Global Data Governance Policy

Policy Owner: Enterprise Data Governance

Date of Revision: April 17, 2026

Revised Policy Effective Date

May 1, 2026

Policy Implementation Date

June 30, 2026

Table of Contents

1. Policy Statement 3
2. Scope 3
3. Roles and Responsibilities 3
4. Policy Details 9
5. Data Governance and Accountability 10
   5.2. Data Domains 11
   5.3. System of Record / Trusted Source of Distribution 11
   5.4. Sensitive Data Inventory 12
   5.5. Third-Party / Outsourcing Data Governance 12
   5.6. Data Dictionary 14
   5.7. Data Catalog 14
6. Critical Information Governance 15
   6.1. Critical Reports 15
   6.2. Critical Data Elements 16
7. Data Consumption and Lineage 16
   7.1. Data Consumption 16
   7.2. Data Lineage 17
8. Data Quality Management 17
   8.1. Data Quality Management 18
   8.2. Data Quality Exception Management 18
   8.3. Data Quality Issue Management 19
9. Projects with Data Impacts 19
   9.1. Projects with Data Impacts 19
10. Data Governance Oversight and Controls 20
   10.1. Data Governance Oversight 20
   10.2. Data Governance Controls 21
11. Key Term Definitions 21
12. Related Policies and Standards 23
13. Policy Administration 23
14. Review and Approvals 24
15. Enforcement and Audit 24
16. Revision and Approval History 24
17. Appendix: Data Risk Taxonomy 25

1. Policy Statement

State Street manages its data to support the realization of business objectives, to comply with related regulatory and contractual obligations, and to deliver strategic value to State Street's overall business. The Corporation has defined the Global Data Governance Policy to provide reasonable assurance that its data is of high quality and managed within a sound control environment. This policy sets forth specific data governance requirements and controls.

2. Scope

This Policy applies to all structured data sources[1] of State Street's business units and corporate functions as well as material legal entities for which State Street has effective control (collectively, "State Street"). All State Street material legal entities, business units, and corporate functions that produce, process, or consume data are in scope for compliance with this Global Data Governance Policy.

3. Roles and Responsibilities

Business units and corporate functions are accountable to manage and govern data owned by their organization. This section describes the key roles that are responsible for driving data management strategy, planning, execution and oversight within each business unit and corporate function:

1. Enterprise Data Governance
2. Material Legal Entity Data Governance
3. Head of Business Unit Data Management and Governance
4. Data Governance Lead
5. Business Data Owner
6. SSBI Business Data Owner (SSBI Only)
7. Critical Report/Metric Owner
8. Data Steward Lead (optional role)
9. Data Steward
10. Technical Data Steward
11. Information Technology Manager
12. Business Risk Manager

[1] Structured data sources include IT systems (e.g. databases, data extracts/feeds, APIs) and business intelligence dashboards and reports. Unstructured data is out of scope. Unstructured data is user-generated content with no pre-defined structure. Examples include file sharing systems (Network Attached Storage, OneDrive, Box) or collaboration tools (e.g., SharePoint, Teams, Confluence, Email). Unstructured data, although out of scope for this policy, must be managed and protected per the policies listed in Section 12.

Enterprise Data Governance	The centralized Enterprise Data Governance function is responsible for defining State Street's Enterprise Data Governance Policy, Standards, and data governance controls. The centralized Enterprise Data Governance function also provides guidance to business unit data management teams to support adoption of enterprise data governance standards leveraging enterprise data governance tools and best practices. Key responsibilities include: 1. Provide product management and implementation support for the enterprise data governance tools (e.g., Data Catalog) including creation of data governance implementation guidelines, training materials and Data Catalog user guide 2. Support business unit adoption of enterprise data governance policy, standards, leveraging enterprise data governance tools (e.g., Data Catalog) 3. Maintain enterprise data domain model and conduct data domain health assessment process to evaluate the relative health of existing data management practices for business applications where the data sub-domain information is currently managed. The data domain assessment also includes identifying recommendations for which business application should be designated as a System of Record or Trusted Source of Distribution. 4. Defines metrics to measure business unit progress implementing data management policy and standards and implement data governance metric dashboards. 5. Define data governance minimum control standards to be implemented by central data governance teams and federated business unit data governance teams. 6. Oversee the risk data aggregation and reporting framework and incorporate BCBS 239 requirements in the Data Governance Policy, standards, and controls including implementation of RDAR data governance metrics reporting.
Material Legal Entity Data Governance[2]	1. Perform Enterprise Data Governance mandate within the Legal Entity (LE) 2. Assume LE accountability for policy adoption and regulatory commitments 3. Ensure all group policies, standards and frameworks include LE requirements 4. Provide LE view of group metrics and report through LE data governance channels 5. Act as a liaison with regulatory bodies and internal Audit for data related LE audits, inspections and remediation of compliance gaps
Head of Business Unit Data Management and	The Head of Business Unit Data Management and Governance is the central point of contact for the business unit's data management

[2] As standard practice, global function owners implement data governance policy requirements for all global legal entities in which the business unit operates. In certain cases, a material legal entity may require a separate data governance function to be established within the material legal entity to meet regulatory requirements. This material legal entity data governance requirement is required for State Street Bank International GmbH. Any changes to material legal entity data governance scope shall be reviewed and approved by Data Governance Board.

