# Information Technology General Controls

## SOC 1® Report
## October 1, 2022–September 30, 2023



STATE STREET.

# Information Technology General Controls

## SOC 1® Report
## October 1, 2022–September 30, 2023

This report is confidential and its use is limited to State Street, the clients of State Street and their auditors.

## Table of Contents

# Section I

Building a better
working world

**Ernst & Young LLP**
200 Clarendon Street
Boston, Massachusetts
02116-5072

Tel: 617 266 2000
Fax: 617 266 5843
www.ey.com

# Independent Service Auditor's Assurance Report

To the Management and Board of Directors of State Street Corporation

## Scope

We have examined State Street Corporation's (State Street's) description entitled "Description of State Street's Information Technology General Controls System" (Description) throughout the period October 1, 2022 to September 30, 2023 of its system (System) for supporting the processing user entities' transactions and the suitability of the design and operating effectiveness of controls described therein to achieve the related control objectives stated in the Description (Control Objectives), based on the criteria identified in the *Assertion Provided by State Street* (Assertion). The Control Objectives and controls included in the Description are those that management of State Street believes are likely to be relevant to user entities' internal control over financial reporting, and the Description does not include those aspects of the System that are not likely to be relevant to user entities' internal control over financial reporting.

The Description indicates that certain Control Objectives can be achieved only if complementary user entity controls assumed in the design of State Street's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

State Street uses various subservice organizations, as described in Section III A6 *Subservice Organizations* to provide certain application development, change management, hosting and data center services. The Description includes only the Control Objectives and related controls of State Street and excludes the control objectives and related controls of subservice organizations. The description also indicates that certain Control Objectives specified by State Street can be achieved only if complementary subservice organization controls assumed in the design of State Street's controls are suitably designed and operating effectively, along with the related controls at State Street. Our examination did not extend to such complementary controls of subservice organizations and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The information included in Section V *Other Information Provided by State Street* is presented by management of State Street to provide additional information and is not a part of State Street's Description. Such information has not been subjected to the procedures applied in our examination of the description of the System and of the suitability of the design and operating effectiveness of controls to achieve the related Control Objectives, and accordingly, we express no opinion on it.

### State Street's responsibilities

State Street has provided the accompanying Assertion about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives. State Street is responsible for preparing the Description and Assertion, including the completeness, accuracy and method of presentation of the Description and the Assertion, providing the services covered by the Description, specifying the Control Objectives and stating them in the Description, identifying the risks that threaten the achievement of the Control Objectives, selecting the criteria stated in the Assertion, and designing, implementing and documenting controls that are suitably designed and operating effectively to achieve the related Control Objectives.

### Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Our examination was also performed in accordance with International Standard on Assurance Engagements 3402, *Assurance Reports on Controls at a Service Organization*, issued by the International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's Assertion, the Description is fairly presented and the controls were suitably designed and operating effectively to achieve the related Control Objectives throughout the period October 1, 2022 to September 30, 2023. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- Performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls to achieve the related Control Objectives, based on the criteria in the Assertion.

- Assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related Control Objectives.

- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related Control Objectives were achieved.

- Evaluating the overall presentation of the Description, the suitability of the Control Objectives, and the suitability of the criteria specified by the service organization in the Assertion.

We are required to be independent of State Street to meet our other ethical responsibilities, in accordance with the relevant ethical requirements related to our examination engagement. We have complied with such independence and other ethical requirements and applied the AICPA's Statements on Quality Control Standards.

We apply International Standard on Quality Control I and accordingly maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

### Inherent limitations

The Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the System that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions in Information Technology General Controls services supporting the processing of user entities' transactions for the applications described in Section III B. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related Control Objectives, is subject to the risk that controls at a service organization may become ineffective.

### Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed in the Section IV *State Street's ITGC Control Objectives and Related Controls and Additional Information Provided by the Independent Service Auditor* (Description of Tests and Results).

### Opinion

In our opinion, in all material respects, based on the criteria described in the Assertion:

a. The Description fairly presents the System that was designed and implemented throughout the period October 1, 2022 to September 30, 2023.

b. The controls related to the Control Objectives were suitably designed to provide reasonable assurance that the Control Objectives would be achieved if the controls operated effectively throughout the period October 1, 2022 to September 30, 2023, and if subservice organizations and user entities applied the complementary controls assumed in the design of State Street's controls throughout the period October 1, 2022 to September 30, 2023.

c. The controls operated effectively to provide reasonable assurance that the Control Objectives were achieved throughout the period October 1, 2022 to September 30, 2023 if complementary subservice organization and user entity controls assumed in the design of State Street's controls operated effectively throughout the period October 1, 2022 to September 30, 2023.

## Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of management of State Street, user entities of State Street's System during some or all of the period October 1, 2022 to September 30, 2023, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Ernst & Young LLP

November 9, 2023

# Section II

State Street Corporation

State Street Financial Center
1 Congress Street
Boston, Massachusetts 02114-2010
+1 617 786 3000

www.statestreet.com

## Assertion Provided by State Street

We have prepared the description of State Street's Information Technology General Controls system entitled, "State Street's Information Technology General Controls ("ITGC") System" (Description) for supporting the processing user entities' transactions throughout the period October 1, 2022 to September 30, 2023 for user entities of the system during some or all of the period October 1, 2022 to September 30, 2023, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider the Description, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

State Street uses subservice organizations to provide application development, change management, hosting and data center services. The Description includes only the control objectives and related controls of State Street and excludes the control objectives and related controls of the subservice organization. The Description also indicates that certain control objectives specified in the Description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The Description does not extend to controls of the subservice organization.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of State Street's controls are suitably designed and operating effectively, along with related controls at the service organization. The Description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

a) The Description fairly presents the System made available to user entities of the System during some or all of the period October 1, 2022 to September 30, 2023 for processing their transactions as it relates to controls that are likely relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the Description:

   1) Presents how the System made available to user entities of the system was designed and implemented to support the processing of user entities' transactions, including, if applicable:

      - The types of services provided.
      - The procedures, within both automated and manual systems, by which those services are provided for user entities of the System.

- The information used in the performance of the procedures and supporting information; this includes the correction of incorrect information and how information is transferred to the reports prepared for user entities.
- How the System captures and addresses significant events and conditions.
- The process used to prepare reports and other information for user entities.
- Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
- The specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls.
- Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

2) Includes relevant details of changes to the System during the period covered by the Description.

3) Does not omit or distort information relevant to the System while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the System and their user auditors, and may not, therefore, include every aspect of the System that each individual user entity of the System and its user auditor may consider important in the user entity's own particular environment.

b) The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period October 1, 2022 to September 30, 2023 to achieve those control objectives, if subservice organizations applied the complementary subservice organization controls and user entities applied the complementary user entity controls assumed in the design of State Street's controls throughout the period October 1, 2022 to September 30, 2023. The criteria we used in making this assertion were that:

1) The risks that threaten the achievement of the control objectives stated in the Description have been identified by management of the service organization.

2) The controls identified in the Description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved.

3) The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

State Street
November 9, 2023

# Section III

# Description of State Street's Information Technology General Controls ("ITGC") System

## A. Overview

### 1. Scope of this Report

This report ("the Report") describes State Street Corporation's ("State Street" or "the Corporation") Information Technology General Controls System Supporting the Processing of User Entities' Transactions throughout the period October 1, 2022 to September 30, 2023 over physical security, logical access, change management, job scheduling and incident management, and backup and recovery processes and controls performed by State Street in support of the applications relevant to the following complementary State Street business control reports unless otherwise noted:

| | |
|---|---|
| Alternatives – Hedge (formerly known as International Fund Services) | ("AISH") |
| Alternatives – Private Markets (formerly known as Alternative Investment Solutions – Private Equity and Real Assets Fund Services) | ("AISPM") |
| French Fund Accounting | ("FFA") |
| Global Fund Accounting and Custody | ("GFAC") |
| Global Services – Taxation Services Australia | ("GS TSA") |
| Global Services – Unit Registry Australia | ("GS URA") |
| Institutional Transfer Agent | ("ITA") |
| Investment Manager Services – Enterprise | ("IMSE") |
| Kansas City Insurance Services | ("KCIS") |
| State Street Global Advisors | ("SSGA") |
| State Street GmbH-KVG Fund Accounting In-sourcing | ("SS GmbH-KVG") |
| State Street GmbH Succursale Italia's Fund Administration, Depositary Bank and Local Custody | ("SS GmbH-Italy") |
| State Street Retiree Services | ("SSRS") |
| State Street Transfer Agency – Hong Kong and Singapore | ("TA-HKS") |
| State Street Transfer Agency – Ireland | ("TA-Ireland") |
| SSTB Co., Ltd. Japan – Investment Manager and Insurance Outsourcing Services | ("SSTB IMIOS") |
| SSTB Co., Ltd. Japan – Trust Business and Standing Proxy Business | ("SSTB TBSPB") |
| U.S. Investment Services | ("USIS") |

In order to effectively interpret the applicability of the processes, controls and EY test results contained within this report, users should consider the following:

- The *Application Listing* in Section III B details all in-scope applications, related IT environment (data center location, operating system platform, database management system, access administration process and access recertification process) and corresponding complementary State Street report(s).
- Not all controls, processes or test results described in this report are applicable to each in-scope application and/or complementary State Street report. Users should review the *Application Listing* in Section III B as well as the *Deviation Summary by Complementary State Street Report* in Section IV C to determine applicability to the user.
- This report should be used in conjunction with the applicable complementary State Street report. The complementary State Street report contains detailed descriptions of the applications, along with the associated business process control objectives and operational controls relevant to transaction processing.

The Report is designed to provide information for use by State Street's clients and their independent auditors who audit the financial statements of an entity that uses State Street as a service organization. The Report is intended to focus on elements that may be relevant to the internal processes supporting State Street's information technology general controls for the in-scope applications described in Section III B.

This report is divided into five main sections:

- Section I contains the Independent Service Auditor's Assurance Report on the Description of State Street's Information Technology General Controls ("ITGC") System provided by Ernst & Young LLP, an independent registered public accounting firm (the global organization herein referred to as "EY").
- Section II contains the Assertion Provided by State Street.
- Section III A provides an overview of State Street; Section III B contains a listing of applications included in the scope of this report; Section III C includes a description of State Street's Information Technology General Controls processes.
- Section IV A details control objectives and related controls identified by State Street and a description of the tests of selected controls performed by EY and the associated results of the tests. Section IV B provides additional information provided by the independent service auditor. Section IV C contains a detailed Deviation Summary mapping of those deviations identified in Section IV A and the applicability to the complementary State Street reports.
- Section V contains other information provided by State Street, the service organization, including an overview of State Street's Business Continuity Planning and Privacy and Data Protection programs.

The scope of this report includes information technology controls provided by the Information Technology and Global Security divisions as well as support from Global Human Resource and Global Procurement Services.

Although the core services of the aforementioned State Street business control reports are not included in the scope of this report, management of these services are responsible for the implementation of corporate-wide programs within their business lines including identity and access management, business continuity and disaster recovery, contract compliance and oversight of vendor partners, as well as the implementation of, and compliance with, Corporate Policies and procedures. Refer to Section III B for a list of in-scope applications which are leveraged to deliver State Street's key offerings to Asset Managers, Asset Owners, Alternative Asset Managers, Insurance Companies, Official Institutions, Global Advisors and Global Markets.

## 2. State Street Overview

### Businesses and Organization

State Street Corporation, referred to as the parent company, is a financial holding company organized in 1969 under the laws of the Commonwealth of Massachusetts. For purposes of this report, unless the context requires otherwise, reference to "State Street" means State Street Corporation and its subsidiaries on a consolidated basis. State Street conducts its business primarily through its principal banking subsidiary, State Street Bank and Trust Company ("State Street Bank"). State Street Bank traces its beginnings to the founding of the Union Bank in 1792. State Street Bank's current charter was authorized by a special act of the Massachusetts Legislature in 1891, and its present name was adopted in 1960. State Street Bank operates as a specialized bank, referred to as a trust or custody bank, that services and manages assets on behalf of its institutional clients.

Including the U.S., State Street operates globally in more than 100 geographic markets. State Street's operations are organized into two lines of business: Investment Servicing and Investment Management, which are defined based on products and services provided. The results of operations for these lines of business are not necessarily comparable with those of other companies, including companies in the financial services industry.

*Investment Servicing*, through State Street Investment Services, State Street Global Markets and State Street Alpha, provides investment services for institutional clients, including mutual funds, collective investment funds and other investment pools, corporate and public retirement plans, insurance companies, investment managers, foundations and endowments worldwide. Products include: back office products such as custody, accounting, regulatory reporting, investor services, performance and analytics; middle office products such as investment book of record, transaction management, loans, cash, derivatives and collateral services, record keeping, client reporting and investment analytics; investment manager and alternative investment manager operations outsourcing; performance, risk and compliance analytics; financial data management to support institutional investors; foreign exchange, brokerage and other trading services; securities finance, including Prime Services products; and deposit and short-term investment facilities.

*Investment Management* provides a broad range of investment management strategies and products for its clients through State Street Global Advisors. State Street's investment management strategies and products for equity, fixed income and cash assets, including core and enhanced indexing, multi-asset strategies, active quantitative and fundamental active capabilities and alternative investment strategies span the risk/reward spectrum of these investment products. State Street's Assets Under Management ("AUM") is primarily weighted to indexed strategies. In addition, State Street provides a breadth of services and solutions, including environmental, social, and governance investing, defined benefit and defined contribution products, and Global Fiduciary Solutions. State Street Global Advisors is also a provider of exchange-traded funds ("ETF"), including the SPDR® ETF brand.

