Global Data Governance Policy

Policy Owner: Enterprise Data Governance and Management
Last Updated: October 2022

Policy Effective Date

August 1, 2020

Revised Effective Date

November 1, 2022

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 implemented an Enterprise Data Governance Framework ('Framework') to ensure its data is of high quality and managed within a sound controls environment. The Framework defines maturity levels for data governance and this policy sets forth specific compliance requirements for data governance.

Scope

This Policy applies to all wholly owned State Street legal entities, Business Units and Corporate Functions globally. This Policy will apply to any Joint Venture where State Street holds a controlling interest. Please see the implementation plan for details.

Policy Details

Background:

The Enterprise Data Governance and Management organization (EDGM) has issued the Policy and associated Framework to guide and enforce effective data management at State Street. This establishes requirements related to:

- Identification of Key Data and Information
- Business Accountability and Context

- Lineage
- Systems of Record/Trusted Sources of Distribution
- Data Quality Oversight
- Data Governance Integration with State Street's various Systems Development Life Cycles (SDLC)

Existing policies and standards which relate to this Policy include the Global Privacy and Personal Data Protection Standard, Corporate Information Security Policy, the Identity and Access Management Policy, the Critical Information Standard, the Data Quality Management Standard and the Data Incident Policy.

Data Governance Maturity Model:

The Framework defines a maturity model consisting of multiple levels. The Maturity Model establishes clear, consistent and actionable processes that deliver meaningful data governance outcomes for Business Units and Corporate Functions, supporting the firm's Risk Excellence objectives and overall Corporate Strategy. The Maturity Model is comprised of distinct maturity levels and core governance attributes that span maturity levels.

Maturity Model Policy Requirements:

There are multiple dependencies that must be met before the Policy can be fully implemented and these are listed in Appendix 1. Under this Policy, compliance requirements for each Business Unit or Corporate Function must be met within the timelines agreed in the implementation plan. The requirements are as follows:

1) Business Units and Corporate Functions will achieve a minimum of Foundational Level of governance for all Applications. All Tier 0 and Tier 1 applications that have not yet met Foundational governance will be the highest priority.
2) Business Units and Corporate Functions must execute Key Information Governance, including Key Reports, Key Metrics and Critical Data Elements identification and governance, as detailed in the Data Governance Framework and Critical Information Standard.
3) Business Units, in collaboration with their IT or technology implementation partners, must govern projects and technology work streams that result in a data impact/changes to the application(s) in scope for the project. New applications will concentrate on governing key information, such as Key Metrics and CDEs as well as consumable data (i.e., Data Files, BI Reports). Project teams will use standard IT development methodology, as detailed in the System Development Lifecycle process.
4) Business Units, in collaboration with IT, must ensure that a Data Consumer/Provider authorization is in place prior to the development, distribution or consumption of any new or modified data between applications within the enterprise data supply chain. In cases where it is determined that no governance is required for the project, the Data Governance Lead (DGL) will need to review the scope and purpose of the project and provide sign off that they agree that no governance is needed for the project. Where possible, the data must be sourced from a System of Record or Trusted Source of Distribution. The only exception to the requirement for a Provider/Consumer Acknowledgement form is where the Business Owner of the Providing Application and Consuming application is the same, or where their direct managers are the same. In this case, the Data Governance Lead has the discretion to decide whether or not to use the form.

5) Business Units or Corporate functions may require that data providers execute on data governance requirements for specific special projects or Regulatory Requests as defined by the data consumers. Delivery dates for this work will need to be agreed upon by both the Provider and Consumer; should there be no agreement on delivery dates, the issues will be escalated to both the Provider and Consumer Data Governance Board (DGB) members for resolution. Prioritization of any work will need to take into consideration any existing deliverables as well as ongoing or new Regulatory Initiatives.

The policy is designed to mandate specific minimum governance requirements for the firm and to establish a consistent set of enterprise-wide data governance capabilities. Business Units or Corporate Functions have the flexibility to exceed the minimum governance requirements at their discretion. The use of corporate data governance catalog is required as part of the implementation of this policy.