Governance (Data Governance Board Member)	strategy planning and data management execution oversight. Key responsibilities include: 1. Engage business unit leaders to assign ownership and accountability for key data management functions (e.g., business data ownership, data stewardship, and data quality management.) 2. Oversight of material data risks and issues in coordination with Business process owners, Business data owners, Data Stewards and Business Risk Managers 3. Represent the business unit on the enterprise Data Governance Board to provide oversight of progress implementing Data Governance Policy/Standards and adoption of enterprise data governance technologies 4. Monitor business unit data management metrics to identify trends, evaluate business impacts and determine if management action is required to reduce data risk 5. Champion adoption of Authoritative Sources (e.g., Master Data Management) within the business unit to drive data management efficiency and improve data quality.
Data Governance Lead	The Data Governance Lead (DGL) directs the data governance execution within a business unit or corporate function. The business unit's DGL is responsible to manage the implementation of data governance policy, standards, and data governance controls for the business unit through proactive engagement with business unit Data Stewards, Business Data Owners, and technology partners to mitigate data risk. DGLs provide day to day leadership and oversight of the business unit's data stewardship activities. Responsibilities include: 1. Lead business unit data governance policy implementation in collaboration with the Chief Data Office, business unit Data Steward community and Business Data Owners. 2. Monitor data governance metrics and present periodic updates on data risks and data governance policy implementation status to Business Risk Committee and Data Governance Board. 3. Coordinate with Business Data Owners to assign Data Stewards / data experts to support execution of BU data governance activities 4. Guide the business unit data stewardship activities and help resolve data management challenges 5. Drive data quality issue resolution through collaboration with key stakeholders 6. Support strategic data-driven initiatives within the business unit including engagement with business unit IT partners to oversee IT project compliance with data governance policy and standards 7. Facilitate the execution of data governance control activities and required certifications in line with the frequencies defined in the Data Governance Policy and Standards Controls (Supplemental Document).

	8. Contribute to data governance policy updates and ongoing improvements to data governance controls
Business Data Owner	The Business Data Owner (BDO) has overall accountability for the meaning, content, quality and distribution of a particular data asset or data set. Responsibilities include: 1. Assignment of qualified data stewards, final approval of data definitions, Data Sharing Agreements and Critical Data Provider Consumer Agreements, data quality control oversight, and data quality issue/exception remediation. This includes ownership of their data assets and the responsibility to understand the data lineage in their business process, metrics, and reports. 2. Where data is received from a different business unit, the Business Data Owner is responsible for ensuring that Data Sharing Agreements and Critical Data Provider Consumer Agreements are in place that cover aspects such as data quality, provisioning times, change management, and issue management. 3. Business data ownership and accountability cannot be outsourced, even if processing is outsourced to an internal or external third party. 4. Business Data Owner must inform Data Consumers of planned changes to the data source that may impact processes. Business Data Owners must also notify data consumers if there are any data quality issues identified that could impact Data Consumers. 5. For CDEs associated with Critical Information (Critical Reports and Key Metrics), the Business Data Owner is accountable for ensuring appropriate definition, authoritative sourcing, and data quality control oversight.
SSBI Business Data Owner[3][4]	The SSBI Business Data Owners (BDO) hold overall accountability within SSBI for the meaning, content, quality, and distribution of their respective business unit data assets and data sets to downstream systems, EUDTs and Reports / Metrics, as well as accountability for the data flow from its origin in a System of Record (SoR), especially if SoR is owned outside of SSBI, to its final point of consumption. This includes accountability for the accuracy, completeness, and timeliness of critical data elements.

[3] SSBI refers to State Street Bank International GmbH. The SSBI Business Data Owner role described in this section is SSBI-specific and does not apply to other State Street legal entities.
[4] As standard practice, global function owners implement data governance policy requirements for all global legal entities in which the business unit operates. In certain cases, a material legal entity may require a separate data governance function to be established within the material legal entity to meet regulatory requirements. This material legal entity data ownership and data governance requirement is required is currently limited to State Street Bank International GmbH. Any changes to material legal entity data governance scope shall be reviewed and approved by Data Governance Board. Refer to the Material Legal Entity Data Owner Guideline published on the Enterprise Data Governance Site for implementation guidance.

	Please refer to Material Legal Entity Data Owner Guideline for additional details.
Critical Report/Metric Owner	Critical Report/Metric owner is a senior manager that is the accountable owner of a Critical Report or Metric that is deemed critical and is accountable to ensure that the Critical Report / Metric is compliant with the applicable global data governance standards. The Critical Report/Metric Owner must assign a person responsible for executing the data governance activities for the Critical Report or Key Metric. The Critical Report or Key Metric Owner is also responsible to define the data sourcing requirements and transformation business rules required to produce the aggregated data needed to produce the Key Metric or Critical Report and the associated data aggregation data quality controls required to verify the accuracy and completeness of the aggregated data set. Refer to the Critical Information Governance Standard for detailed roles and responsibilities related to Critical Report/Metric data governance.
Data Steward Lead	Data Steward Lead is an optional role implemented in certain business units who act as subject matter experts with respect to data governance policy requirements, standards, and controls. The Data Steward Lead is the first point of contact for Data Stewards within their business unit or corporate function. Working together with the Data Governance Lead, they ensure that the Data Governance Policy is adhered to and executed as required, where applicable.
Data Steward	Data Stewards are subject matter experts for certain data sets typically aligned with business applications. Data Stewards maintain business metadata within the Data Catalog to enable a common understanding of data context, meaning and lineage. Data Stewards also support the Business Data Owner to document data management controls related to data quality and data use. Responsibilities include: 1. Partner with the Business Data Owner to: a. Maintain data dictionary to ensure data context and meaning is clear to Data Consumers and other stakeholders b. Manage Data Provider/Consumer relationships and confirm that data is fit for purpose c. Engage Business Data Owners to verify that operational controls (business and IT) are implemented and fully documented to mitigate data quality risks 2. Partner with Technology Manager and IT data experts to: a. Document technical metadata and associate physical data structures to business data element definitions within the Data Catalog b. Ensure that application data lineage (inputs, outputs) is accurate and updated in the Data Catalog c. Participate in data integration projects to ensure appropriate data is used, data quality controls are implemented, and the Data Catalog is updated