State Street's clients include institutional investors, such as mutual funds, collective investment funds, undertakings for collective investment in transferable securities, hedge funds and other investment pools, corporate and public retirement plans, insurance companies, official institutions, foundations, endowments, and investment managers. In both State Street's asset servicing and asset management businesses, State Street endeavors to attract institutional investors controlling large and diverse pools of assets, as those clients typically have the opportunity to benefit from the full range of State Street's expertise and service offerings. Approximately 43,000 employees are focused on providing state-of-the-art services.

### Financial Highlights

Total assets under custody and/or administration as of September 30, 2023, were $40.02 trillion, including assets under custody of $29.11 trillion, representing an increase of approximately 12.1% and 10.0%, respectively, from September 30, 2022. Total assets under management as of September 30, 2023, were approximately $3.9 trillion, an increase of 12.9% from September 30, 2022. As of September 30, 2023, State Street Corporation's consolidated total assets were $284.42 billion. Cash, liquid assets and other short-term investments, which have less credit risk and higher marketability than loan and other long-term assets, comprised approximately 29% of total consolidated assets. Loans, less allowance for credit losses, comprised approximately 12% of total consolidated assets. The short maturity structure of cash and money market assets enhances State Street's liquidity.

State Street manages its business to maintain high ratings on its debt, as measured by the major independent credit rating agencies. This not only minimizes borrowing costs, but also enhances State Street's liquidity by helping to ensure the largest possible debt market. As of September 30, 2023, State Street's senior debt was rated A by Standard & Poor's, A1 by Moody's Investor Services and AA– by Fitch, Inc.

### Regulation

State Street Bank is a state-chartered bank and a member of the Federal Reserve System ("the Fed" or "FED"). State Street Bank's operations are supervised and examined by its primary regulators, the Federal Reserve Bank of Boston and the Massachusetts Commissioner of Banks. In addition, State Street Bank is subject to the rules and regulations of the United States Securities and Exchange Commission ("SEC") applicable to custodians, fund accountants, administrators and transfer agents of regulated investment companies and as an issuer of registered securities. Records maintained on behalf of the registered investment companies are subject to SEC examination.

State Street Bank is subject to government regulations for insured depository institutions under the Federal Deposit Insurance Corporation Improvement Act ("FDICIA") of 1991 regarding internal controls over financial reporting and compliance with certain designated laws and regulations.

### Insurance Coverage

The Corporate Insurance Department within Enterprise Risk Management ("ERM") works with State Street management to evaluate and select insurance risk transfer coverage for State Street. All domestic insurers are rated by AM Best and have a rating of A– or better. State Street's global insurance program, as of September 30, 2023, is comprised of the following policies:

- Financial Institution Bond including Computer Crime Coverage
- Directors' and Officers' Liability
- Professional Liability
- Cyber/Network Security and Privacy Liability
- Property
- Casualty

### Standard of Conduct

The Standard of Conduct details the code of business conduct for State Street and all of its subsidiaries. The Standard of Conduct, together with policies that address specific topics or policies that are issued by individual business areas and corporate functions, establish a set of requirements and guidance regarding the way in which employees of State Street are to conduct themselves. Every employee is expected to remain informed about and to comply with the Standard of Conduct, related company policies and the regulatory and legal requirements that apply to State Street as a company and to each individual employee. The Standard of Conduct is described further in Section III A3 *State Street Governance and Structure – Corporate Compliance*.

### Regulatory Environment

As described above in the *Regulation* section of this overview, State Street is a highly regulated entity subject to reporting obligations to, and examinations by, federal and state regulatory agencies in the U.S. and local regulatory agencies in the international jurisdictions in which State Street operates.

### Financial Crimes Compliance

State Street and its subsidiaries are committed to combating money laundering, terrorist financing, and other illicit financial activity (collectively referred to as "financial crime") and complying fully with all applicable laws and regulations designed to combat financial crime in the jurisdictions in which it does business. State Street is also committed to complying with all sanctions that are legally binding on it and its business across all of the jurisdictions in which it operates.

State Street has appointed a Global Head of Financial Crimes Compliance Officer who leads a team of employees with experience in this area to oversee State Street's Anti-Money Laundering and Sanctions compliance program (the "Global AML and Sanctions Program" or the "Global Program"). State Street's Global AML and Sanctions Program is comprised of written anti-money laundering and sanctions policies, standards, procedures, internal controls and systems, which include but are not limited to the following: a customer identification program and procedures; procedures to collect and update, as appropriate, customer due diligence information; screening of customer and transactions against sanctions and other watch lists; processes to assess money laundering, terrorist financing and sanctions risks at the program, customer and product levels; processes and systems to monitor customer transactions and activity; processes and systems to identify and report suspicious activity; training of employees on AML and sanctions requirements; processes to retain required records; and regular independent testing conducted by Corporate Audit.

The Global AML and Sanctions Program is periodically evaluated, updated and enhanced in order to reflect changes to State Street business activities, as well as to ensure compliance with applicable supervisory standards and legal requirements. The global program is approved by the Board of Directors on an annual basis. State Street cooperates fully with law enforcement and regulatory investigations and inquiries.

Also included as part of State Street's Financial Crimes Compliance ("FCC") Program is the oversight of anti-bribery and corruption and fraud. The following policies are approved by the Core Compliance and Ethics Committee and the Global Financial Crimes Committee: Fraud Risk Management Policy; Global Gifts and Entertainment Policy; Global Anti-Bribery and Corruption Policy; and Global Political Contributions and Activities Policy.

### Risk Assessment

State Street has established a robust risk assessment process to identify and evaluate the full scale and scope of its exposures, to analyze how its business activities might evolve as economic and market conditions change, and to help ensure that State Street is operating within the risk appetite defined by the Board of Directors. The Material Risk Identification ("MRI") Process is one of State Street's primary risk identification programs and utilizes a bottom-up approach to identify State Street's most significant risk exposures across all on- and off-balance sheet risk-taking activities, including credit, market, liquidity, interest rate, operational/technology, fiduciary, business, reputational, and regulatory risks. The primary output from the program is a firm-wide Material Risk Inventory, which is a comprehensive list of the risks that could significantly impact State Street, irrespective of their likelihood or frequency. The material risks are reviewed by management and the Board of Directors on an annual basis to ensure that significant changes to the firm's risk profile are captured on a timely basis. In addition, the quarterly MRI updates focus on identifying emerging risks and triggering events that could cause State Street's exposures to materialize. The Material Risk Inventory forms a holistic view of the firm's risk profile and is used as a foundational element in State Street's risk management and capital planning processes. ERM, and State Street's control functions more broadly, are responsible for providing review and challenge during the risk identification process to ensure that they are effectively capturing all key risks to which the business is exposed.

#### Monitoring

State Street management is responsible for continuously monitoring risk exposure across the company and assessing the design and operating effectiveness of its controls. The monitoring process is accomplished through a variety of ongoing activities, including risk monitoring activities performed by the First and Second Lines of Defense (described in Section III A3 *State Street Governance and Structure*), operational event reporting, credit exposure reporting, key risk and performance indicator reporting, and consolidated risk reporting to senior management, oversight committees and the Board of Directors. Management also reviews the results of separate evaluations performed by regulators and Corporate Audit and takes appropriate action to remediate any identified issues. State Street's Board of Directors and senior management provide overall oversight and management review of operating performance. Risk management is a shared responsibility between the business units and ERM. State Street employs a three lines of defense model in which risk management is a shared responsibility between all lines of defense. Refer to the description of the three lines of defense in Section III A3 *State Street Governance and Structure – Enterprise Risk Management* for further details on State Street's approach to risk management and the related responsibilities.

#### Third-Party Risk Management

State Street leverages and relies on third-party providers for products and services to support its operations, services and initiatives. "Third-Party Provider" is broadly defined as any entity that has entered into a contractual relationship with State Street to support its business functions and activities. While using third-party services assists in obtaining necessary expertise, expanding product offerings, improving services and managing cost, it also introduces potential risks inherent with involvement of a third-party provider. Such risks need to be assessed prior to engaging with the third party and requires ongoing monitoring and management throughout the lifecycle of a third-party engagement. As a result, State Street has implemented a Third-Party Risk Management ("TPRM") program for assessing and managing risks associated with the use of third-party products and services throughout the engagement lifecycle in a manner consistent with compliance and regulatory requirements.

TPRM is managed within a governance structure that includes oversight from State Street's Board of Directors including the Technology and Operations Risk Committee, the Third Party and Outsourcing Risk Committee, and the three lines of defense as detailed in Section III A3 *State Street Governance and Structure – Enterprise Risk Management*. TPRM begins with an Inherent Risk Questionnaire ("IRQ") which must be completed by the

Business Unit Manager engaging the third party. The IRQ measures the level of inherent risk within a State Street function that is looking to leverage the products or services of a third party to support its business activities. Both the inherent risk rating for the product or service as well as the required due diligence to be performed on the proposed third party are driven by the level of inherent risk determined through the IRQ. The due diligence process includes a series of control review programs that are completed by the third party to provide visibility on the design of the third party's controls prior to contracting. The program has defined an ongoing monitoring program. The level of inherent risk determines the timeframe for re-assessment, including annual review and update of the IRQ, or whenever there are significant changes to the scope of products or services. Scheduled updates to control reviews with the third party occur on a frequency based on the level of inherent risk.

### 3. State Street Governance and Structure

State Street's approach to risk management involves all levels of management, from the Board of Directors and its committees, including the Risk Committee, the Examining and Audit Committee, the Human Resources Committee, and the Technology and Operations Committee, to each business unit and each employee. Responsibility for risk oversight is allocated so that risk/return decisions are made at an appropriate level and are subject to robust and effective review and challenge. Risk management is the responsibility of each employee and is implemented through a three lines of defense framework.

**The First Line of Defense.** The business and functional units who perform day-to-day operational and/or support activities that may give rise to risk operate as the First Line of Defense ("FLOD"). The FLOD owns the risks associated with their activities and is responsible for establishing effective internal controls to manage such risks to an acceptable level and promoting a strong culture of risk awareness.

**The Second Line of Defense.** Control functions independent of the FLOD, such as Enterprise Risk Management and Corporate Compliance, operate as the Second Line of Defense ("SLOD"). The SLOD is responsible for setting the corporate risk appetite limits, developing policies and procedures to evaluate whether risks remain within the appropriate limits, monitoring risk-taking, and providing credible review and challenge to the FLOD risk management practices. Refer to additional details in *Enterprise Risk Management* and *Corporate Compliance* sections below.

**The Third Line of Defense.** Corporate Audit operates as the independent Third Line of Defense ("TLOD"). The TLOD is responsible for assessing the effectiveness of the First and Second Lines of Defense as it relates to managing risk and providing reporting to the Board of Directors and management. Refer to additional details in the *Corporate Audit* section below.

#### Enterprise Risk Management ("ERM")

The Chief Risk Officer leads ERM globally and has a dual reporting line directly to State Street's Chairman and Chief Executive Officer and the Risk Committee of the Board of Directors. The Chief Risk Officer is also a member of the Executive Committee, the Firm's most senior policy-making committee.

As part of its mandate, ERM maintains the Firm's Risk Appetite Framework, including the supporting risk policies and limits, that set boundaries for firm-wide risk-taking and ensures business strategy, risk processes, and controls contain risk within acceptable bounds. To support this Risk Appetite Framework, ERM has implemented a comprehensive governance structure that provides focused oversight of material risks, establishes corporate risk guidelines and provides a formal mechanism to undertake the consistent identification, management and mitigation of risk. In fulfilling its monitoring and oversight responsibilities, ERM is responsible for proactively monitoring firm-wide risk-taking and has established regular processes for reporting on top risk exposures and emerging risk issues to senior management and the Board of Directors. In addition, ERM is responsible for developing, or ensuring the integrity of, the risk measurement methodologies and tools that are used to monitor the Firm's risk profile relative to its risk appetite. In situations where a material exposure is at-risk of breaching the Firm's risk appetite, ERM is charged with taking the actions it deems appropriate to mitigate or reduce the potential impact to the Firm's earnings, capital or reputation. In the event of a risk appetite breach, ERM has established a formal escalation process to promptly inform the Management Risk and Capital Committee and the Board of Directors of any risk issues that could materially impact the Firm.

ERM manages its responsibilities globally through a three-dimensional organization structure, which includes:

(1) Dedicated "Vertical" business unit-aligned risk groups that support business managers with risk management, measurement and monitoring activities;

(2) "Horizontal" risk groups that monitor risks that cross all of State Street's business units, such as operational risk and credit risk, or that develop, maintain, and assess the effectiveness of the infrastructure that is used to support all of ERM's activities, such as Centralized Modeling and Analytics; and

(3) Risk oversight of international activities, which combines intersecting "verticals" and "horizontals" through a hub-and-spoke model to provide important regional and legal entity perspectives to the global risk framework.

