Data Governance Glossary – Key Terms & Definitions

Term	Term Definition
Critical Data Elements	– Critical data elements (CDEs) are data attributes (e.g., a column in a database table or a field in a file/report) used to run the Bank and are **critical to the decision-making process** of one or more functions – CDEs represent "**the data that is critical to success**" in a specific business area (line of business, shared service, or group function) – CDEs are the **core building blocks of data governance**. The Data Governance function is responsible for the identification and framework for managing CDEs
Data Lineage	– Data lineage is the **documentation of a critical data element's origin**, what happens to it, and where it moves over time to the point of final consumption – Data lineage **gives visibility to trace errors back to the root cause** in a data analytics process
Data Owner (1st Line of Defense)	– A **business or support person** who has administrative control over and has officially been designated as accountable for a specific information asset in a data set
Data Steward **(1st Line of Defense)**	– A **business or support person** appointed by functional area senior leadership to act as the hands-on resource within the business to create / manage critical data elements, report data quality issues, and to conduct other data governance responsibilities around control and use of data
Data Steward **(2nd Line of Defense)**	– A **Data Governance team member** responsible for collaborating with Data Owners and Data Stewards in the business and support areas of the Bank to provide clarity to Data Governance policies and standards and to drive overall data governance compliance
Internal Audit (3rd Line of Defense)	– An internal audit team member responsible for the periodic audit of the Data Governance policy and program. Internal audit will review the processes, and any related gaps will be identified as findings to be monitored and remediated
Data Custodian	– A Data Custodian is an **information technology (IT) person or a line-of-business representative** responsible for data assets from a technical perspective – A Data Custodian is responsible for the technical environment and database structure and the technical controls of data including security, scalability, configuration management, availability, audit trail, and the ongoing maintenance of technical standards and policies in coordination with IT and Information Security personnel

Data Governance Glossary – Key Terms & Definitions

Term	Term Definition
Data Dictionary	– Represents a **central repository for all critical data elements and information on the data (metadata)**, meaning the structure, quality, definitions, and usage of that data in key processes, reports, models and analytics
Data Quality Rule	– Logical rules that can be implemented to measure the "good quality" in the data – Can be applied to one or more critical data elements across one or more data quality control dimensions (e.g., data timeliness, data completeness and data reconciliation between systems)
Data Quality Issue	– A data quality issue represents any matter that causes the high quality of the data to be in dispute (i.e., the data is no longer fit for its intended use) – A data quality issue represents **a repeated event** impacting the accuracy, completeness and timeliness of the data shared between Data Providers and Data Consumers
Data Quality Issue Remediation Program	– Managed by the **Data Quality Issue Management Forum** comprised of representatives from business, support, IT, risk management and data governance areas – Represents a "best practices" process and operating model around the effective identification and resolution of systemic data quality issues resulting in ongoing financial and operational benefits to the Bank
Data Governance Committee	– The Data Governance Committee is accountable for setting the plans, objectives, priorities, and performance measures for the data governance effort – Oversees and evaluates the activities and the identification, monitoring and mitigation of the risks associated with the Bank's data governance program (including critical data elements, data strategy and management, data quality and lineage, data remediation, and data stewardship)

Data Governance Glossary – Key Terms & Definitions

Term	Term Definition
Change Impact Notification	– A methodology between Data Providers and Data Consumers for managing and communicating changes made to the availability, delivery and consumption of **Critical Data Elements (CDEs) within the data supply chain** – Represents any change to a system or process that affect CDEs, the data structure or how the data is provided at the point of consumption
Service Level Agreement	– A formal document between Data Providers and Data Consumers to address possible or known data issues impacting the timeliness, completeness and reliability of critical data required for key business processes, reporting, models and analytics
Data Domain	– Data Domains are the primary vehicle for assigning data management accountability. A Data Domain is a logical grouping of data, based on shared characteristics (e.g., retail banking data, customer and account data, etc.)
Authorized Data Source	– An Authorized Data Source (ADS) is a designated data provisioning point application and **single source** of Bank sanctioned physical data elements for a Business Data Domain. – Note: Not all data on the system is officially sanctioned; therefore, an ADS must indicate which physical data elements are authorized to be sourced from the ADS application
Data Governance Assessment	– A Data Governance Assessment is a standard process in organizations to determine the maturity of Business Area adoption of the data governance program. A periodic Data Governance Standards Assessment Scorecard will be issued for critical Bank functions with a **rating of Below, Meets, Above, or Exceeds Standards compliance levels**.