	3. Drive resolution of data quality issues and exceptions by collaborating with Business Data Owners, technology experts or other key stakeholder and subject matter experts Note: For non-CDE data elements, these activities and responsibilities are encouraged but are not required by this Policy.
Technical Data Steward	Technical Data Stewards have expertise on system data architecture, data models and data integration for specific systems or data assets that they are assigned to support. Technical Data Stewards support Data Stewards by providing technical support needed to support the cataloging of application metadata. Examples of business application metadata include data model, data dictionary, data location, data integration interfaces, file and report layouts and system metadata connectivity points to enable discovery of application metadata within the Data Catalog. Technical Data Steward is responsible to execute the following data governance requirements: 1. Provide application database connection details to be updated in Collibra to enable system metadata scanning process 2. Capture system data dictionary details in the Data Catalog and validate accuracy 3. Provide technical details needed to capture technical data lineage information in the Data Catalog (where required) and validate accuracy and completeness of the data lineage within the Data Catalog 4. Support implementation and documentation of technical data quality controls (including automated Data Quality Rules where applicable) within the system for inclusion in the consolidated CDE data quality control inventory. 5. Support execution of Critical Data Provider Consumer Agreements by enabling creation and maintenance of CDE technical lineage (where required) and communicating technical changes that occur and may impact CDE lineage or related controls. Note: The Technical Data Steward will be defaulted to the IT Manager assigned to the application in the Application Inventory (AIW). Optionally, the IT Manager can choose to delegate the application Technical Data Steward role to another member of the IT team.
Information Technology Manager	Information Technology (IT) Managers, in collaboration with the Data Steward(s), are responsible for ensuring the execution of data governance tasks with respect to project planning and completion. This includes development projects and BAU changes and enhancements. IT project plans must include applicable data governance tasks as required to comply with data governance policy and standards. If the IT Manager determines that the project has no data governance impacts, the business unit Data Governance Lead

	(DGL) must be consulted to confirm the project has no data governance requirements. IT Managers (or delegate) must provide support to Business Data Owners and Data Stewards with respect to the cataloging of application data by providing information on data element location, lineage, file and report layouts and connectivity points to enable discovery of application metadata. IT Manager must also ensure that application details are accurately documented in the Application Inventory (AIW). IT Managers must ensure that Technical Data Steward is allocated to support data management activities that are required to comply with the Data Governance Policy. This includes system data SMEs needed to effectively execute the following data governance requirements: 1. Capture system data dictionary details in the Data Catalog and validate accuracy 2. Capture data lineage information in the Data Catalog (where required) and validate accuracy 3. Document technical data quality controls implemented within the system for inclusion in the consolidated CDE data quality control inventory, where applicable
Business Risk Manager (BRM)	Business Risk Management supports their first line businesses / corporate functions to manage their data management risk, by supporting and advising on establishment of a control environment and provide periodic testing of first line owned Key Controls in Archer in accordance with the FLOD Assurance Standard to verify that the data management controls are effectively implemented within the business unit/corporate functions. BRM shall provide oversight of Data Quality Issues/Exceptions and include periodic Data Quality Management reporting within the Business Risk Committee materials as provided by Business Unit Data Governance teams and their periodic update to Business Risk Committees (or equivalent Data Governance oversight forums).

4. Policy Details

The Enterprise Data Governance organization has issued this Policy with input from Data Governance Board members and material Legal Entities to direct and enforce effective data management at State Street. The core objectives are to:

1. Define business unit and corporate function accountabilities as owners of their respective data and information, its movement and its use
2. Establish joint accountabilities for information technology leads with business unit and corporate functions in managing data and the associated data controls

3. Establish standard Data Domains to position data for enterprise use and to enable cross-functional issue resolution
4. Enforce transparency of key data flows, quality, meaning, location and use across the enterprise
5. Ensure proper data quality management practices to mitigate risks of inaccurate data leading to misinformed analyses, reporting, decisions, or operational losses
6. Ensure data is appropriately managed given its uses and flows across the organization
7. Ensure consumption of the right data for the right purpose
8. Enable consistent data management, standardization, integration, and consumption across the enterprise to efficiently, and accurately perform required business activities

This Global Data Governance Policy establishes requirements related to:

1. Data Governance and Accountability
2. Critical Information Governance
3. Data Consumption and Lineage
4. Data Quality Management
5. Projects with Data Impacts
6. Data Governance Roles and Responsibilities
7. Data Governance Oversight and Controls

5. Data Governance and Accountability

5.1.1. Business units and corporate functions must define clear accountability, controls, and governance for managing their organization's data. Data ownership is fundamental to successful data governance. Business data ownership must be assigned for all data. An important responsibility of the Business Data Owner is to ensure that the authoritative sources and authorized distributors of their data are identified, and consumption is governed. The Business Data Owner must provide reasonable assurance that the data drawn by its Data Consumers is fit-for-purpose by engaging Data Consumers to understand how data is being used.

5.1.2. When a recurring data transfer is implemented to support a business process, the Data Consumer Data Steward must create a Data Sharing Agreement and obtain approval from Business Data Owner prior to the development, distribution, or consumption of any new or modified data transfers between applications to verify that both the Data Provider and Data Consumer mutually agree that the data transfer is fit for purpose.

5.1.3. IT Manager must be assigned to each application/data environment to provide required IT support to business unit and corporate functions so that they have full transparency into the data architecture, system data model, and technical data lineage.