Sitting on top of this three-dimensional organization structure is the Risk Superstructure, which is responsible for the aggregation of risk exposures across the vertical, horizontal and regional dimensions, for consolidated reporting, for setting the corporate-level Risk Appetite Framework and associated limits and policies, and for dynamic risk assessment across State Street. At its foundation is the Recovery and Resolution Planning function, responsible for developing and maintaining the firm-wide strategy for rapid and orderly resolution in the event of material financial distress or failure of State Street, the Centralized Modeling and Analytics function, which provides modeling and analytical support for ERM and Global Treasury, and Corporate Compliance, which establishes the firm-wide approach to identify, assess, monitor and report on compliance risk globally.

### Corporate Compliance

Corporate Compliance maintains State Street's Compliance Risk Management Policy, which establishes the firm-wide approach to identify, assess, monitor and report on compliance risk globally. Compliance risk is defined as the risk of legal or regulatory sanctions, material financial loss, or loss to reputation resulting from failure to comply with regulatory obligations.

State Street has defined two categories of compliance risk: core compliance risk and embedded compliance risk. Corporate Compliance is responsible for overseeing the management of core compliance risk, which are those instances where the primary risk exposure is the failure to comply with regulatory obligations, through the administration of the Core Compliance Oversight Program ("CCOP"). Corporate Compliance is also responsible for ensuring policies to address the management of material core compliance risks are developed and communicated, as necessary. Embedded compliance risk, defined as instances where compliance with regulatory obligations is a component of another risk exposure but not the prevailing risk (e.g., credit risk, technology risk), is managed through specialized risk management programs administered by Enterprise Risk Management.

The Chief Compliance Officer reports to the Chief Risk Officer and is responsible for overseeing the design, development and implementation of the CCOP globally. The Chief Compliance Officer meets regularly with the Examining & Audit Committee ("E&A Committee") to discuss the effectiveness of the CCOP and has the authority to communicate directly with the E&A Committee on any issues relevant to the CCOP. Annually, the Chief Compliance Officer liaises with the Senior Risk Officers responsible for overseeing areas of embedded compliance risk to compile and report an opinion of compliance risk management practices for each area of embedded compliance risk to the E&A Committee.

State Street also has a Standard of Conduct that describes the principles of business conduct expected of all employees of State Street and its subsidiaries globally.

The Standard of Conduct addresses a variety of business and personal conduct matters and sets forth the acceptable conduct required of all employees. The matters covered include:

- Our Values
- Ethical Decision-Making
- Expectations for Managers
- Speaking Up
- Reinforcing Our Standards
- Empowering Our People

- Workplace Safety
- Protecting Company Assets and Information
- Avoiding Conflicts of Interest
- Money Laundering and Sanctions
- Bribery and Corruption
- Fraud
- Working with Outside Parties
- Using Social Media and Public Forums

The Standard of Conduct at State Street is both a statement of ethical principles as well as a guide for employee conduct. Employees are required to comply with and annually certify to its provisions. As such, it is an essential part of State Street's risk management process. The Standard of Conduct is available to employees on both the internet (www.statestreet.com) and State Street's intranet.

### Corporate Audit

Corporate Audit's mandate is to provide the Board of Directors and management with independent and objective assessments of the design and operating effectiveness of State Street's system of internal controls covering the integrity of the company's financial statements and reports; compliance with laws, regulations, and corporate policies; and the effective management of risks faced by the company in executing on its strategic and tactical operating plans. Corporate Audit applies a systematic, disciplined approach to evaluate and recommend improvements to the design and operating effectiveness of State Street's global risk management, control, and governance processes. State Street's Corporate Audit Department is staffed by more than 270 professionals who report directly to the E&A Committee of the Board of Directors.

Corporate Audit issues formal audit reports to the executives responsible for the business area reviewed, as well as the various management levels reporting up to the Chief Executive Officer, including executives from Legal, Risk and Compliance. The E&A Committee of the Board of Directors receives copies of all audit reports as well as summaries of less than satisfactory and unrated reports.

### Finance

The Finance division is responsible for financial accounting and reporting, regulatory reporting, subsidiary accounting, tax compliance and reporting, profit center and financial evaluations, as well as the development and review of State Street's financial accounting controls. The division executes its responsibilities through central corporate accounting, reporting and tax functions and through a network of area, division and subsidiary finance groups that have responsibility for business-unit-level accounting and controller activities.

### Global Human Resources and Corporate Citizenship

The Global Human Resources and Corporate Citizenship ("GHRCC") function at State Street Corporation provides services designed to support the recruitment, ongoing development, and retention of employees across the firm. GHRCC develops and executes on their Human Capital Management ("HCM") strategy, which is intended to enable and support State Street's broader business strategy and key business priorities. GHRCC provides regular updates to the Board of Directors' Human Resources Committee, who oversees the overall HCM strategy.

GHRCC is comprised of Centers of Excellence globally in order to deliver on the HCM strategy and facilitate the employee experience:

- Talent Development and Learning
- Employee Relations and Conduct
- Talent Acquisition
- Global Employee Onboarding
- Global Total Rewards (includes Compensation, Benefits, Performance Management, & Global Mobility)
- Global Inclusion, Diversity and Equity
- Employee Engagement, Corporate Citizenship, & Culture
- Shared Services including HR Service Centers
- HR Technology and Workforce Planning and Insights
- HR Business Partners
- Transformation/Organizational Design
- Internal Communications

### Legal

The Legal division provides counsel that helps State Street successfully navigate complex legal and regulatory environments; maximize business opportunities; and minimize legal, regulatory, reputational and other risks. Legal division professionals strive to provide proactive and practical solutions to support the company's needs, at both the business line level and the corporate level.

## 4. ITGC Overview

### Information Technology

State Street's approach to IT has developed from a singular focus on meeting the needs of global institutional investors. Creating operational scale and efficiency is critical to State Street's ability to deliver value for clients, and as such, State Street has closely aligned its IT strategy with its business model. Members of IT leadership are embedded within the business lines, helping prioritize project development, to help ensure business goals are met and leveraging synergies wherever possible.

State Street uses third-party providers for the operation of various ITGC processes and execution of certain tasks related to infrastructure support services over: change management, job scheduling and incident management, and backup and recovery processes and controls. State Street uses these third-party providers as a vendor staff augmentation model under State Street's direction and within State Street's Information Security Environment to perform certain tasks which are relevant to the criteria and specified controls. State Street has monitoring and oversight mechanism and controls in place to evaluate the effectiveness of the tasks executed by these third-party providers to confirm they are performed accurately, completely, and timely. Such control activities include periodic status meetings and processing reports that monitor the tasks performed by the providers.

State Street's IT division, led by the Office of the Chief Information Officer ("CIO"), identifies, establishes and communicates the IT strategic vision and direction globally as well as oversees enterprise technology infrastructure, application development and maintenance, systems architecture and information security.

The Office of the CIO is supported by the following groups and functions:

- Business Chief Information Officer ("BCIO") group provides end-to-end technology solutioning for many of State Street's businesses and corporate functions. The BCIO group provides services across the System Development Lifecycle from analysis, design and project management, through architecture, development and testing.

  - Each dedicated group within the BCIO is responsible for performing Software Quality Assurance ("SQA") testing of changes to State Street applications, specifically including their core capabilities around functionality testing, regression testing, and reporting security vulnerabilities while complying to the SDLC tollgate requirements for formal testing, as applicable.

  The people, process and technology used to support the access administration functions for these applications are designed based on the specific needs of the application and users. Refer to Section III B for the Security Administration processes in place to support each application.

- State Street Global Advisors Information Technology ("SSGA IT") provides application development including SQA testing of changes to the applications, security administration and production processing support to SSGA businesses and functions for SSGA IT applications with the exception of Global Corporate Action System, CApTAIN/WCApTAIN, Enterprise Reference Platform, Global Transaction Manager, Multicurrency Horizon, SSGA Recordkeeping System, Transaction Lifecycle Management and TSTAR/GX Light, which are supported by State Street's other IT groups described within this section. Herein, SSGA IT supported applications will be referred to as "SSGA IT."

- Global Cybersecurity ("GCS") identifies and implements industry leading practice policies, solutions and standards designed to enable State Street permanent employees, contingent workers, business partners and clients to conduct business and exchange information in a secure environment where risk is carefully managed. The following programs are managed by GCS:
  - The Cybersecurity Center ("CSC") identifies, assesses and defends against security threats. Functions include monitoring and remediating enterprise security events, enterprise-wide analytics, analysis and reporting.
  - The Information Security Officer ("ISO") Network creates a managed relationship between GCS and State Street business units and works to consistently integrate the information security requirements into the business processes.
  - Security Administration Services ("SAS") is responsible for security administration and includes the following:
    - SAS: Responsible for access administration for core systems and applications and includes the International Security Administration Services ("ISAS") group; focused on implementing automation and enhanced processes to improve service levels; support includes security administration for applications used by local markets.
    - Help Desk: Responsible for corporate-wide password resets and access administration of first-time passwords for systems and applications.
    - IAM Centralized Certification team: Responsible for overseeing access recertifications utilizing the SailPoint tool that are performed on a regularly scheduled basis on behalf of the business.
- Technology Platform Engineering and Operations ("TPEO") manages State Street's global infrastructure footprint by delivering resilient, business focused computing services as well as providing network, security administration and help desk services to users across State Street Corporation. TPEO manages all IT Service Management disciplines, including Availability Management. TPEO staffs are located in North America; the Asia Pacific ("APAC") region; and the Europe, Middle East and Africa ("EMEA") region.
  - AIS IT: A dedicated group within TPEO is responsible for access administration, SQA testing of changes to certain applications, and production support for applications supporting the Alternatives sector. Please refer to Section III B for a complete list of these applications.

### Global Security

The Global Security division's mission is to protect State Street's people, clients' assets, information, continuity of operations and reputation worldwide. Three teams within the division — Protective Services, Investigations and Strategies and Initiatives — work together to adopt and help enforce industry-leading practices to help create a safe and secure work environment for all employees as well as meet or exceed regulatory and customer requirements.

The Global Security team provides leadership with centralized oversight and governance of security risk management, incident management, policy, administration, and operations. This includes security monitoring and compliance, physical security design, engineering and management, background investigations, cyber investigations and legal support as well as assistance with information security protection, incident response and overall security service delivery.

### Global Delivery

The Global Delivery division provides asset owners and managers with a wide range of support, from core custody and cash, accounting, fund administration and shareholder recordkeeping to complete investment operations outsourcing solutions and servicing for complex assets like OTC derivatives, private equity and real estate. Based on business requirements, Global Delivery performs security administration activity for the following applications: FundSuiteArc (EMEA Instance), NAVigator, Recon Plus (a tool within Global Services Reconciliation) and T-STAR/TX.

## 5. Complementary User Entity Controls

State Street's controls represent only a portion of the overall internal control environment of each client. Clients also need to implement and maintain effective internal control. Each client's internal control depends upon the nature of the transactions processed, the degree of interaction of controls and the terms of agreement with State Street. This section highlights those controls that State Street believes should be present for each State Street client ("Complementary User Entity Control"). State Street has considered Complementary User Entity Controls in developing the controls that are described in Section IV A of this report.

This report should be used in conjunction with the applicable complementary State Street business control reports. Those reports may also include complementary user entity controls necessary to achieve certain control objectives identified in the complementary State Street business control reports. Additionally, the complementary user entity control presented below does not represent a comprehensive set of all the controls that may be necessary at user entities.

### Client Interface and Communication Considerations

Each client (and its independent auditor) must evaluate its own internal controls to determine if procedures are in place for the following:

| Complementary User Entity Control | Control Objective Reference |
|---|---|
| Clients are responsible for authorizing and maintaining appropriate logical access to State Street applications. | 2 |

### 6. Subservice Organizations

State Street utilizes subservice organizations to perform a range of services that are relevant to clients' internal control over financial reporting.

The principal subservice organizations, which are not included in the scope of this report (i.e., reported using the carve out method), are described below:

- **Application Service Provider –** State Street uses Application Service Providers ("ASPs") to provide application development, change management and hosting services.

  For the following applications, State Street is responsible for application access administration, including access authorization and modification and access recertification activities within Control Objective 2 (i.e., controls 2.5 through 2.8 and controls 2.11 through 2.15). In addition, T-STAR/TX is tested for control 2.3 at the application level. State Street is also responsible for certain aspects of change management of Colline which is tested in controls 3.3 and 3.4.

| Application | Application Service Provider | Applicable Complementary Business Report |
|---|---|---|
| Bloomberg AIM | Bloomberg | SSGA |
| Business Process Management ("BPM") (Australia instance) | SS&C Technologies | GS URA |
| Colline | Vermeg | GFAC, IMSE |
| Compliance Extract | Appian | SSGA |
| FeeCom | SS&C Technologies and Abraxas | TA-HKS |
| FundSuiteArc (U.S. and EMEA instances) | Donnelly Financial Solutions, Inc | GFAC |
| Geneva and Lumis | SS&C Technologies | AISH |
| Spire | Stonewain | GFAC |
| T-STAR/TX | NRI Financial Solutions | SSTB IMIOS |

- **Data Center Service Provider – NTT Managed Services Americas ("NTT Managed Services") –** State Street engages NTT Managed Services to provide Data Center hosting services in support of the NAV Collection, PAM for Mortgages and PAM for Investments applications. NTT Managed Services is responsible for the physical security and physical access controls. NTT Managed Services provides managed cloud services, application hosting, managed services, managed security services, end user services and IT consulting services.

### Monitoring of Subservice Organizations

As referenced in the Third Party Risk Management ("TPRM") section, the output of the IRQ determines the level of due diligence required to be performed on the vendors, including the subservice organizations identified above.