Required data governance tasks associated with policy compliance are specified within the Framework document.

Accountability for Data:

Accountability for data rests with the Business Unit and Corporate Function owners. Within the Enterprise Data Governance Framework, the roles of Business Owner and Data Steward are used to identify the individuals associated with these accountabilities.

Business Owners are aligned with business lines and corporate functions. They are accountable for driving the adoption of Enterprise Data Governance within their areas and ensuring that their data adheres to Global Data Governance and Management policy.

Data Governance Leads are Individuals who are responsible for executing on Data Governance Activities for their Business Unit/Corporate Function. The Data Governance Lead partners with the Data Governance Board Member, Data Steward Lead and Data Stewards to drive adoption across their Business Unit/Corporate Function.

Data Steward Leads are subject matter experts with respect to data governance processes and procedures. The Data Steward Lead is the first point of contact for Data Stewards within their Business Unit/Corporate Function. Working together with the Data Governance Lead they ensure that Data Governance Policy is adhered to and executed on.

Data Stewards ensure that data is fit for use at a specific location or place of rest. Typically, a place of rest is an application, database or table. Data Stewards provide expertise to create better transparency around data meaning, quality, lineage and use.

Business Risk Management Executives (BRME) oversee the effectiveness of data controls as part of the FLOD controls and testing practices. They ensure data governance controls are appropriate and report Data Quality exceptions to the Business Risk Committees.

Information Technology Managers are responsible for assuring the applications within their scope of responsibility are represented accurately in the Application Inventory Warehouse. They also provide support of

Business Owners, Data Steward Leads 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 an application. IT Delivery Managers, in conjunction with the Data Steward(s) are also responsible for the enforcement of the execution of Data Governance Tasks with respect to project development and completion; this includes BAU changes and enhancements.

Maturity Model Attribute Overview:

Taken together, the measures outlined within the Data Governance Maturity Model will lead to stronger data integrity and a greater assurance that data is being sourced and consumed appropriately to each business purpose.

Identification of Critical Information: The data and information that are most material to the firm's business operations, decision making, and management of risks must be identified to prioritize governance implementation (i.e., Key Reports, Key Metrics, Critical Data Elements). The application of effective data governance and management activities will improve Data Quality and ensure appropriate use of data.

Business Accountability and Context: While ownership ultimately lies with the legal entities that source, originate or create data, accountability for the quality and appropriate use of data lies with the Business Units and Corporate Functions that own the applications and processes that manage data as it flows throughout the enterprise. Applications that are deemed as being Systems of Record or Trusted Sources of Distribution will be identified and described as such by each business unit owning the application to enable consumers to source reliable and trustworthy data.

Data Lineage: Data Lineage documents the movement of data from its System of Origin to the various information assets and business processes that consume the data through a series of provider / consumer relationships. The documentation of these associations formally establishes data provider and consumer relationships as well as reveals dependencies on data for key information. The availability of this information is imperative to ensure the appropriate root cause and resolution of data exceptions.

Systems of Record/Trusted Sources of Distribution: A System of Record (SOR) is an application that stores data that is non-redundant, verified, deemed critical to a business unit or corporate function and is as close to the point of data creation / origination as possible. In some cases, a System of Record is not able to distribute data downstream in a consumable format. When this occurs, a Trusted Source of Distribution (TSD) is created. Trusted Source of Distribution is an application, database, or repository that contains a copy of one or more System(s) of Record or is responsible for gathering data from one or more System(s) of Record. This may be done to normalize the format for Information Delivery purposes when a System of Record is not able to distribute downstream in a consumable format. In addition, a TSD may also be used for information gathering purposes, containing data sets from multiple Systems of Record. The data in the TSD is the raw data set from the SOR and is not transformed or altered; the only exception would be to normalization of the naming convention of the data elements to align with enterprise taxonomies. An application, repository or database can also be SOR if

new data elements are created from the SOR data. Data Consumers will be required to source data from a SOR or TSD (provided a SOR or TSD has been identified), heightening the importance of a high level of data quality, clear definitions and accurate lineage of data maintained within the applications. The governance of SOR and TSD provides heightened assurance over data governed in these applications.