5.2. Data Domains

Effective data management requires all stakeholders to have a clear and consistent understanding of the meaning of data. Data Domains are logical groupings of data that are organized by data subject (e.g., Client, Security Master, Lending Transactions).

5.2.1. Enterprise Data Governance maintains the Enterprise Data Domain Model as core component of the Data Catalog.

5.2.2. Business units, corporate functions, and IT utilize the Enterprise Data Domain Model to categorize data that they produce and consume into standard Data Domains to consistently support data management and use throughout the organization.

5.2.3. Business unit data governance teams, supported by IT, can request updates to the Enterprise Data Domain Model as needed by engaging the Enterprise Data Governance team to ensure that the Enterprise Data Domain Model appropriately describes data ingested, created and consumed throughout the enterprise.

5.3. System of Record / Trusted Source of Distribution

5.3.1. Business units and corporate functions must consume data from authoritative sources. An authoritative data source is a system or data repository that has been determined to be a reliable and accurate data source for defined Data Domains or specific data elements, as applicable. A System of Record (SoR) is an authoritative data source containing the original version of data, captured either via manual data entry, systematic data creation/generation, or received from an external data source.

5.3.2. A System of Record must have internal controls in place to ensure that the data is processed and validated such that the data meets the required data quality dimensions of accuracy, completeness, and timeliness for use. Refer to the Data Quality Management section for additional information.

5.3.3. In some cases, a Trusted Source of Distribution (TSD) may be used to aggregate and/or distribute data. A TSD must have internal controls implemented to provide reasonable assurance that the copy of data stored or distributed by TSD is consistent with the SoR data.

5.3.4. The Data Governance Board provides oversight of applications designated as authoritative data sources (e.g., SoR or TSD) for defined Data Domains.

5.3.5. The SoR/TSD inventory must be approved annually by the Data Governance Board.

5.3.6. If a business unit identifies a key business function or critical report that is consuming data from a non-authoritative data source, then they must document the use of a non-authoritative source as a data risk and report this data risk to the business unit Data Governance Board Member to evaluate the risk level and business impact.

5.3.7. The Data Governance Lead of the business unit consuming the data will ensure that the data consumer documents the use of a non-authoritative data source as a self-identified data risk and either defines a remediation plan or obtains risk acceptance approval.

5.3.8. The Enterprise Software Development Lifecycle (eSDLC) framework must have proper controls and governance to ensure the development life cycle adheres to the SoR and TSD requirements.

5.4. Sensitive Data Inventory

5.4.1. Business units and corporate functions must identify the sensitive data that is processed or stored within their organization.

5.4.2. Business units must maintain a sensitive data inventory within the Data Catalog. The sensitive data inventory identifies the business applications where sensitive data is processed and stored within their business unit and which sensitive data categories are included in their applications. Identification of applications that contain sensitive data is essential to inform the implementation of sensitive data protection information security controls defined in the Information Protection Standard, as well as the Global Privacy and Personal Data Protection Standard. Sensitive data categories are defined and maintained in the Sensitive Data Category User Guide, which also details Collibra implementation approach.

5.4.3. Applications that contain sensitive data must be appropriately classified in the Data Catalog and associated to the applicable sensitive data categories.

5.4.4. Identifying these high-risk data assets that contain sensitive data elements shall be used to prioritize implementation of data protection controls.

5.4.5. Refer to the Global Privacy and Personal Data Protection Standard managed by the Global Privacy Office for additional requirements related to personal data and Records of Processing Activities (RoPA).

5.5. Third-Party / Outsourcing Data Governance

State Street uses third-party service providers and outsourcing arrangements to support its business, material legal entities, and its global operations.

5.5.1. Critical data or sensitive data that is provided by, processed by, or stored by third-party service providers or cloud service providers must meet minimum data governance

requirements regardless of whether the data is stored or processed internally or externally. Minimum data governance requirements for business units that utilize third-party service providers include:

1. Assign Business Data Owners and Data Stewards responsible to govern the data processed by the third-party
2. Identify the data domains processed by or accessed by the third-party
3. Determine whether a third-party system is a System of Record or Trusted Source of Distribution for specific data domains
4. Catalog any inbound or outbound data transfers between the third-party service provider and any other State Street system or other third-party systems (E.g., data traceability diagram)
5. Identify and catalog any sensitive data categories processed by or stored by the third-party
6. Identify and catalog any Critical Data Elements processed by or stored by the third-party
7. Define data element definitions for all Critical Data Elements processed by or stored by the third-party
8. Document any data sharing agreements and data use restrictions, where applicable
9. Document data quality controls and data quality exception management procedures for any Critical Data Elements.

5.5.2. The business unit Data Governance Lead and the Engagement Manager of the associated third-party engagement, with support from Third Party Risk Management (TPRM), Enterprise Data Governance, and IT Manager (where applicable), should document any third-party service providers that are non-compliant with minimum data governance requirements. Any such findings must be managed in accordance with the Third-Party Risk Findings Management Standard.

5.5.3. If an outsourcing engagement involves a third-party providing, processing, or storing critical data or sensitive data, then applicable due diligence must be completed to verify that the service provider's controls meet State Street's data governance and information security standards. These standards are designed to mitigate risks relating to data quality issues or the potential loss, alteration, destruction, or unauthorized disclosure of any State Street sensitive data. Identification of required due diligence and distribution and review of responses will be completed as part of the TPRM process.

5.5.4. In addition, the contract/agreement must follow the Vendor Contracts Requirement Standard, which includes a requirement to define the locations where data will be processed, stored,

and accessed by the third-party provider or cloud service provider and various other requirements.

Refer to the Third-Party and Outsourcing Risk Management Policy and Standards managed by the Third-Party Risk Management (TPRM) organization for additional details.