The due diligence process includes a series of control review programs, which are completed by the vendor to provide visibility on the design of the vendor's controls prior to contracting. The TPRM includes defined ongoing monitoring program activities such as: review of the subservice organizations' SOC reports; periodic due diligence reviews; and review of output reports based on either service-level agreements or scope of services provided (e.g., accounting report reconciliations, etc.) The level of inherent risk determines the timeframe for re-assessment, and includes a schedule for updating the IRQ, including any changes to the scope of products or services and updates to the control reviews with the vendor.

### Expected Complementary Subservice Organization Control Considerations

State Street has evaluated the services provided by each subservice organization and has identified the controls State Street management assumes, in the design of State Street's system, are implemented by the subservice organizations. The controls described below are applicable to the applications as noted above within the *Subservice Organizations* section and are necessary to achieve the control objectives stated in State Street's description of its ITGC System. For ASPs, the Complementary Subservice Organization Controls ("CSOCs") related to Control Objectives 1 through 5 below are relevant. For the Data Center Service Provider, the CSOCs related to Control Objective 1 below are relevant.

| Complementary Subservice Organization Control | Control Objective Reference |
|---|---|
| Physical access to data centers and other computer rooms, which house the entity's IT resources, is documented, authorized and based on business need.<br>Access to data centers and other computer rooms is restricted through the use of keycard access or biometric devices.<br>Physical access to data centers and other computer rooms is reviewed on a periodic basis.<br>Upon termination, access to the data center and other computer rooms is disabled. | 1 |
| Password controls for production applications, databases, operating systems and the network are in place to prevent unauthorized access to system resources.<br>Access to the IT infrastructure supporting the hosted application is documented, authorized and restricted to authorized personnel based on business need.<br>Access to production applications, databases, operating systems and the network hosted by the subservice organizations is reviewed on a periodic basis.<br>Upon termination, access to production applications, databases, operating systems and the network hosted by the subservice organizations is disabled.<br>Where applicable, access is granted by dedicated security administration groups according to the access privileges specified in the access request. | 2 |
| Management employs a systems development life cycle ("SDLC") methodology that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology.<br>Changes to the system components, including applications, databases and operating systems are formally documented, tested, and approved prior to implementation into production.<br>Segregation of incompatible duties exists within the change management environment.<br>Emergency changes that require deviations from standard procedures (i.e., Firecall IDs) are logged and reviewed. | 3 |

| Complementary Subservice Organization Control | Control Objective Reference |
|---|---|
| Changes to job schedules are authorized and monitored.<br>Production jobs are monitored for successful completion. Failed jobs are tracked, prioritized and addressed in a timely manner.<br>Production processing incidents are identified and resolved. | 4 |
| Relevant technology, including application servers and databases, as applicable, are backed up on a periodic basis in accordance with written backup policies and procedures. Backups are monitored for successful completion and failures are researched and resolved.<br>Backup data is sent or copied to an off-site facility on a periodic basis and is available for restoration in the event of processing errors and/or unexpected interruptions. | 5 |

### 7. Changes in State Street Operations

#### Identity and Access Management Program

This multi-year program consists of two workstreams: Identity and Access Management ("IAM") and Privileged Access Management ("PAM"). The objective of the IAM workstream is to apply a set of consistent identity and access controls to applications based on a tiered approach. The objective of the PAM workstream is to develop and apply a set of consistent controls across the enterprise, enabled via a centralized privileged access management solution.

The IAM program is implementing centralized platform capabilities for requesting and approving access to systems, role management, rules and separation of duties policy enforcement, recertifications, and discovery through a single pane of glass view of user access privileges. Please refer to the *Application Listing* in Section III B, which identifies the Security Administration and Access Recertification process for each in-scope application.

As part of the program, for certain applications, access administration functions for employees and contingent workers are administered through SailPoint, a self-service tool for identity storage, access requests and entitlement provisioning. SailPoint is used to provision and recertify access to the applications as documented in Section II B *Application Listing* and applications continue to be on-boarded onto SailPoint in a phased approach.

## B. Application Listing

State Street addresses the unique infrastructure needs of specific lines of business and corresponding requirements to leverage economies of scale across the organization. The functions and core services of State Street business control reports rely on applications which are supported using various types of infrastructure, including:

- **Operating System Platforms:** Linux, Mainframe, OpenVMS, Private Cloud (State Street's Private Cloud is hosted on the Linux operating system), Tandem, UNIX and Windows.
- **Databases:** DB2, Hive, ISAM, Nonstop SQL, Oracle, Oracle Exadata, MS SQL, Sybase, VSAM and vendor proprietary.

The functions and core services of State Street business control reports, as described in the complementary State Street reports, are supported by the following in-scope applications and related control processes. For a description of the applications' function, please refer to the Complementary State Street Report. For details surrounding each of the Security Administration or Access Recertification processes identified below, please refer to Section III C:

## Application Listing

| Application | Complementary State Street Report | Operating System Platform | Database | Data Center/ Computer Room Location | Security Administration Process | Access Recertification Process |
|---|---|---|---|---|---|---|
| Acquisition Management[1] | GFAC | Private Cloud | Oracle Exadata | North America | eSF | SailPoint |
| Active Rebalancing Tool – PRO | SSGA | Linux | Oracle | North America | SSGA IT | SSGA IT |
| Advantage (Fee Advantage)[1] | IMSE | Windows | MS SQL | North America | SailPoint | SailPoint |
| Alerts and Events Framework[1] | GFAC | Private Cloud | Oracle Exadata, DB2 | North America | eSF | SailPoint |
| Alpha Frontier[1] | AISH | Windows | MS SQL | North America | SailPoint | SailPoint |
| Alveo[1] | GFAC<br>IMSE | UNIX | Oracle Exadata | North America | SailPoint | SailPoint |
| ANOVA | SSGA | UNIX | Sybase | North America | SSGA IT | SSGA IT |
| ARO™ [1] | AISH | Private Cloud | Oracle | North America | SailPoint | SailPoint |
| Assets Under Management | SSGA | Linux | Oracle | North America | SSGA IT | SSGA IT |
| Automated Fund Workflow[1] | GFAC | Private Cloud | Oracle | North America | eSF | SailPoint |
| Automated Wash Sales[1] | GFAC | Linux | Oracle | North America | Application Specific & SailPoint | SailPoint |
| Bank Electronic Support System[1] | GFAC<br>USIS | Tandem | Nonstop SQL | North America | SAS & eSF | SailPoint |
| Bank Institutional Delivery System | GFAC | Mainframe | DB2 | North America | SailPoint | SailPoint |
| Bloomberg AIM[2] | SSGA | Third-Party Vendor | Vendor Proprietary | Third-Party Vendor | SSGA IT | SSGA IT |
| Business Objects[1] | AISPM | Linux | Oracle | North America | Application Specific & SailPoint | SailPoint |
| Business Process Management (Australia)[2] | GS URA | Third-Party Vendor | Third-Party Vendor | Third-Party Vendor | SAS & SailPoint | SailPoint |
| Business Process Management (North America)[1] | ITA<br>USIS | Private Cloud | Oracle | North America | SailPoint | SailPoint |

| Application | Complementary State Street Report | Operating System Platform | Database | Data Center/ Computer Room Location | Security Administration Process | Access Recertification Process |
|---|---|---|---|---|---|---|
| Caliber™[1] | AISH<br>AISPM | UNIX, Windows | Sybase | North America | AIS IT & SailPoint | SailPoint |
| CapStock | TA-Ireland | UNIX | Oracle | Europe | SailPoint | SailPoint |
| CApTAIN/WCApTAIN[1] | GFAC<br>IMSE<br>SSTB TBSPB<br>SSGA | Private Cloud | Oracle | North America | SAS | SailPoint |
| Cash Flow Module (eCFM) | GFAC<br>AISPM | Private Cloud | DB2 | North America | SailPoint | SailPoint |
| Cash Management Instruction[1] | AISPM | Windows | MS SQL | North America | SailPoint | SailPoint |
| Cash Portal | SSGA | Linux | Oracle, Oracle Exadata | North America | SSGA IT | SSGA IT |
| Cash Views 5.0 | SSGA | Linux, UNIX, Windows | Sybase, Oracle Exadata | North America | SSGA IT | SSGA IT |
| Collateral Management Workstation[1] | GFAC<br>IMSE | Linux, UNIX | Oracle Exadata | North America | eSF & SailPoint | SailPoint |
| Collateral Plus[1] | GFAC<br>IMSE | Linux | Oracle, Hive | North America | eSF | SailPoint |
| Colline[2] | GFAC<br>IMSE | Third-Party Vendor | Third-Party Vendor | Third-Party Vendor | Application Specific & SailPoint | Application Specific |
| Compliance Extract[2] | SSGA | Third-Party Vendor | Vendor Proprietary | Third-Party Vendor | SSGA IT | SSGA IT |
| Continuous NAV[1] | GFAC | Private Cloud | Oracle Exadata | North America | eSF | SailPoint |
| Corporate Action Monitoring System[1] | GFAC | Mainframe | DB2 | North America | SailPoint | SailPoint |
| Data Management Hub – Japan Trust Operations[1] | SSTB TBSPB | Private Cloud | Oracle Exadata | North America | eSF | SailPoint |
| Data Management Hub – Middle Office Trade Management[1] | SSTB IMIOS | Private Cloud | Oracle Exadata | North America | eSF | SailPoint |
| Data Management Hub – RTS[1] | GS-TSA | Private Cloud | Oracle Exadata | North America | eSF | SailPoint |
| Data Management Hub – UIT[1] | GFAC | Private Cloud | Oracle Exadata | North America | eSF | SailPoint |
| Derivatives Hub[1] | GFAC<br>IMSE<br>SSTB TBSPB<br>SS GmbH-Italy | Private Cloud, Linux | Oracle Exadata | North America | SAS | SailPoint |
| Distribution, Metering and Entitlements[1] | GFAC | Private Cloud | Oracle Exadata | North America | eSF | SailPoint |

| Application | Complementary State Street Report | Operating System Platform | Database | Data Center/ Computer Room Location | Security Administration Process | Access Recertification Process |
|---|---|---|---|---|---|---|
| Dollar Market Logic[1] | GFAC | Mainframe | DB2 | North America | SailPoint | SailPoint |
| Dual Verification Database | TA-HKS<br>TA-Ireland | UNIX | Oracle | Europe | ISAS | SailPoint |
| Dynamic Cash Allocation[1] | GFAC | Windows | MS SQL | North America | eSF | SailPoint |
| Enterprise Horizon | GFAC<br>USIS | Mainframe, Private Cloud | DB2 | North America | eSF & SailPoint | SailPoint |
| Enterprise Pricing Web[1] | GFAC<br>FFA<br>IMSE<br>AISH<br>SS GmbH-Italy<br>SS GmbH-KVG<br>SSTB IMIOS | Private Cloud | Nonstop SQL | North America | eSF | SailPoint |
| Enterprise Reference Platform[1] | IMSE<br>SSGA | Private Cloud | Oracle Exadata | North America | eSF | SailPoint |
| Enterprise Reporting Platform | AISH | Windows, UNIX | MS SQL | North America | AIS IT | Application Specific |
| Enterprise Servicing Platform (AIS)[1] | AISH | Private Cloud | Oracle | North America | eSF & SailPoint | SailPoint |
| Enterprise Servicing Platform (APRA)[1] | GFAC | Private Cloud | Oracle Exadata | North America | SailPoint | SailPoint |
| Enterprise Servicing Platform (DataGX)[1] | SSTB IMIOS | Private Cloud | Oracle Exadata | North America | SailPoint | SailPoint |
| Enterprise Servicing Platform (Japan)[1] | SSTB TBSPB<br>SSTB IMIOS | Private Cloud | Oracle Exadata | North America | SailPoint | ISAS |
| ETF Global Platform[1] | GFAC | Private Cloud, Linux | Oracle Exadata | North America | eSF | SailPoint |
| Exchange Traded Products[1] | USIS | Private Cloud, Linux, Windows | Oracle, Oracle Exadata | North America | eSF | SailPoint |
| Expense Manager | GFAC | Mainframe, Private Cloud | DB2 | North America | SailPoint | SailPoint |
| FeeCom[2] | TA-HKS<br>TA-Ireland | Third-Party Vendor | Vendor Proprietary | Third-Party Vendor | ISAS | Application Specific |
| Financial Data Repository | GFAC | Linux, UNIX | Oracle, Oracle Exadata | North America | SAS & SailPoint | SailPoint |
| FI Maintenance | SSGA | UNIX | Sybase | North America | SSGA IT | SSGA IT |
| FI Pricing | SSGA | UNIX | Sybase | North America | SSGA IT | SSGA IT |
| Fund Accounting Systems[1] | AISPM | Windows, Linux | Oracle | North America | SailPoint | SailPoint |
| FundSuiteArc (EMEA Instance)[2] | GFAC | Third-Party Vendor | Vendor Proprietary | Third-Party Vendor | Application Specific | Application Specific |
| FundSuiteArc (U.S. Instance)[2] | GFAC | Third-Party Vendor | Vendor Proprietary | Third-Party Vendor | Application Specific | Application Specific |