There is currently a multi-year program underway, the Domain Assessment and Data Taxonomy Workstream, to apply a standard assessment survey across the domains to identify the candidate applications to be defined as Systems of Record. Additionally, a set of Common Business Terms will be established and defined for each domain. Going forward, a Domain Owner will be established and responsible for managing and overseeing different aspects of the domain across the company. For further information, please refer to the System of Record and Trusted Source of Distribution Standard.

Data Quality Exception Tracking: Effective Data Quality management depends on the implementation of operational data quality controls and the reporting of data quality exceptions experienced by data consumers. Data Quality exception tracking will expose common data exceptions as well as loss or risk items caused by these exceptions. For further information, please refer to the Data Quality Management Standard.

Data Quality Oversight: A well-controlled data supply chain is fundamental to ensuring reliability and availability of data that is critical to operations and influences business decisions. Providers are accountable for their data and are responsible for meeting the Data Quality expectations of their consumers and regulatory requirements. Consumers are responsible for raising Data Quality exceptions and working with the Provider to remediate the exceptions identified. Providers and Consumers are both accountable for identifying and correcting Data Quality exceptions as far upstream in the supply chain as possible. For further information please refer to the Data Quality Management Standard.

For further guidance on the expectations of Incidents and Issues, including those related to Data Quality, please refer to the Incident Capture & Management Policy and the Issue Management Standard, respectively.

Implementation:

Oversight

- The Data Governance Board (DGB) will provide policy adoption oversight, escalation support, change control – e.g., application governance, Key Reports, DQ exceptions etc., and ongoing effectiveness assessment and challenge across implementation activities as defined below. The DGB is a sub-committee of the Executive Data Management Committee (EDMC). The EDMC is responsible to:

    - Set firm-wide data management strategies and practices
    - Oversee execution of data management programs, operating model, and risk reduction
    - Serve as escalation for material and emerging enterprise-wide data management issues

Application Governance

- Business Owners must ensure that all Applications they own maintain a Foundational Level of Governance as described in the Data Governance Framework.

Critical Information Governance

- Business Units and Corporate Functions are accountable to self-identify and catalog in the Data Governance Catalog all Key Reports and Key Metrics annually. Business Units and Corporate Functions must execute Critical Information governance in accordance with the Data Governance Framework and Critical Information Standard. The Key Reports and Key Metrics will be reported to the DGB annually. Any aged tasks over 90 days, will be escalated to the DGB quarterly. The inventory of Key Metrics and Key Reports can be found in the Data Governance Catalog. Note: The governance of Key Reports/Key Metrics includes the adherence to the Critical Information Standard which can be found on the Corporate Policy and Standard Collaborate site.

- It is the responsibility of the providing Data Steward and Data Governance Lead to drive the implementation of the required data governance tasks once alerted by the consumer. These tasks include, but are not limited to, the governance of Data File, BI Reports, Database Columns and Database Tables. The consumer of the data for the Key Report/Key Metric, in conjunction with their BU Data Steward/Data Governance Lead, is required to define the full project scope or required data with the data providers and impacted Data Governance Leads to collectively agree to a timeline for the deliverables. Execution conflicts should be escalated between Data Governance Leads. In the event that effective resolution cannot be obtained, issues will be escalated to the appropriate Data Governance Board members as well as to EDGM.

IT Development Initiatives

To address the need to sustain progress made in managing data within the State Street enterprise, IT development initiatives with a data impact must be governed according to the requirements set forth in the Data Governance Framework, the Software Development Lifecycle (SDLC) requirements and the SDLC Playbook. It is the responsibility of the Data Steward and the IT Development Teams to ensure the Data Governance tasks are executed accurately and completely. Application or Domain Data Stewards will work with the project team to identify all data governance tasks and artifacts that will be required for a project; where necessary, they will consult with the DGL to ensure all tasks and artifacts are identified. The Project Manager will capture these tasks and artifact deliverables in the project plan and ensure completion. Any outstanding or late items will be escalated to the Data Governance Lead.