5.6. Data Dictionary

5.6.1. Data Stewards must maintain the application data dictionary with precise business definitions for all data elements classified as Critical Data Elements (CDEs), with approval of the Business Data Owner, to establish a shared understanding of the business meaning of data elements processed and stored within all new or updated system development projects.

5.6.2. Data element should be defined in context of the business process in which the data is created or ingested.

5.6.3. Applications that consume data from other applications should adopt the data element definitions from the source system where the data element is created to avoid having inconsistent data element definitions.

5.6.4. Data Dictionary must be defined and maintained in the Data Catalog for all data elements classified as a critical data element.

5.6.5. Given data structure complexity within the applications, IT Managers (or Technical Data Steward) must work with business Data Stewards to capture clear definitions for business data elements included in the data dictionary.

5.7. Data Catalog

The Data Catalog is the global repository for managing information about data assets to enable effective data governance and to help promote efficient data reuse. The Data Catalog is the data management knowledge base to capture information about Data Domains, business ownership of data assets, Authoritative Sources (e.g., SoR or TSD), Critical Reports, Data Dictionary, sensitive data identification and critical data identification, data traceability/lineage, and Data Sharing Agreements.

5.7.1. Data Stewards and IT Manager (or Technical Data Steward) must actively maintain the Data Catalog for data assets that they are assigned to govern.

5.7.2. System metadata must be ingested into the Data Catalog, for critical data, to be used by Data Stewards to associate physical data structures (APIs, schema/table/columns, report attributes, data files) with the business metadata (e.g., Business Owner, data definitions, Critical Data Element tagging).

5.7.3. Certain systems may be exempt[5] from Data Catalog metadata ingestion due to technical limitations, or the system being deemed low risk or not applicable for data governance. System metadata exceptions must be tagged in the Data Catalog and approved by the Data Governance Board.

5.7.4. IT Managers (or Technical Data Stewards) need to provide appropriate support to ensure system metadata ingested is accurate and complete.

5.7.5. Where manual metadata capture is required, IT Manager (or Technical Data Steward) must support the business Data Steward to update the required metadata within the Data Catalog.

6. Critical Information Governance

The information and data that is essential to the firm's management decision making, and risk management and regulatory reporting must be identified and cataloged as a priority for data governance execution. Critical Reports, Key Metrics and Critical Data Elements (CDEs) are designated as critical information to identify data elements that require a heightened level of data governance and internal control. Identification of CDEs enables Business Data Owners and Data Consumers to execute end-to-end governance over data elements that have a material impact on the accuracy and completeness of Critical Reports.

6.1. Critical Reports

6.1.1. Business units and corporate functions must maintain the Critical Report Inventory in the Data Catalog. Critical Reports contain critical information including Key Metrics that are distributed on a recurring basis to:

1. State Street Board of Director Committees and Subcommittees
2. Corporate Risk Committees (e.g., Management Risk and Capital Committee, Operational Risk Committee, Asset Liability Committee, Credit and Market Risk Committee)
3. Regulators for Tier 1 Critical Regulatory Reports

6.1.2. State Street material legal entities, business units or corporate functions may identify Critical Reports that do not meet the criteria above, but the report requires rigorous data governance to meet regulatory expectation or management requirements.

6.1.3. Business units and corporate functions must re-certify their business unit's Critical Report Inventory on a semi-annual basis to confirm that their Critical Report metadata defined in the Data Catalog is accurate and complete.

[5] Exemptions from automated metadata ingestion do not exempt a system from data governance requirements; required metadata must be captured via approved manual processes.

6.2. Critical Data Elements

6.2.1. Business units and corporate functions that consume data must identify Critical Data Elements (CDEs) that are essential to produce a Critical Report, Key Metric, or other critical functions with heightened regulatory oversight (e.g., Financial Crimes Compliance regulatory requirements).

6.2.2. CDEs must be managed as a priority to avoid misinformed management decisions, incorrect regulatory reports, or other regulatory compliance issues.

6.2.3. CDEs must be defined in the Data Catalog and associated to an Authoritative Data Source. Business data lineage associations between Critical Report attributes and CDE data sources must also be maintained in the Data Catalog.

6.2.4. Critical Data Provider Consumer Agreements must be documented and approved by Provider Business Data Owner and Data Consumer (consuming Business Data Owner or Critical Report Owner or Key Metric Owner). Critical Data Provider Consumer Agreements must be reviewed on an annual basis and re-approved to ensure these agreements are maintained accurately.

Refer to the Critical Information Governance Standard for additional details.

7. Data Consumption and Lineage

7.1. Data Consumption

7.1.1. Business units and corporate functions that consume data from other business units must ensure that their data usage is consistent with the expectations and intentions of the System of Record Business Data Owner. Understanding the source of data and the movement of data from source to consumption provides confidence in the data used in key business processes, analytics and reports. For complex applications and data aggregation-related processes, it is essential to understand and document how the data moves from system-to-system and how the data is aligned to business definition and standard meaning.

7.1.2. Data transfers between applications (i.e., application-to-application lineage) must be documented in the Data Catalog for all business applications and approved by Data Stewards from both the Data Provider and Data Consumer to confirm that the data transfer is effectively controlled and fit for purpose.

7.1.3. A Data Sharing Agreement must be approved prior to the distribution, or consumption of any new or modified data transfers between applications.

7.1.4. Business Data Owners must identify and document any applicable data use restrictions to inform data sharing agreements and must review these restrictions with Data Consumers.

7.1.5. Data Consumers must indicate agreement to adhere to the data usage restrictions. Common sources of data use restrictions include third party data licensing agreements, contractual agreements, or local laws and regulations.