| Application | Complementary State Street Report | Operating System Platform | Database | Data Center/ Computer Room Location | Security Administration Process | Access Recertification Process |
|---|---|---|---|---|---|---|
| FundSuite SX[1] | GFAC | Windows | MS SQL | North America | Application Specific & SailPoint | SailPoint |
| Geneva[2] | AISH | Third-Party Vendor | Vendor Proprietary | Third-Party Vendor | SailPoint | SailPoint |
| Global Corporate Action System[1] | GFAC<br>IMSE<br>SSGA<br>SS GmbH-Italy<br>SSTB IMIOS | UNIX | Oracle | North America | SailPoint | SailPoint |
| Global Income Control | GFAC | Mainframe | DB2 | North America | SailPoint | SailPoint |
| Global One[1] | GFAC | UNIX | Oracle, Oracle Exadata | North America | SailPoint | SailPoint |
| Global Performance Database[1] | AISPM | Linux, Windows | Sybase | North America | SAS & SailPoint | SailPoint |
| Global Realty Investment Database[1] | AISPM | Linux | Sybase | North America | SailPoint | SailPoint |
| Global Securities Movement and Control[1] | GFAC<br>SS GmbH-Italy | Mainframe | DB2 | North America | SailPoint | SailPoint |
| Global Services Application | GFAC | Linux | Oracle | North America | SAS & SailPoint | SailPoint |
| Global Services Reconciliation | GFAC | Mainframe | DB2, VSAM | North America | Application Specific & SailPoint | SailPoint |
| Global Tax Systems[1] | GFAC | Private Cloud | Oracle Exadata | North America | eSF | SailPoint |
| Global Trade Confirmation System/Global Trade Management System | SSGA | UNIX | Sybase, Oracle | North America | SSGA IT | SSGA IT |
| Global Transaction Manager[1] | GFAC<br>IMSE<br>KCIS<br>SS GmbH-Italy<br>SS GmbH-KVG<br>SSTB IMIOS<br>SSGA | Private Cloud, UNIX | Oracle, Oracle Exadata | North America | eSF & SailPoint | SailPoint |
| GP3 | FFA | UNIX, Linux | Oracle | North America | ISAS & SailPoint | SailPoint |
| Great Plains[1] | AISPM | Windows | MS SQL | North America | SailPoint | SailPoint |
| Hogan[1] | GFAC<br>ITA<br>SSRS | Mainframe | VSAM | North America | eSF & SailPoint | SailPoint |
| InCash[1] | SS GmbH-Italy | Mainframe | DB2, Oracle | North America | SailPoint | SailPoint |
| Information Management Centre | SSGA | Linux | Oracle Exadata | North America | SSGA IT | SSGA IT |

| Application | Complementary State Street Report | Operating System Platform | Database | Data Center/ Computer Room Location | Security Administration Process | Access Recertification Process |
|---|---|---|---|---|---|---|
| Instruction Initiation Platform[1] | GFAC<br>SSTB TBSPB | Private Cloud | Oracle Exadata | North America | eSF | SailPoint |
| Integrated Banking System[1] | GFAC | OpenVMS | NEXSYS (proprietary) | North America | SAS & Application Specific | SailPoint |
| International Cash | GFAC | Mainframe | DB2 | North America | SailPoint | SailPoint |
| Invest*AI*[1] | AISPM | Windows | MS SQL | North America | SailPoint | SailPoint |
| InvestLend[1] | USIS | Private Cloud | Oracle Exadata | North America | eSF | SailPoint |
| Investment General Ledger System | AISH<br>AISPM | UNIX, Windows | Sybase | North America | AIS IT | SailPoint |
| Investor Services System[1] | AISH<br>AISPM | Windows | Oracle | Europe | SailPoint | SailPoint |
| Investran | AISPM | Windows | MS SQL | Europe | SailPoint | SailPoint |
| Invest*TA*[1] | ITA | UNIX, Windows | Oracle, MS SQL | North America | SAS | SailPoint |
| Iris Trading and Operations Platform[1] | GFAC | Private Cloud | Oracle Exadata | North America | eSF | SailPoint |
| Italian Fund Accounting ("ITF")/GP3[1] | SS GmbH-Italy | UNIX | Oracle | North America | SailPoint | SailPoint |
| Japan Accounting and Reporting System[1] | SSTB IMIOS | Windows | Oracle | Asia Pacific | ISAS | SailPoint |
| Livewire | GFAC | Windows | MS SQL | Europe | SailPoint | SailPoint |
| Loan Ops Portal | GFAC | Windows | MS SQL | North America | eSF | SailPoint |
| Lumis[2] | AISH | Third-Party Vendor | Vendor Proprietary | Third-Party Vendor | SailPoint | SailPoint |
| Market Data Framework | SSGA | UNIX, Windows | Oracle, MS SQL, Sybase | North America | SSGA IT | SSGA IT |
| Market Effect System | SSGA | UNIX | Oracle, Oracle Exadata, Sybase | North America | SSGA IT | SSGA IT |
| Minerva | SSGA | Linux | Oracle | North America | SSGA IT | SSGA IT |
| Monitor Multi Level[1] | SS GmbH-Italy | Windows | MS SQL | North America | SailPoint | SailPoint |
| Mosiki[1] | AISH | Linux | Sybase | North America | SailPoint | SailPoint |
| Multicurrency Horizon[1] | GFAC<br>IMSE<br>SSTB IMIOS<br>SSGA<br>SSTB TBSPB<br>USIS | Mainframe | DB2 | North America | SailPoint | SailPoint |
| MyMML[1] | SS GmbH-Italy | Windows | MS SQL | North America | SailPoint | SailPoint |

| Application | Complementary State Street Report | Operating System Platform | Database | Data Center/ Computer Room Location | Security Administration Process | Access Recertification Process |
|---|---|---|---|---|---|---|
| MyStateStreet[1] | GFAC | Linux, UNIX | Oracle Exadata | North America | eSF | N/A |
| MyView[1] | GFAC<br>IMSE<br>USIS | Private Cloud | Oracle Exadata | North America | eSF | SailPoint |
| NAV Collection[1] | KCIS | UNIX | Oracle | Third-Party Vendor | SailPoint | SailPoint |
| NAVigator[1] | GFAC | Tandem, Windows | Nonstop SQL | North America | Application Specific & SailPoint | SailPoint |
| Non-Securities Reference Data | SSGA | Linux, UNIX | Oracle, Sybase | North America | SSGA IT | SSGA IT |
| Open System Accounting – Accounting Systems Audit | GFAC | UNIX | Oracle Exadata | North America | SAS & SailPoint | SailPoint |
| Oracle Financials | AISPM | Linux | Oracle | North America | Application Specific | Application Specific |
| PAM® for Investments | KCIS | Windows | Oracle, MS SQL | Third-Party Vendor | SAS | SailPoint |
| PAM® for Mortgages[1] | KCIS | Windows | MS SQL | Third-Party Vendor | SailPoint | SailPoint |
| Participant Record Keeping System | SSGA | UNIX | Oracle, Oracle Exadata, Sybase | North America | SSGA IT | SSGA IT |
| Payment Services Account Repository[1] | GFAC | UNIX | Oracle | North America | SailPoint | SailPoint |
| PEP+[1] | SSRS | Mainframe | DB2, VSAM | North America | SailPoint | SailPoint |
| Phoenix[1] | GS URA | UNIX | ISAM | Asia Pacific | SailPoint | SailPoint |
| PLUS | SSRS | Linux | ISAM | North America | SAS & SailPoint | SailPoint |
| PLUS Web[1] | SSRS | Linux | Oracle | North America | Application Specific | SailPoint |
| Portia | SSGA | Windows | MS SQL | North America | SSGA IT | SSGA IT |
| Post-Settlement Lifecycle Management | FFA<br>IMSE<br>SS GmbH-Italy | Private Cloud | Oracle, Oracle Exadata | North America | eSF & SailPoint | SailPoint |
| Property Management Interface[1] | AISPM | Linux | Oracle | North America | SailPoint | SailPoint |
| Recon Portal | SSGA | Windows | SQL | North America | SSGA IT | SSGA IT |
| Recordkeeping System (IMS)[1] | IMSE<br>SSTB TBSPB | Linux, UNIX, Windows | Oracle Exadata | North America | SailPoint | SailPoint |
| Recordkeeping System (Japan)[1] | SSTB IMIOS<br>SSTB TBSPB | Linux, UNIX, Windows | Oracle Exadata | Asia Pacific | SailPoint | SailPoint |

| Application | Complementary State Street Report | Operating System Platform | Database | Data Center/ Computer Room Location | Security Administration Process | Access Recertification Process |
|---|---|---|---|---|---|---|
| Recordkeeping System (SSGA) | SSGA | Linux, UNIX, Windows | Oracle Exadata | North America | SailPoint | SSGA IT |
| Report System Warehouse[1] | SSTB IMIOS<br>SSTB TBSPB | Private Cloud, Windows, UNIX | Oracle, Oracle Exadata | North America | eSF | SailPoint |
| Revenue Management System | SSGA | Linux, UNIX, Windows | Oracle | North America | SSGA IT | SSGA IT |
| RKS Outbound Repository | SSGA | Linux | Oracle | North America | SSGA IT | SSGA IT |
| Securities Lending Credit Management System | SSGA | Linux, UNIX | Oracle | North America | SSGA IT | SSGA IT |
| Securities Lending Enterprise[1] | GFAC | Private Cloud | Oracle, Oracle Exadata, Sybase | North America | SailPoint | SailPoint |
| Securities Movement and Control[1] | GFAC<br>USIS | Mainframe | DB2 | North America | SailPoint | SailPoint |
| Securities Transfer System[1] | GFAC | Tandem | Nonstop SQL | North America | SAS & eSF | SailPoint |
| Sentinel | SSGA | Linux | Oracle | North America | SSGA IT | SSGA IT |
| SMS[1] | SSRS | Mainframe | VSAM | North America | SailPoint | SailPoint |
| Spire[2] | GFAC | Third-Party Vendor | Vendor Proprietary | Third-Party Vendor | SailPoint | SailPoint |
| Tax Efficient Lot Selector | GFAC | Linux | Oracle | North America | Application Specific & SailPoint | SailPoint |
| Tax Reclaim System[1] | GFAC | Windows | Oracle | North America | SailPoint | SailPoint |
| Trade Portal | SSGA | Linux, UNIX | Oracle, Sybase | North America | SSGA IT | SSGA IT |
| Transaction Lifecycle Management[1] | FFA<br>IMSE<br>SS GmbH-Italy<br>SS GmbH-KVG<br>SSGA<br>SSTB IMIOS | Private Cloud | Oracle, Oracle Exadata | North America | SAS & SailPoint | SailPoint |
| Transaction Lifecycle Management Premium[1] | FFA<br>GFAC<br>AISH | Private Cloud | Oracle, Oracle Exadata | North America | SAS | SailPoint |
| T-STAR/GX Light[3] | SSTB IMIOS<br>SSGA | Windows | MS SQL | Asia Pacific | N/A | N/A |
| T-STAR/TX[2] | SSTB IMIOS | Third-Party Vendor | Vendor Proprietary | Third-Party Vendor | ISAS | Application Specific |
| Universal Custody Management[1] | GFAC | Linux | Oracle | North America | SailPoint | SailPoint |
| Variation Margin Wire | GFAC<br>ITA | Private Cloud, UNIX | Sybase | North America | eSF & SailPoint | SailPoint |

| Application | Complementary State Street Report | Operating System Platform | Database | Data Center/ Computer Room Location | Security Administration Process | Access Recertification Process |
|---|---|---|---|---|---|---|
| Wall Street Office[1] | GFAC | Windows | MS SQL | North America | Application Specific & SailPoint | SailPoint |
| Wall Street Office (Alternatives)[1] | AISH | Windows | MS SQL | North America | eSF | SailPoint |
| WAMP[1] | SS GmbH-Italy | Windows | Oracle | North America | SailPoint | SailPoint |

[1]The SailPoint movers capability (i.e., control 2.16) is enforced for this application.

[2]Information technology general controls in place for this application are not covered in the scope of this report, except for select controls as noted in Section III 6 *Subservice Organizations*, please refer to that section for further details. In addition, the SailPoint movers capability (i.e., control 2.16) is enforced for the following applications: Geneva and Lumis.

[3]Information technology general controls in place for this application are not covered in the scope of this report, except for select controls related to physical access, change management release of changes, backup and restore.

## C. Description of Information Technology General Controls Processes

Although the control objectives and related controls are included in Section IV, they are the responsibility of State Street Management and are an integral part of Management's description of the ITGC system.

### Physical Security

The in-scope production applications, databases and operating systems are physically located in State Street data centers and computer rooms or co-located data centers in North America, Europe and Asia Pacific (collectively referenced as "data centers"). Although the co-located data centers in Asia Pacific are managed by data center co-location vendors, State Street owns and operates the physical security equipment installed on State Street's restricted cages within these co-located data centers. The controls described in Section IV, Control Objective 1 are in place to support the physical security of State Street's equipment located in restricted cages within co-located data centers and are included in the scope of this report. Physical security controls performed by the co-located data center vendors are not included in the scope of this report.

Certain applications are hosted in a third-party data center located in North America. Please refer to Section III 6 *Subservice Organizations* for further details.

Please reference Section III B for information about data center and computer room locations for in-scope applications.

### Policies and Procedures

State Street has developed and implemented written policies and procedures to guide State Street personnel through the process of requesting and granting access to State Street facilities, including data centers and computer rooms for permanent employees and contingent workers.