- Note: There are pre-requisites to these activities. See Appendix 1 for the pre-requisites for the governance of IT Development Initiatives.

- Accountability for ensuring execution of data governance requirements for IT development initiatives resides with both the Business and IT Owners who will be held accountable through the SDLC and Tollgate process. Procedures for the enforcement of development practices related to data governance

are outlined further in State Street's development methodologies. These procedures are designed to match the scope and scale of development being performed. Note: See Appendix 1 for the prerequisites for the governance of IT Development Initiatives.

Advanced Governance Requirements

- Business Units or Corporate Functions may self-determine governance requirements beyond those noted above based on their business objectives or regulatory requirements.

- It is the responsibility of the providing Business Unit or Corporate Function Owner to drive the implementation of the required data governance. The consuming Business Owner is required to review governance compliance requirements and define the full project scope with data providers and impacted Data Governance Leads to attain commitment to adhere to timeline requirements. Execution conflicts should be escalated to determine appropriate prioritization, Business Owner organization to Business Owner organization, with input from the Data Governance Lead, for resolution as a first action. In the event that effective resolution cannot be obtained, the Business Owner's Data Governance Board member should be informed to enable escalation to the DGB.

Implementation Clarification:

Data Governance requirements are independent and not sequential. Business Units and Corporate Functions are required to determine applicability of each requirement individually and comply as necessary.

The compliance requirements are designed to mandate specific minimum governance standards for the firm, to establish a consistent enterprise-wide data governance competency. Business Units or Corporate Functions have the flexibility to exceed the minimum governance requirements at their discretion. The use of corporate data governance tools for cataloging is required as part of the implementation of this policy. The Data Governance Toolkit
provides the capability for users to log Data Quality Exceptions and remediation plans, but Business Units and Corporate Functions may utilize other tools available to their organizations. The tool suite is reviewed and updated on an ongoing basis. EDGM welcomes specific and beneficial feedback and suggestions for enhancements from all users of the tool suite.

Required data governance responsibilities are specified within the Data Governance Framework document.

Implementation Support:

As Policy owner, EDGM provides implementation support services to Policy recipients, in accordance with corporate policy standards. EDGM also provides adoption compliance tracking metrics to the DGB across all levels as required.

EDGM provides the required tools, and in conjunction with Data Governance Leads, Data Steward Leads and BU Data Stewards, provides execution support including training, catalog management, change control, escalation and reporting on policy compliance.

Management Oversight / Committee Structure:

Senior Management provides oversight of Enterprise Data Governance capabilities and adoption of the Global Data Governance Policy through the Data Governance Board (DGB). There is representation from each Business Unit and Corporate Function on the DGB. The DGB Chair is also the Head of EDGM. The DGB reports into the Enterprise Data Management Council (EDMC).

Policy Administration and Communication

EDGM is responsible for the interpretation and administration of this Policy. This Policy shall be posted to the Corporate Policy and Standard Center Collaborate Site and distributed to Data Governance Board Members. Data Governance Board members are responsible for ensuring adherence to this Policy and for further distribution of this Policy to other relevant stakeholders and throughout their business units to facilitate a corporate wide awareness of Data Governance requirements.

EDGM, in conjunction with the Data Governance Board and Data Governance Leads, are responsible for communicating this Policy across the Enterprise. Training shall be provided firm wide, as developed by EDGM, on the Policy and what it means to the individual stakeholder.

Regulated 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 DGB for approval.

Review and Approvals

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

Enforcement and Audit

Compliance with this Policy and any related 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.