7.1.6. Data assets or specific data attributes that are subject to data use restrictions must be identified to mitigate the risk of a breach in contract, which may result in fines, penalties, or reputational damage.

7.2. Data Lineage

7.2.1. Data element lineage must be updated in the Data Catalog for CDEs to fully document the movement of each CDE from its designated authoritative source (System of Record, governed EUDTs, or governed manual sources) to the point of consumption including all data aggregation processes and final report production and distribution. Data lineage provides visibility into where data is stored, where it came from, and where it is being consumed.

7.2.2. CDE data lineage captured in the Data Catalog must be verified by the Business Data Owner (or subject matter expert delegate) to confirm that the CDE data lineage is accurate and complete. Understanding the data lineage enables efficient investigation of data errors and impact analysis for planned changes to data sources or applications involved in the data supply chain. It is important for Data Providers to establish a communication process to notify Data Consumers of changes to their data sources, which may impact downstream processes.

7.2.3. IT teams must provide documentation to specify system data inputs/outputs (i.e., data feed, data extracts, and reports) to capture technical data lineage information in the Data Catalog.

7.2.4. If CDE data aggregation process for a Critical Report relies on an end user developed tools (EUDT) or a manual process, then the EUDT and/or Manual Process must be added to Collibra for inclusion in the Critical Report data lineage and the EUDT must be governed in accordance with the EUDT Standard.

8. Data Quality Management[6]

A well-controlled data supply chain is fundamental to ensuring accuracy, completeness and timeliness of data that is critical to business operations, decision making, and risk management.

[6] The formal requirements for managing the data quality of Critical Data Elements (CDEs) are defined in the Data Quality Management Standard.

8.1. Data Quality Management

8.1.1. Business Data Owners with the support of IT Managers are accountable for managing the quality of their data to meet the requirements of Data Consumers and any applicable regulations (e.g., BCBS 239).

8.1.2. Data Consumers are responsible to document their Data Quality needs and expectations in the Critical Data Provider Consumer Agreements and obtain agreement with the Provider to mutually agree that the data is fit for use.

Data Quality rules and controls are required at each stage of the data lineage from source system where data is created or ingested through the various processing steps through to data consumption or report generation.

8.1.3. For Critical Data Elements, Data Quality rules and corresponding controls are required at each stage of the data lineage—from the point where data is created or ingested through processing steps to the point of consumption or report generation—to verify accuracy, completeness, and timeliness.

8.1.4. The Business Data Owner of critical data, with support of IT Manager, must ensure that data quality controls are effectively implemented at appropriate points along the data lifecycle including data capture, processing, and data distribution process.

8.1.5. The data quality internal controls must address the relevant data quality dimensions[7] and must cover all critical data elements.

8.1.6. The Business Data Owner, with support of IT Manager, of critical data should maintain documentation to evidence that data quality rules and controls fully cover all CDEs and all applicable data quality dimensions.

8.2. Data Quality Exception Management

8.2.1. Data Consumers are responsible for reporting any identified data quality exceptions to the Data Provider so the data problem can be investigated and remediated in the authoritative source, as far upstream in the data supply chain as possible and data quality operational controls can be enhanced as needed.

8.2.2. Data quality exceptions identified by a Data Consumer that impacts CDE data quality must be tracked in the centralized data governance platform.

8.2.3. CDE data quality exceptions must be investigated to determine the root cause, and remediation actions must be documented in the centralized data governance platform to evidence resolution of the CDE data quality exception.

[7] Data quality dimensions include accuracy, completeness and timeliness. Refer to the Data Quality Management Standard for additional details.

8.2.4. If a Data Provider identifies a data error after the data has been distributed, then the Data Provider must notify Data Consumers and other impacted stakeholders about the data error to enable consumers to evaluate the impact and determine appropriate mitigating actions to address the data error.

Refer to the Data Quality Management Standard for additional information.

8.3. Data Quality Issue Management

A Data Quality Issue is a data-related deficiency in the design or effectiveness of a control or operating environment that could lead to undesired risk exposure, or noncompliance, or potential noncompliance, with applicable policies, standards, procedures or legal/regulatory requirements.

8.3.1. Data Quality Issues (as defined in the Data Quality Management Standard) must be logged and managed in the Global Issue Management Tool (Archer) in accordance with the Global Issue Management Standard. The Data Quality flag must be populated in Archer for Data Quality Issues.

9. Projects with Data Impacts

9.1. Projects with Data Impacts

9.1.1. All projects or change initiatives that impact data management, data processing or storage, and data transfer, distribution or reporting must adhere to the applicable data governance requirements and controls as defined in the Data Governance Policy and related standards. This applies to projects executed by business units, governed via New Business Product Review and Approval process (NBPRA), and IT projects, governed via Software Development Lifecycle (SDLC) Standard.

9.1.2. Project leads (business or IT) must engage the relevant Data Governance Lead and Data Steward(s) to identify and plan the required data governance tasks and execute data governance deliverables.

9.1.3. For technology projects, the Enterprise Software Development (eSDLC) framework must include data governance tasks and artifacts to evidence that data governance requirements are effectively embedded in the eSDLC framework, supporting tools and the overall system development control environment.

9.1.4. Business Data Owners, Data Governance Leads, and Data Stewards must be engaged by the project lead when the project begins.

9.1.5. The IT Manager (or delegate) must capture the required data governance tasks and artifacts/deliverables in the project plan or project management tool and ensure completion.

9.1.6. The IT Manager must consult the business unit Data Governance Lead or the assigned Data Steward to request approval that all required data governance tasks and artifacts are executed accurately and completely.