### Physical Access Administration

Initial access requests to State Street facilities, excluding data centers and computer rooms, are primarily initiated by Global Human Resources ("GHR") within GHRCC for permanent employees and Global Procurement Services for contingent workers. Contingent workers include temporary employees, contractors and vendors. Requests for additional access to State Street facilities, excluding data centers and computer rooms, must be approved by designated State Street personnel. Requests for access to data centers and computer rooms must be submitted to designated State Street IT personnel. Designated State Street IT personnel are authorized to approve access requests to data centers and computer rooms based on the business need for the access requested. Global Security will process approved access requests. Permanent employees and contingent workers are assigned a unique access card to gain entry to State Street facilities. Global Security uses physical security management tools to assign and manage access card information, including the access card ID number, the individual's GHR ID, hire date, access card expiration date and facilities access privileges. Physical security management tools are also used for alarm monitoring, recording digital video, photo ID badging and visitor management. Update access to physical security management tools is restricted to designated Global Security personnel, based on job responsibilities.

Permanent employees and contingent workers who have lost or damaged their access card are responsible for timely notifying Global Security personnel to disable the access card and to have a new access card issued.

#### Access Revocation

Designated State Street personnel communicate terminations for permanent employees and contingent workers to GHR and Global Procurement Services, respectively. GHR, Global Procurement Services and/or hiring managers are primarily responsible for updating the employment status in the Human Resources Management System ("HRMS") application or Contingent Labors application, for contingent workers with the last date worked. Designated State Street personnel may update the HRMS application directly.

Global Security personnel are notified of permanent employees' and contingent workers' termination status in a timely manner. The HRMS application sends a file to the physical security management tool, used to assign and manage access card information to data centers, co-located data centers and computer rooms globally. Through automated job schedules (North America and Asia Pacific) or through an automated workflow process by which Global Security personnel receive and upload the file to the physical security management tool (Europe), the HRMS file automatically updates the terminated permanent employee's or contingent worker's expiration date in the access card record with the termination date or agency end date from the HRMS file. This file is sent twice daily, except for weekends. The logic used to produce the HRMS file includes the earliest of the termination date, agency end date or last date worked from the HRMS file. The file automatically updates the terminated permanent employee's or contingent worker's expiration date in the access card record with the earliest of the termination date or last date worked from the HRMS file. Global Security personnel have the ability to manually block the access card of permanent employees and contingent workers who require immediate termination. Upon termination, a permanent employee's or contingent worker's access card is automatically disabled based on the expiration date in the access card record.

#### Physical Access Recertification Activities

Access to data centers and computer rooms is restricted to designated State Street employees and contingent workers. On an annual basis, designated State Street IT personnel review the access to determine whether existing access remains appropriate based on job responsibility. In addition, periodic review of existing access is performed by IT personnel responsible for the data centers and computer rooms. Modifications to data center and computer room access privileges are communicated to Global Security personnel for processing.

### Facility Access Controls

Valid access cards are required to enter State Street facilities. In addition to the facilities' access card, authentication through keypad readers and/or biometric devices may be required to gain access to the data centers and computer rooms.

Physical security management tools record access to data centers and computer room entry. Video cameras record access to data center entry and/or exit points. Global Security personnel monitor and respond to unauthorized activity at State Street data centers and computer rooms.

Visitors, including State Street permanent employees, contingent workers or non-affiliated third parties, requiring access to data centers or computer rooms must be pre-registered by authorized State Street personnel. A visitor must show identification before being granted access to the data center or computer room and is required to sign in and out at the lobby security desk. Visitor activity is monitored by designated State Street personnel while on the premises.

### Logical Access

Procedures, including the State Street Global Cybersecurity ("GCS") Standards and the Identity and Access Management Policy and Standards, related to user administration are in place to guide Global Technology Services personnel in the process of adding, modifying or deleting users to/from the local network, databases and environments. State Street has developed and implemented written policies and procedures to guide State Street personnel through the process of requesting and granting of access to State Street facilities, including data centers, for permanent employees and contingent workers.

### Policy, Standards and Procedures

State Street has a Global Cybersecurity Policy, which is approved annually by the Technology and Operational Risk Committee of the board. State Street's GCS group has developed and implemented written information security standards to guide State Street personnel through the process of managing and monitoring access to production applications, databases and operating systems, and the corporate network for State Street permanent employees and contingent workers.

State Street also has a comprehensive GCS Program to protect the information and data owned and used by State Street, its subsidiaries and affiliates, permanent employees, contingent workers, business partners, clients and other third-party relationships. Contingent workers include temporary employees, contractors and vendors. State Street has aligned these controls to the NIST 800 53R4 special publication and is in the process of aligning to the NIST 800 53R5 revision.

To help achieve the GCS Program objectives, State Street has established a global ISO network. The ISO network creates a strong relationship between GCS and State Street business units and works to consistently integrate the information security controls into State Street's business processes.

### User ID and Password Management

State Street permanent employees and contingent workers are required to access State Street's corporate network prior to authenticating at the application, database, and/or operating system-level through the use of a valid Local Area Network ("LAN") user ID and password combination. Application-level authentication may occur through the LAN user ID or may require a separate application, database, and/or operating system user ID and password combination. When accessing the network remotely, users are required to use multi-factor authentication.

Authentication standards have been established by the GCS group and include single factor using a password or multi-factor leveraging a Secure ID Token with a password and/or PIN. Password and PIN standards have been established by the GCS group and require production applications, databases, and operating systems be configured by designated personnel (where technically feasible) to adhere to minimum requirements. A process exists for management to review password settings for production applications, databases and operating systems that do not comply with GCS standards and evaluate the potential risks and mitigating controls associated with the current password settings.

Security settings for operating systems have been configured, including LAN authentication, for a limited number of invalid access attempts before the account is locked. A time delay is in place for disabled LAN user IDs before the user ID owner can re-authenticate to the system. A State Street permanent employee or contingent worker who has locked their account is required to either contact the Help Desk or access an on-line self-service tool and provide at least two forms of identification to unlock their account.

### Access Administration

State Street has dedicated Security Administration groups within IT or support teams within the business unit responsible for administering access to production applications, databases and operating systems, including the corporate network, and tools used to manage job scheduling, event monitoring and backup management control activities.

Access to production applications is managed through various processes. For certain applications, multiple levels of authentication may be required and the provisioning of each level of authentication may be managed by different groups. Please refer to Section III B *Application Listing*, which identifies the Security Administration process for each of the in-scope applications, which are further described below:

- SailPoint: A self-service tool for identity storage, access requests and entitlement provisioning. For access managed in SailPoint, access requests are managed through designated approval processes, with restricted access approved by designated authorized approvers.

- Security Administration Services ("SAS"): Responsible for access administration for certain core applications. For access not administered by SailPoint, access requests are submitted using a web-based access request tool that automates the initiation, approval routing, and business unit notification of user access requests or via email.

- International Security Administration Services ("ISAS"): Responsible for regional centralized access administration for applications within the EMEA and APAC regions. For access not administered by SailPoint, access requests are submitted and actioned via a web-based ticketing tool or via email.

- SSGA Security Administration ("SSGA IT"): Responsible for access administration for SSGA IT applications. User Provisioning System ("UPS"), a role-based access system, is also used to support access recertifications for SSGA applications and environments on a periodic basis and at least once every calendar year.

- AIS IT: A dedicated group within TPEO is responsible for access administration for applications supporting the Alternatives sector.

- Application Specific Security Administration: Based on business requirements, designated support teams perform Security Administration for certain business aligned applications. The people, process or technology used to manage the security administration process is unique to each application.

- Enterprise Security Framework ("eSF"): For certain applications, including those residing in the Private Cloud, access administration functions for employees and contingent workers are administered through eSF, a self-service tool for access requests and entitlement provisioning.

Additional information about the access administration process for State Street permanent employees and contingent workers globally is described in further detail below:

### Access Authorization and Modification Requests

User access is managed through the joiner, leaver and mover processes to help ensure user access rights are appropriate to the user's job responsibilities/function. New access requests are managed through designated approval processes, with restricted access approved by designated authorized approvers. Initial access to the State Street corporate network (i.e., Active Directory LAN) is provisioned to new employees and contingent workers automatically through the SailPoint birthright provisioning automated process (aka Joiner). Managers initiate access requests through SailPoint self-service or using Business as Usual ("BAU") processes for entitlement access not supported by SailPoint. Privileged access follows the standard IAM controls but would have an additional level of approval to ensure access is appropriate and is restricted to technology operational roles. Where technically feasible, certain privileged access activity is logged and certain high risk events are monitored within the SIEM tool (see Security Monitoring section below).

Designated State Street personnel communicate transfers and terminations for permanent employees and contingent workers to GHR and Global Procurement Services, respectively. GHR and Global Procurement Services are primarily responsible for updating the work location and/or department in the HRMS application. However, designated State Street personnel may also have the ability to update the HRMS application directly. Designated State Street personnel may also submit an access modification request to State Street Security Administration personnel as a result of a change in a permanent employee's or contingent worker's job responsibilities, a recertification or as the result of a transfer. Upon daily notification of movers from the HRMS application, for certain applications on SailPoint, the user's access is automatically taken "back to birthright" or a notification is sent to the employee and their manager to review the access remains appropriate based on the employee's current job responsibilities. Please refer to the relevant SailPoint footnote within Section III B *Application Listing* for details.

For access administered outside of SailPoint, access authorization and modification requests may be submitted to SAS, ISAS or dedicated State Street Security Administration groups through email or through the access request tools. For access requests submitted through access request tools, these tools have been configured to help enforce segregation of duties between access requestors and access approvers. For access requests submitted to the Help Desk or dedicated State Street Security Administration groups through email, Security Administration personnel manually review the access request for completeness and determine whether approvals are appropriate by cross-referencing the listing of authorized approvers or validating that the individual approving the access request is the permanent employee's or contingent worker's hiring manager, supervisor or higher level individual within the same business unit. In addition, State Street Security Administration personnel also manually check that the access approver is not the same individual for whom the access is being requested.

Access is granted by State Street Security Administration personnel according to the access privileges specified in the access request. State Street Security Administration personnel responsible for processing an access request are not involved in the approval of that same access request.

Administrator IDs with the ability to grant access to production applications, databases and operating systems, and the corporate network are restricted to designated business and/or IT personnel through the Firecall ID process, as described later in this section, or to designated State Street Security Administration personnel.

### Access Revocation Requests

Designated State Street personnel communicate terminations for State Street permanent employees and contingent workers to GHR and Global Procurement Services, respectively. GHR and Global Procurement Services are primarily responsible for updating the employment status in the HRMS application for employees or in the Contingent Labors application for contingent workers with the last date worked and termination date. The Contingent Labors application sends an automated feed to the HRMS application daily, except for Saturday and Sunday. Designated State Street personnel may also have the ability to update the HRMS application directly.

For employees and contingent workers whose termination request was entered more than five business days post-termination date, GHR and Contingent Labor Support, respectively, perform a monthly review of logical and physical access to determine whether access was used for the period between the termination date and when the termination request was entered into the HRMS application. Access usage, if any, is documented and analyzed for potential impact and tracked to resolution.

Daily, an automated feed containing terminated permanent employee or contingent worker status from the HRMS application is sent to security administration tools for access revocation.

For access managed by SailPoint, the leaver process initiates removal of a user's access for users identified by GHR as terminated. For conforming applications (communicate via connector), access is automatically removed by SailPoint. For non-conforming applications, SailPoint initiates a work item to security administrators who manually remove the access. Active Directory LAN accounts are disabled and moved to a terminated organizational unit ("OU") on termination day 1. The Active Directory LAN account is then deleted on day 31.

User IDs for the Mainframe, Linux and UNIX operating systems and database user IDs for permanent employees and contingent workers in select work locations are automatically deprovisioned through Security Administration tools based on the reported termination date except for SSGA IT. SSGA IT IDs are manually deprovisioned by Security Administration personnel. For other user ID revocation requests that are not managed through Security Administration tools, GHR sends a Joiners and Leavers report to dedicated State Street Security Administration personnel groups through email on a daily, weekly or biweekly basis. State Street Security Administration personnel may also manually generate a GHR report to identify permanent employees' or contingent workers' termination status, to determine access that needs to be revoked, and then manually disable or delete user IDs.

An "expedited" termination process exists for urgent/sudden high-risk terminations where manual notification from GHR is sent to State Street Security Administration personnel for immediate access revocation. The HRMS application or the Contingent Labors application is subsequently updated manually by GHR to reflect a permanent employee's or contingent worker's termination status, respectively.

### Access Recertification Activities

Access to production applications and privileged access for operating systems, databases, job scheduling, event monitoring, and backup tools is restricted to designated State Street personnel based on job responsibilities and is reviewed on a periodic basis and at least once every calendar year by designated State Street business and/or IT personnel. Access recertifications for production applications are executed in various ways based on the application as noted in Section III B *Application Listing*.

#### SailPoint

The IAM Centralized Certification team uses an automated recertification tool to perform access recertifications for certain applications and infrastructure and business privileged applications including database and operating system levels as well as access approval authority and change approvers, on a periodic basis and at least once every calendar year. Recertifications are performed for database and operating system administrator IDs as part of the infrastructure and privileged access review. Recertifications for application level administrator IDs are performed as part of the general access recertification through SailPoint or through the infrastructure and privileged access review.

The list of users and respective entitlements are programmatically or manually delivered to a secure location for collection into the recertification tool. A comparison check is performed to evaluate the data from the source file against the data pulled into the automated recertification results. This comparison check confirms the completeness of the data collection for the recertification. For any user IDs that cannot be matched to the hierarchical manager based on the HRMS record, the IAM Centralized Certification team is responsible for researching and re-assigning the entitlements to a new manager.

