	Data Lineage
DA2	Metadata capture
DA3	DQ attestation of model data
DP1	Data processing checks
DP2	Data feeds to EDW reconciliation with loan extract/product files.
DP3	Product balance in EDW reconciliation to accounting sub-ledger file
DP4	Adjustment / Correction to data in EDW
DU1	EUC (End User Computing) Monitoring
DU2	Access control on data entry/updates



5 | Appendix

Recommended governance and controls framework

Below is EY's recommended governance and controls framework. The section highlighted in green outlines the design and implementation process for data, IT and model controls.



BCBS 239 Principles' take on data controls

BCBS 239 Principles[1] outlines the set of principles to solidify institutions' risk data aggregation and risk reporting capabilities to enhance risk management and decision-making processes in banks.

Below is a table listing the key principles in BCBS-239 Principles on data controls.

#	BCBS 239 principle number (paragraph number)	Paragraph description
1	2 (34)	Roles and responsibilities should be established for ownership and quality of risk data for both business and IT functions. The owners (business and IT), in partnership with risk managers, should ensure there are adequate controls throughout data lifecycle. The role of the business owner includes ensuring data is correctly entered by front office, kept current and aligned with data definitions, and ensuring that RDARR practices are consistent with firms' policies.
2	3 (36.a)	Controls surrounding risk data should be as robust as those applicable to accounting data
3	3 (36.b)	Where a bank relies on manual processes and desktop applications (e.g. spreadsheets, databases) and has specific risk units that use these applications for software development, it should have effective mitigants in place (e.g. end-user computing policies and procedures) and other effective controls that are consistently applied across the bank's processes
4	13 (78)	Supervisors should require effective and timely remedial action by a bank to address deficiencies in its risk data aggregation capabilities and risk reporting practices and internal controls.

1 BCBS 239 Principles

AIRB Data Maintenance Notes relating to data controls

OSFI's CAR guideline A-1 provides details on adopting the internal ratings based (IRB) approach for institutions. In conjunction with that approach, OSFI's AIRB Data Maintenance Notes[1] outline the various requirements that institutions should satisfy if they are adopting the IRB approach to calculate capital for credit risk.

Below is a table listing the key paragraphs in AIRB Data Maintenance Notes[1] on data controls.

#	AIRB paragraph number	AIRB data requirement
1	1(b)	Senior management should establish an enterprise-wide data management framework defining, where appropriate, the institution's policies, governance, technology, standards and processes to support the data collection, data maintenance, **data controls** and distribution of processed data, i.e., information.
2	3 (d)	Institution's data processing should establish adequate **controls** to ensure processing by authorized staff acting within designated roles and established authorities.
3	3 (e)	Institution's data processing should institute appropriate **change control procedures** for changes to the processing environment, including, where applicable, change initiation, authorization, program modifications, testing, parallel processing, sign-offs, release, library controls.
4	4 (b)	Institutions should ensure that access controls and data/information distribution are based on user roles/responsibilities and industry best practices in the context of effective segregation of duties, "need to know", as validated by institutions' internal compliance and audit functions.

1 Data Maintenance at IRB Institutions

Authors

Vishal Gossain

Partner

Risk Consulting, EY Canada

vishal.gossain@ca.ey.com

Anil Sood

AI Governance and Model Data Management Lead

Financial Services Risk Management,

EY Canada

anil.sood@ca.ey.com

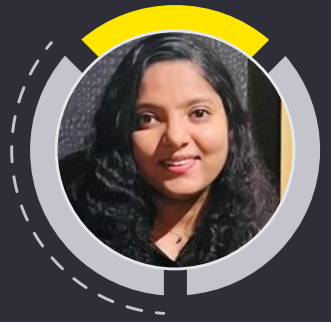
Ishant Arora

Manager | Risk Consulting

Financial Services Risk Management,

EY Canada

ishant.arora@ca.ey.com



Gauri Rajgopal

Senior | Risk Consulting

Financial Services Risk Management, EY Canada

gauri.rajgopal2@ca.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

ey.com/ca