9.1.7. During the Solution Architecture approval tollgate (e.g., Architecture Review Board process or equivalent), the Business Data Owner (or delegate) must review and approve the project data architecture, and the business unit Data Governance Lead (or delegate) must review and approve the data governance scope (including confirmation where the initiative is determined to have no data impact / no data governance requirements).

9.1.8. Certain technology projects may be exempt from data governance if project does not involve processing or storage of any structured data. IT projects deemed to be exempt from the data governance policy requirements must be approved by the business unit Data Governance Lead.

9.1.9. Any incomplete data governance requirements for non-exempt IT projects should be documented and reported to IT management, business unit Data Governance Lead and Business Risk Manager prior to the system production release to evaluate the impact and relative risk of the incomplete data governance deliverables.

10. Data Governance Oversight and Controls

10.1. Data Governance Oversight

10.1.1. The Data Governance Board (DGB) provides oversight of Enterprise Data Governance capabilities and adoption of the Global Data Governance Policy. The DGB is chaired by the Head of Enterprise Data Governance, and it includes senior manager representatives from each business unit and corporate function.

The DGB is responsible to:

1. Set data governance priorities, such as regulatory initiatives
2. Approve policies and standards and monitor their adoption
3. Drive data governance maturity and best practices in the business units and corporate functions
4. Review data quality metrics to identify trends and impacts at the enterprise level; Respond to data quality escalations
5. Provide a forum for the resolution of escalated, complex, or important data-related issues

10.1.2. The DGB reports to the Enterprise Data Management Committee (EDMC). The EDMC is responsible to:

1. Set enterprise-wide data management strategies and practices

2. Oversee execution of data management programs, operating model, and risk reduction
3. Serve as escalation for material and emerging enterprise-wide data management issues
4. Ensure alignment of data governance with corporate and business unit strategies
5. Ensure clear business data ownership and associated accountabilities
6. Advise on the vision, objectives, priorities, and goals of Enterprise Data Governance

10.2. Data Governance Controls

10.2.1. Business units and corporate functions must implement data governance controls to mitigate data management risks.

10.2.2. Standard data governance controls have been defined by the central enterprise data governance team to be adopted across business units and corporate functions to mitigate data risk(s) and provide reasonable assurance for achievement of the organization's strategic objectives including reliability and integrity of financial and operational information.

10.2.3. The detailed control objectives and control descriptions, including ownership and execution frequency, are documented in Data Governance Policy and Standards Controls (Supplemental Document), which accompanies this Policy. The supplemental document consolidates Enterprise Data Governance controls, Business Unit Data Governance controls, and IT Data Governance controls.

10.2.4. This Policy establishes the requirement to implement and maintain these controls. Evidence of control execution must be retained in accordance with record-retention requirements and made available for audit and supervisory review, as applicable.

11. Key Term Definitions

Please refer to the Global Technology Services Glossary of Terms <*Link*>

Principle	Rationale
Authoritative Data Source	A system or repository that has been determined to be a reliable and accurate data source for a specific type of information.
Critical Data Element	A data element that is deemed materially important to a Critical Business Service, Critical Report, or Key Metric
Critical Business Services	Services that State Street provides which, if significantly disrupted, could cause harm to financial markets, clients, or the firm. Such services are determined to be critical business services. Critical Business Service details are defined and maintained by the Enterprise Resiliency Office in

Principle	Rationale
	collaboration with Business Data Owners and operational risk management teams.
Critical Report	Critical Reports contain Critical Information including Key Metrics that are distributed on a recurring basis to: • State Street Board-level Risk Committees and Subcommittees • State Street material Legal Entity Board-level Risk Committees • Regulators for Tier 1 Critical Regulatory Reports
Data Catalog	The Data Catalog enables understanding and management of data and information. It is a repository that enables data governance by storing and managing metadata such as data meaning, ownership, use, and lineage. The Data Catalog is maintained by federated data stewardship teams.
Data Consumer	A process, application or stakeholder that receives or uses data from a Business Data Owner.
Data Lineage	Information about the movement and transformation of data from a point of origin to its destination or point of consumption and use.
Business Data Owner	The person with overall accountability for the meaning, content, quality and distribution of a particular data set.
Data Sharing Agreement	An agreement that sets out a common set of rules between the Business Data Owner and Data Consumer that establishes terms and restrictions of the use of consumed data.
Critical Data Provider/Consumer Agreement (P/C Agreement)	A documented agreement between Business Data Owners (Data Provider) and Data Consumer that defines the critical data being provisioned across the Critical Report and Key Metric supply chain, including the Data Consumer's Data Quality requirements that the Data Provider agrees to satisfy.
Derived Data	Data that are created from other data or data that is calculated.
Key Metric	A Key Metric is a measurable and traceable financial or non-financial data point (e.g., number, count, percentage, dollar value, etc.) that is contained within a Critical Report and that is deemed material to the report communication objective. Key Metric(s) are automated and/or manual and are created utilizing one or more system applications and/or end user computing tools. Key Metric(s) are produced on a recurring basis
Metadata	Metadata is defined as 'data about data'. It includes meaning/definition, use, and Lineage. Metadata is captured in the Data Catalog.
System of Record	A data source containing the original version of data, captured either via manual data entry, systematic data creation/generation, or received from an external data source
Trusted Sources of Distribution	A system used to aggregate and/or distribute data that has been designated as an authoritative data provisioning point for a specific Data Domain or data element(s)

12. Related Policies and Standards

Refer to Corporate Policy and Standard Center for related Policies and Standards <Site link>. Related guidance documents may be maintained outside of CPSC by the document owner.