After activation of the review, the recertification tool sends an email notification to each user's hierarchical manager based on the HRMS record. The hierarchical manager is required to log in to the tool and select the appropriate access recertification decision. For infrastructure and business privileged applications reviews, the hierarchical manager's business unit senior manager or above is required to sign off on each manager's recertification decision.

Upon completion of the automated access recertification, items not reviewed are marked for revocation and the review is closed online. Upon request, a report summarizing revocation requests and review decisions is generated by the tool. This Revocation Report is sent to Security Administration teams for processing as required.

The automated recertification tool automatically enforces segregation of duties, preventing users from recertifying their own access.

The Security Administration team notifies the IAM Centralized Certification team when the requested revocations are completed and a validation process is performed to confirm that access identified for revocation has been removed. A new programmatic or manual file is used to re-run the collection process on the recertification tool and verify that all access marked for revocation has been processed. Upon review, if revocations have not been processed, the IAM Centralized Certification team notifies the Security Administration team, requesting completion of the outstanding revocations. Upon completion, the validation is re-run.

### SSGA User Provisioning System ("UPS")

SSGA IT utilizes User Provisioning System ("UPS"), a role-based access system, to support the recertification of SSGA user IDs by the users' manager for all SSGA applications, infrastructure and tools. In addition to the manager level general access recertification, UPS facilitates additional recertifications requiring business unit senior manager approval. Examples include privileged IDs, secondary or change approver, and Firecall ID owners.

See the *Access Authorization and Modification Requests* within this section for additional information on the process for submitting access modification requests as a result of the periodic access reviews.

### Manual Access Recertifications – Applications

For applications that are not recertified using an automated recertification tool, centralized groups or the business application owner are responsible for coordinating the manual execution of management's recertification of access. When necessary, the ID(s) requiring modification/deletions are communicated to State Street Security Administration personnel for processing. See the Access Authorization and Modification Requests within this section for additional information on the process for submitting access modification requests as a result of the periodic access reviews.

### Manual Recertifications – Administrator IDs

Administrator ID recertifications for applications, databases, operating systems and the corporate network are included in either an automated recertification described within the *Automated Application Recertification Tool* section above or recertified manually, depending on the platform or the Application Access recertification method. Administrator IDs with access to databases, operating systems and the corporate network are restricted to designated personnel based on job responsibilities and are reviewed on a periodic basis and at least once every calendar year by State Street designated IT managers at the SVP level or above. Administrator IDs with the ability to grant access to production applications, databases and operating systems and the corporate network are restricted to designated State Street Security Administration personnel and are reviewed on a periodic basis and at least once every calendar year by State Street designated IT or business managers, or are restricted to designated personnel through the Firecall ID process.

Reference the *Production Processing* and *Backup and Restore* sections for information on access recertification activities related to tools used to manage the job scheduling, incident management (e.g., event monitoring) and backup management processes.

#### Access Approver Recertifications

Except as described below, designated State Street personnel, IT designees or business units designees review State Street personnel authorized to approve access requests for new or modified access to production applications, databases, operating systems and the corporate network on a periodic basis and at least once every calendar year. Access approver responsibilities may be revoked for an authorized approver, if their approval authority is not reviewed by the designated business or IT manager in a timely manner. Access approver recertifications are performed using either the automated recertification tools as part of the infrastructure and business privileged applications recertification process described within the *Automated Application Recertification Tool* section above, or manually, depending on the application or platform.

Access administration processes for select applications follow organizational hierarchy for authorization of access requests and no periodic review is required. In such cases, access requests must be authorized and approved by the permanent employee's or contingent worker's hiring manager, supervisor or higher level individual within the same business unit. These applications include: Colline, Dual Verification Database, FeeCom, Global Services Reconciliation, GP3, Japan Accounting and Reporting System and T-STAR/TX.

See the *Access Authorization and Modification Requests* within this section for additional information on the process for submitting access modification requests as a result of the periodic access reviews.

### Network Security

Internet access to and from State Street's network is controlled by firewalls installed at each of the internet access points. Internet firewall rules are reviewed quarterly by designated State Street IT personnel. Changes to firewall rules follow the Operating System Change Management Process.

### Production Data Access

Firecall IDs are used to provide authorized personnel with read and/or update access to production data to upgrade third-party vendor applications, resolve production processing problems or support change management activity. Firecall IDs supporting applications, databases and operating systems are either granted to approved requestors or are activated by escalating the access privileges of an existing requestor's user ID.

The Firecall ID process is managed by the following IT departments:

- Security Administration Services ("SAS") utilizing a manual deactivation ("SAS Manual") – OpenVMS, Tandem, and RACF platforms and the GlobalOne, Minerva and Sentinel applications

- SAS utilizing an automated deactivation ("SAS Automated") – application, database, and operating system level IDs for SAS managed applications not following the SAS Manual Firecall process
- SSGA Security Administration ("SSGA IT") – application, database, and operating system level privileged IDs for SSGA IT managed applications
- Technology Platform Engineering and Operations ("TPEO") – application, database, and operating system level IDs for the remaining in-scope applications

Firecall ID access request processes above require the requestor to initiate a Firecall ID access request describing the reason for the access and/or reference of a change request or incident management ticket number. Firecall IDs are approved by designated State Street IT or business personnel. Authorized State Street IT and business approvers are reviewed manually or through automated tools periodically, at least annually, by a designated business unit senior manager or above for appropriateness. Firecall ID passwords are reset manually or automatically based on predetermined time parameters, generally not to exceed 24 hours.

For SAS administered Firecall IDs, the requestor submits the Firecall ID access request form or the ServiceNow request to designated State Street personnel who are authorized to approve Firecall access requests. The authorized approver reviews the Firecall ID access request form for reasonableness and subsequently forwards their approval via email to the SAS Help Desk mailbox, or approves the ServiceNow request within the tool, to authorize State Street Security Administration personnel to grant access to the requested Firecall ID. State Street Security Administration personnel manually check that the Firecall ID access request approver is not the same individual for whom the Firecall ID access is being requested. ServiceNow enforces this automatically. Firecall ID access requests exceeding 24 hours require an additional ISO and SVP approval prior to granting the access. When the requestor calls the SAS Help Desk for a Firecall password, they are authenticated by Voice Bio. Additional authentication procedures are required if requestor is not able to authenticate via Voice Bio. SAS then confirms that the request was approved prior to issuing the password. In the event of an emergency, SAS will release the Firecall ID without pre-approval from an authorized approver as long as the requestor provides completed documentation relating to the request as well as the name of the individual who will be the authorized approver. Final request form and approvals will be obtained within 24 hours of request fulfillment.

For SSGA IT, Firecall and Business Support IDs are approved by an MD or above when created. Firecall IDs are used to diagnose and correct production emergencies, while non-emergency support functions utilize Business Support IDs. When the requestor calls the SAS Help Desk for a Firecall or Business support password, they are authenticated by Voice Bio. SAS then confirms that the request was approved prior to issuing the password. For Business Support IDs, a change ticket is required before the ID will be activated by the Help Desk. Business Support IDs follow the same controls as the Firecall IDs; therefore references to SSGA "Firecall IDs" within Section IV are inclusive of Business Support IDs. Firecall and Business Support

IDs are automatically deactivated, except for Minerva and Sentinel which are manually deactivated, within predetermined time intervals not to exceed 24 hours, except when opened for a weekend, where it is not to exceed 48 hours. SSGA Firecall ID owners are recertified through their annual recertification process and approved by an MD or above.

For TPEO administered Firecall IDs, the self-service security tool has been configured to help enforce segregation of duties between Firecall ID access requestors and approvers. In addition, the self-service security tool requires entering a change request or an incident management ticket number. In the case that the change request or incident management ticket number is not available, a description of the reason for the Firecall ID usage is required. For the Linux, UNIX, and Windows operating systems and supporting databases, certain users are pre-approved to elevate their access privileges to perform functions as part of their job responsibilities. Users are required to provide a change request, incident ticket or a description of the reason for elevating their access. Access is automatically deactivated based on predetermined time parameters, generally not to exceed 24 hours. Users with the ability to elevate their privileges are reviewed at least annually by business unit senior managers as part of the infrastructure and privileged access review.

### Security Monitoring

#### Cybersecurity Program

State Street's Global Cybersecurity ("GCS") organization defines and manages the enterprise-wide Information Security Program. GCS partners with IT, corporate offices and business units to implement controls designed to protect information assets. State Street's program currently aligns to the National Institute of Standards and Technology ("NIST") Special Publication 800 53R4 standard and is in the process of aligning to the NIST 800 53R5 revision.

The components of the program are:

**Cybersecurity Center**

- Analyzes areas such as authentication activities, risky privilege combinations, unusual printing activity, suspicious and/or inappropriate web activity, data leakage vulnerabilities, unusual web use, etc.
- Performs analysis of correlated events to more fully understand behavior and proactively identify scenarios that could lead to abuse.
- Creates actionable reporting for management, focusing on identification of emerging threats and opportunities to enhance management of security.

**Cyber Defense Center ("CDC")**

- Consists of a 24x7x365 Security Operations Center ("SOC") together with a Cyber Fusion Center, which jointly focus on enhancing network security monitoring and providing an agile, dynamic response capability. These resources allow State Street to perform near real-time monitoring of security events to identify and address risky and suspicious activity. The SIEM suite of tools collects log data from the firewall, performs intrusion detection/prevention, uses proxy and other security logging tools and generates security-related alerts as t hey occur. The SIEM monitors inbound and outbound web traffic, as fed to the SIEM through SSC system monitoring data feeds, to detect malicious web activity and provide a defense against shareware, malware and access to unauthorized software. Identified issues are reported centrally to the Security Operations Center and IT management.

- Provides cybersecurity monitoring, event correlation and security incident management across IT infrastructure elements.

- Regularly analyzes security information from multiple sources and industry forums to identify potential vulnerabilities.

In addition, State Street shares information on cyber threats and engages in cross-sector collaboration. Four external organizations, the Financial Services Information Sharing and Analysis Center ("FS-ISAC"), the Financial Systemic Analysis and Resilience Center ("FSARC"), the Analysis & Resilience Center ("ARC") for systemic risk, and the Financial Services Sector Coordinating Council ("FSSCC"), serve as the basis by which the financial services sector develops critical infrastructure protection policy and shares cybersecurity and other threat data.

Certain privileged access activities for platforms are captured through the SIEM tools. Automated alerts are generated through this tool to cover specific privileged access activities. Activities monitored include production library modification, critical security configuration modifications and failed logon attempts for some platforms (refer to the below table for monitoring activities per platform). The in-scope operating system platforms are covered by this monitoring where technically feasible (i.e., the platform can create a log and events are captured); including RACF, Mainframe, Tandem, Windows, Linux, UNIX, and OpenVMS.

| Monitoring Activities | RACF/Mainframe | Tandem | Windows (Domain Controller) | Linux/UNIX | OpenVMS |
|---|---|---|---|---|---|
| Production Library Modification | Yes | No | No | No | No |
| Failed logon attempts | No | No | Yes | Yes | No |
| Critical Security Configuration | No | Yes | No | No | Yes |

For all in-scope platforms other than Mainframe and OpenVMS, events are sent as they occur. Mainframe and OpenVMS events are sent through an overnight batch cycle. Alerts are reviewed within two business days by GCS personnel and escalated to designated State Street IT personnel as necessary for further action.

## Change Management

### Policies and Procedures

State Street has developed and implemented written policies and procedures to guide personnel through the development of production applications and the process of making changes to existing production applications, databases and operating systems.

### Systems Development Lifecycle

A State Street-approved Systems Development Lifecycle ("SDLC") methodology is required to be followed for the development and acquisition of production applications. The SDLC methodology consists of two frameworks: Waterfall (DPF, SRF, SF (in support of SSGA)) and Agile (SCRUM, Kanban, Scale). The Framework defines the core quality standards underlying the development process and provides a flexible yet disciplined methodology, consistency, a common language and defined accountabilities. Each framework has approaches that refer to process models for system development (e.g., DPF, SRF, SF, iA SCRUM, iA Kanban, iA Scale). Techniques are the methods used to accomplish an activity and/or produce deliverables. Tools facilitate the management of the development process and the completion of deliverables. Project documentation is developed in accordance with written SDLC policies and procedures for application development projects.

Technology development and acquisition projects follow one of the following SDLC frameworks:

- **Industrialized Agile Software Development ("Agile"):** Agile is an interactive development process based on the principles of collaboration, adaptability and continuous improvements. Requirements and solutions evolve through collaboration between cross-functional teams, including users, promoting iterative, rapid and flexible response to change and consisting of the following approaches:
  - **SCRUM:** SCRUM is an incremental, iterative approach that brings customer and the implementation team together to deliver valuable business outcomes based on a customer feedback.
  - **Kanban:** Kanban is an incremental approach that optimizes flow of value to deliver results consistently.
  - **Scale:** Scale uses SCRUM in its foundation with the ability to align multiple component and/or feature-based teams.
- **Waterfall:** A linear approach to software development, including the following:
  - **Development Process Framework ("DPF"):** DPF is the methodology used for developing large-scale technology projects and consist of Ideation (includes funding approval), Analysis (details documentation of business requirements), Design (detail documentation of technical design and requirements), Development (code development), Test (code testing), and Deployment (code deployment to production) phases. These phases are managed using detailed project plans and milestones. Each phase consists of milestones delivery and proper documentation capture and approval.
  - **Small Request Framework ("SRF"):** SRF has been created as an abbreviated lifecycle methodology, based on the DPF, to specifically address small request and enhancement projects.