Key Term Definitions

Application Lineage	Application to Application Lineage is created when one application systematically (ETL, Direct DB connections, data files etc.) sends information to another application.
Data Lineage	Documentation of the sequence of movement and/or transformation of data as it flows between the consumer and the provider(s).
Data Quality	The definition and application of controls to ensure that data is fit for use.
Key Application	Key Applications are a point in time designation, which were previously defined as applications that serve a critical enterprise purpose or hold sensitive data. Examples include those categorized as Tier 0/1, Interagency, Crown Jewel, as well as additional drivers (e.g. regulatory) as assessed by the DGB. This designation is used to reference the first set of governed applications. Any application that now serves a critical enterprise purpose or holds sensitive data should be prioritized for governance in the current year.
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 Key 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
Key Report	Key Reports contain Critical Information including Key Metrics that are distributed on a recurring basis to: • State Street Board of Director Committees and Subcommittees • Corporate Risk Committees (e.g., Management Risk and Capital Committee, Operational Risk Committee, Asset Liability Committee, Credit and Market Risk Committee) • Regulators for Tier 1 Critical Regulatory Reports
Software Development Lifecycle (SDLC)	A conceptual model that describes the stages involved in an information system development project, from an initial feasibility study through maintenance of the completed application Systems.
System of Origin	The System of Origin refers to the source of a data element. The data value may have been created by an individual in the business process, manually captured in a Document, sourced manually or captured electronically from an external provider.
Systems of Record	Stores data that is non-redundant, verified, is associated with an application that is deemed critical to a business unit or corporate function and is closest to the point of data creation/origination
Trusted Sources of Distribution	A Trusted Source of Distribution presents a copy of one or more System(s) of Record or is responsible for gathering data from one or more System(s) or record and formatting it for Information Delivery purposes.

Related Policies, Procedures, Standards and Guidance

- State Street Enterprise Data Governance Framework
- State Street Data Adjustment Standard
- State Street Critical Information Standard
- The Data Quality Management Standard
- Corporate Information Security Policy
- Corporate Information Security Controls Manual
- Identity and Access Management Policy
- Identity and Access Management Controls
- Global Privacy and Personal Data Protection Standard
- Data Incident Policy
- Incident Capture & Management Policy
- Issue Management Standard
- Incident Capture and Management Guidelines
- Record Retention and Destruction Policy - Global

Appendix 1

Pre-Requisites for the Governance of IT Development Initiatives:

Reporting must be developed to allow the business to have a view into all the current and proposed IT Projects and BAU projects for the current year for both Agile and Waterfall methodologies. The GTS SDLC Office is working to provide the reports needed for all projects across all methodologies.

Revised processes and standards for the integration of governance within IT projects must be developed and distributed to all impacted parties. All Agile Labs, Waterfall Projects, BAU Labs/Projects and Small Request Projects must adhere to the standards put forth by IT to incorporate Data Governance into the Project Lifecycle. The GTS SDLC Office is working to create and distribute these standards to the appropriate teams.

Pre-Requisites for general Policy execution: Training materials (including Job Aids, Data Steward Forum presentations, and training modules) will be provided to IT Project and Application Support staff to support the execution of the policy requirements.

Shared services support will be provided to BU's and CF's to support execution of the policy.

Revision History

Version	Title	Date	Submitted By	Reviewed By	Revision Notes:
1.0	Global Data Governance Policy	8/16/17	J. Looney	Data Governance Board	
2.0	Global Data Governance Policy	11/26/19	D. Lorenzen	Data Governance Board	Annual Policy Updates
3.0	Global Data Governance Policy	4/8/2020	D. Lorenzen	Data Governance Board	Annual Policy Updates
4.0	Global Data Governance Policy	6/25/2020	D. Lorenzen	Data Governance Board	Annual Policy Updates
5.0	Global Data Governance Policy	11/8/2021	D. Lorenzen	Data Governance Board	Annual Policy Updates
6.0	Global Data Governance Policy	10/24/2022	D. Lorenzen	Data Governance Board	Annual Policy Updates

End of document