DOCUMENT TITLE
Global Critical Information Governance Standard
Global Data Quality Management Standard
Data Governance Policy and Standards Controls (Supplemental Document)
Sensitive Data Category User Guide
Global Privacy and Personal Data Protection Standard
Global Cyber Security (GCS) Policy
Information Protection Standard
Internal Control Standard
Issue Management Standard
The Operational Risk Incident Standard
Data Incident Policy
Record Retention and Destruction Policy
Identity and Access Management Standard
Third-Party and Outsourcing Risk Management Policy
Third-Party and Outsourcing Risk Lifecycle Management Standard
Third Party Risk Findings Management Standard
Vendor Contracts Requirement Standard
FLOD Control Assurance Standard
New Business and Product Policy
Enterprise Software Development Lifecycle Standard
End User Developed Tool Standard
Material Legal Entity Data Owner Guideline

13. Policy Administration

Enterprise Data Governance is responsible for the interpretation and administration of this Policy. This Policy shall be posted to the Corporate Policy Center. Enterprise Data Governance, in conjunction with the Data Governance Board and Data Governance Leads, are responsible for communicating this Policy across the enterprise.

Regulated material legal entities within State Street may be required to develop additional policies to meet local regulatory requirements. These policies must be consistent with this global policy and no less restrictive. In cases where exceptions are required due to local regulatory requirements, business requirements and/or technology limitations, such exceptions must be documented and escalated to the Data Governance Board for approval.

14. Review and Approvals

Enterprise Data Governance is responsible for review and revision of this Policy and the associated implementation plan, subject to Data Governance Board approval. This policy and implementation plan are subject to review on an annual basis, or otherwise as needed.

15. Enforcement and Audit

Compliance with this Policy and any related standards and procedures may be reviewed by State Street at any time. Corporate Audit performs independent reviews of the Enterprise Data Governance capability and reports to the Examining and Audit Committee of the Board of Directors and Senior Management.

16. Revision and Approval History

Revision Date	Policy Owner	Document Revision Description	Approvals
11/30/2017	J. Looney	Initial Policy Creation	Data Governance Board
11/26/19	D. Lorenzen	Annual Policy Updates	Data Governance Board
4/8/2020	D. Lorenzen	Annual Policy Updates	Data Governance Board
6/25/2020	D. Lorenzen	Annual Policy Updates	Data Governance Board
11/8/2021	D. Lorenzen	Annual Policy Updates	Data Governance Board
10/24/2022	D. Lorenzen	Annual Policy Updates	Data Governance Board
2/28/2024	J. Doray	Policy was re-written to consolidate relevant information from the Data Governance Framework document, clarify existing policy requirements, incorporate references data governance control standards and add a few new policy requirement topics including: - Data Domains - Sensitive Data Inventory - Third-Party / Outsourcing Data Governance - Elaboration/updates to data consumption and lineage - Elaboration/updates to data quality management - Elaboration/updates to roles and responsibilities	Data Governance Board Technology Risk Committee
4/3/2025	J. Doray	• Added new role for Material Legal Entity Data Governance (e.g., SSBI) • Updated Business Data Owner and Business Risk Manager descriptions and responsibilities (sec. 3) • Revised Sensitive Data Inventory policy description (sec. 5.7) • Revised DQ Issue Management policy description (sec. 8.3)	

Revision Date	Policy Owner	Document Revision Description	Approvals
		• Added requirement review Critical Data Provider Consumer Agreements annually and re-approved (6.2.4) • Referenced New Business and Product Policy and Enterprise Software Development Lifecycle Standard (sec. 12) • Added reference to Sensitive Data Implementation Guideline (sec. 5.4.5) • Added Material Legal Entity Data Owner Guideline footnote in the Data Owner role and responsibility section and sec. 12.	
4/17/2025	J. Doray	• Added footnotes under the Material Legal Entity Data Governance Role and Business Data Owner roles to indicate that enhanced Material Legal Data Governance and Data Ownership changes are currently limited to the State Street Bank International GmbH legal entity.	
5/15/2025	J. Doray	• Replace the referenced document Incident Capture & Management Policy for the Operational Risk Incident Standard	
3/15/2026	J. Doray	• Removed Sensitive Data Category examples (sec. 5.7) • Data Quality dimensions aligned with Data Quality Management Standard (sec. 8) • Added Data Governance Board Control to Enterprise Data Governance Controls (sec. 10.2.2) • Removed and Revised Business Unit Data Governance Controls (sec. 10.2.3) • Added SSBI Business Data Owner role (sec. 3)	Data Governance Board
4/17/2026	J. Doray	• Removed detailed control descriptions from Section 10.2 and consolidated them into a separate Data Governance Policy and Standards Controls (Supplemental Document). • Removed the Sensitive Data Guidelines reference and replaced it with the Sensitive Data Category User Guide.	Data Governance Board

17. Appendix: Data Risk Taxonomy

Data governance policy and controls are intended to mitigate data risk related to the following data risk types.

#	Data Risk Type	Description
1	Data Accountability	The risk that ineffective data ownership or oversight leading to ineffective data management, loss, reputational damage, or inappropriate use of data assets.
2	Data Use / Fit for Purpose	The risk that data sourced for a specific purpose does not meet the definition and requirements of that purpose. Also includes the risk that data provided for a specific purpose is consumed for a purpose outside its intended use without the knowledge of the data owner / provider.
3	Data Quality	The risk of the erosion of data accuracy, completeness and timeliness, leading to misinformed analyses, decisions, and reporting.
4	Data Mastering	The risk that duplicated data appears across multiple systems or platforms, creating varying sources of truth, potentially leading to misinformed or incomplete reporting, analyses, and decisions.
5	Data Architecture	The risk that the enterprise data architecture does not enable consistent data management, standardization, integration, and consumption across the enterprise to efficiently, and accurately perform required business activities.

End of document