- **Sequential Framework ("SF"):** SF has been created as an abbreviated linear lifecycle methodology to allow the development work to progress in sequential phases. The initial scope of the deliverable is defined in the Initiate Phase and subsequently moves through the phases of Analyze/Select/Architect, Develop/Accept, and finally Deploy.

State Street licenses certain applications from third-party vendors who are responsible for the application code development.

State Street is responsible for following the SDLC methodology relevant to the acquisition of the production applications and maintains responsibility for testing and approving application functional changes. State Street is responsible for releasing the changes to State Street's production environment, as described below and within Control Objective 3.

### Change Management Process

State Street utilizes a formal change management system to document and assign application, database, and operating system change requests. Change management requests for application, database, and operating system changes utilize ServiceNow or designated tools to standardize the methods and procedures for the change request lifecycle from initial request through closure.

For all application, database, and operating system changes, except Colline, responses to predefined questions relating to the nature, timing and extent of the change, as well as the results from the change risk calculator, a risk rating and corresponding "change type" is systematically applied by ServiceNow to the change control record. The Change Risk Approval Policy documents the required approvals related to each change type. The Change Advisory Board ("CAB") is in place to review and approve major, critical, or emergency risk-rated changes and to assess the impact to the environment. The CAB meetings take place no less than weekly and are attended by representatives from each service delivery infrastructure and application area. The change types and required approvals include:

- **Standard Pre-Approved Changes:** Eligible infrastructure database and operating system changes that have been successfully implemented and approved at least ten times previously are systematically pre-approved and do not require additional approvals as long as the criteria in the change control record aligns with the standard pre-approved change.

- **Low Changes:** Requires first line approval by IT personnel. Required approvals must be obtained within ServiceNow, prior to implementing the change. In the event of a production outage, the emergency change management process is followed.

- **Medium Changes:** Requires first line approval by IT personnel, as well as approval by Designated Approvers and Application or Infrastructure Reliability Operations Approvers, prior to implementation of the change.

- **Major or Critical Changes:** Requires first line approval by IT personnel similar to Medium changes, as well as approval by Designated Approvers and Application or Infrastructure Reliability Operations and approval by the CAB. Required approvals must be obtained within ServiceNow prior to implementing the change.

- **Emergency Changes:** Infrastructure database, operating system and application changes require approvals by authorized individuals. Emergency change approvals can be documented in the ServiceNow Change Request subsequent to the emergency change implementation.

### Application, Database, and Operating System Changes – Testing and Approval

Production application, database, or operating system changes may be requested by State Street personnel, which may include business users, production support, or the BCIO group. Changes for databases and operating systems may also be requested by System Administrators. The BCIO group includes project managers, business analysts, application support personnel and application developers. For situations where State Street does not own the source code, vendors may also provide State Street with a new application release or upgrade or develop changes based on State Street business requirements.

Testing is required in a User Acceptance Testing ("UAT") environment for functional changes prior to change implementation, defined as changes (including vendor provided patches) that affect the business logic or usability features of the application. Changes are tested where technically feasible and testing is reviewed prior to approval. Testing for functional changes is performed by designated State Street personnel, which may include business users and/or SQA or an automated tool. Technical changes, including performance improvements, configurations, sizing and job script changes that do not affect the business logic, are reviewed and tested, where technically feasible, by State Street personnel, which may include business users and/or SQA. Defect identification and tracking is also conducted during the testing process for both functional and technical changes.

Except Colline, all application, database, and operating system changes require ServiceNow tickets and documentation. The following processes require additional approvals:

- For Business Objects, Cash Management Instruction, FundSuite SX, and Great Plains applications, changes are requested and approved through designated ticketing tools or email.

- For the Colline application, changes are requested, tested, and approved by State Street through the application service provider's ticketing tool.

### Application, Database, and Operating System Change Implementation

IT personnel responsible for change implementation activities check that necessary change approvals are obtained and documented in the change management package, ticket, or tool prior to implementing application changes, database and operating system changes to the production environment. Change management tools may be used to obtain and document approvals from designated State Street personnel. Changes may be implemented to the production environment by the applicable library management tool or State Street IT personnel using designated access or Firecall IDs. Change implementation may also be performed through an automated tool by designated IT personnel. Application, database, and operating system changes should not be implemented by IT personnel to the production environment if approvals or required testing are missing or are not from designated IT personnel authorized to approve the change.

Access to tools used to manage change implementation activities, including managing versions of application source code libraries, are restricted to designated IT personnel based on job responsibilities.

### Change Approver Recertification

Personnel that are designated to approve application, database, and operating system changes are reviewed on a periodic basis and at least once every calendar year by State Street business or IT unit senior manager or above. Refer to the *Access Recertification Activities* section above for further details on the SailPoint recertification process. Application-change management processes for the Colline application have a small number of change approvers and no periodic review is required.

### Segregation of Duties

Separate UAT and production environments exist to segregate application testing and change implementation activities.

State Street IT personnel with the responsibility to develop application changes are segregated from State Street IT personnel with change implementation responsibilities. Access privileges for application development and change implementation activities are enforced through library management tools, file system security permissions, Systems Administrator level access or through eSF access entitlement tools.

Library management tools may also be used to manage versions of the application source code and/or restrict access to executable code libraries, which are used to move compiled executable code changes from UAT to production. Library management tools time-and-date stamp the application source code, to provide an audit trail of changes performed by State Street IT personnel.

### Development of Macros

Macros may be used by State Street users to facilitate certain data analysis activities. Users can submit a new macro or modification request to Global Macro Automation Services ("GMAS") through its website.

A standard request form on the GMAS website is completed by the requestor to initiate a new macro or modification request. Once the request form has been completed, a Developer creates the macro for a new request or makes the enhancements for a modification. The Developer then uses the Multi Document Interface ("MDI") Validation tool to validate the macro adheres to the outlined GCS standards, lock down the macro code and any cells with formulas and add the versions control. The Developer then uploads the MDI validated macro and the MDI encrypted file to the GMAS website for Business Team approval. Macros identified by the MDI Validation tool that need additional code review will go through a Code Review Process before being moved to the Business Team approval stage. Macros that do not require any additional code review will move to the Business Team approval stage. The Business Team Owners assign a tester that can approve or reject the macro. After all Business Teams approve the macro, the macro moves into production and is available on the GMAS production website.

## Production Processing

### Policies and Procedures

State Street has developed and implemented written policies and procedures to guide State Street personnel through production processing activities, including making changes to job schedules in the production environment and monitoring and responding to incidents.

### Job Scheduling Process

Designated State Street personnel are responsible for processing and approving changes to jobs, emergency schedule change requests and job failure resolution. Changes to job schedules are authorized and approved by appropriate personnel prior to implementation in the production environment.

Job schedule change requests for applications (other than Alpha Frontier, Caliber™, Enterprise Reporting Platform, Investment General Ledger System, Investor Services System, Mosiki and Wall Street Office (Alternatives) and SSGA IT) residing on Mainframe, OpenVMS, Linux, UNIX and Windows operating systems are submitted to designated personnel who review the requests and validate that each request was made by a valid approver and included the job script and valid job code.

For applications residing on the Tandem operating system, applications running in the Private Cloud and the following applications: Alpha Frontier, Caliber™, Enterprise Reporting Platform, Investment General Ledger System, Investor Services System, Mosiki and Wall Street Office (Alternatives) and SSGA IT applications, job schedule changes follow the change management process.

Update access to job scheduling tools is restricted to designated IT personnel based on job responsibilities and is reviewed on a periodic basis and at least once every calendar year by a designated IT senior manager or above. The process for requesting and granting access to job scheduling tools follows the *Access Administration* process described in the *Logical Access* section.

### Incident Management Process

Incident management and event monitoring tools are used by designated IT personnel to identify transaction processing interruptions and assign a severity level to prioritize resolution. The severity level is either automatically assigned by event monitoring tools or manually updated by designated IT personnel based upon documented severity levels in the Standard Operating Procedures. Alert priorities are dependent on type of application or transaction and time of day.

Certain production jobs are monitored by designated IT personnel for successful completion through the use of event monitoring tools. Designated IT personnel are notified of a failed job by a service request ticket or email. Certain jobs are configured to automatically create service request tickets or emails. Alerts are tracked, prioritized and addressed by designated IT personnel in a timely manner.

Update access to event monitoring tools is restricted to designated IT personnel and is reviewed on a periodic basis and at least once every calendar year by State Street ISOs and/or designated managers at the IT Senior Manager or above. The process for requesting and granting access to event monitoring tools follows the *Access Administration* process described in the *Logical Access* section.

Production processing incidents are tracked through various reports, email communications and meetings, which may include:

- Data Center Status report – A report which summarizes prior day major incidents and outages for aspects of the production environment which includes all platforms and their servers. Outstanding incidents remain on the report until resolved.

- Daily IT Operations Risk Review – Daily meeting to review the incidents from the Daily IT Operations Risk Review report and a summary of major incidents impacting service levels and the business are being communicated to State Street Executive Management.

- Problem Initiation Review – Daily meeting to review major incidents with IT personnel to begin Root Cause Analysis.

### Problem Management

Monitoring software is used by the GTS Network Architecture group to identify system interruptions and to classify each interruption according to a specified level of severity. The monitoring software automatically sends out an alert to management when predefined thresholds are reached. Processing issues and errors are logged into the CRM tool to facilitate the identification/avoidance of recurring issues, allowing tracking and research of problems to resolution. Escalation and crisis management procedures are documented to provide guidance to system administrators for the communication of production processing issues to the appropriate individuals.

The Incident Management policies and procedures are reviewed annually to confirm accuracy. The IT Service/ Help Desk identifies, logs, and escalates incidents, as needed, to assure tracking of remediation.

The CDC analyst assigned to the security event completes key fields about event details within ServiceNow before the ticket is closed. This provides the source of information about performance and operational issues, and documents identification and execution of remedial actions. Root Cause Analysis is used by the CDC following incident resolution as appropriate. The team sends metrics and reports to Senior Management.

IT senior management receives a daily report from GCS that documents incidents. In this way, affected stakeholders receive notification of the impact of incidents.

## Backup and Restore

### Policies and Procedures

State Street has developed and implemented written policies and procedures to guide State Street personnel through the process of performing backups of applications and data, sending backups off-site and processing data restore requests.

### Backup Management Process

State Street uses backup management and job scheduling tools to manage the process of performing and monitoring backup management activities. Appropriate IT personnel research backups failures and resolve or escalate them through the incident management process described in the *Production Processing* section. Specific information about backup management processes are as follows:

- Mainframe applications and operating systems – Backup management tools have been configured to perform full backups weekly and incremental backups daily. In certain cases, tape backups are also performed. Applications and data are copied by backup management tools directly to virtual drives located at State Street's disaster recovery site.

- Linux (including applications in the Private Cloud), UNIX and Windows operating systems – Backup management and job scheduling tools have been configured to perform daily incremental backups of operating system and application data onto virtual tape libraries. The virtual tape libraries are also replicated daily to off-site recovery locations. For certain data that continues to be backed up to tape, backup management tools perform daily backups onto two sets of backup tapes. The first set of backup tapes is stored on-site, while the second set of backup tapes is sent to an off-site location.

- Tandem and OpenVMS operating systems – Real-time data replication occurs daily for Tandem and OpenVMS to off-site recovery locations. Operating system utilities and automated tools are used to schedule tape backups for Tandem and OpenVMS, respectively. Tape backups are performed using a combination of automated tool processes and tape management tools. The backup schedule is customized according to application needs. The schedule is implemented through automated tools for OpenVMS and Tandem.

Update access to backup management tools is restricted to designated IT personnel based on job responsibilities and is reviewed on a periodic basis and at least once every calendar year by the State Street ISO or designated business or IT manager. The process for requesting and granting access to backup management tools follows the *Access Administration* process described in the *Logical Access* section.

### Data Restore Process

A service request ticket is created for data restore requests submitted through service request tools. Once the data restore has been performed by IT personnel, the business user who made the request is notified that the data restore has been completed. The service request tool is configured to request confirmation from the business user that the restore was completed as requested.

# Section IV

## State Street's ITGC Control Objectives and Related Controls and Additional Information Provided by the Independent Service Auditor

### A. Control Objectives, Controls and Tests of Operating Effectiveness

The description of control objectives and related controls are the responsibility of State Street management and are an integral part of management's Description of their ITGC system. The control objectives are as follows:

1. Controls provide reasonable assurance that physical access to data centers and computer rooms is restricted to authorized personnel based on business need.

2. Controls provide reasonable assurance that logical access to production applications, databases and operating systems, including the corporate network, is restricted to authorized personnel based on business need.

3. Controls provide reasonable assurance that a Systems Development Lifecycle ("SDLC") process is followed for the development of production applications, and changes to production applications, databases and operating systems follow a documented change management process that requires changes be tested, approved and implemented by authorized personnel to support the effective functioning of application controls and to result in the complete, accurate and timely processing and reporting of transactions and balances.

4. Controls provide reasonable assurance that processing of production applications, databases and operating systems is authorized and executed in a complete, accurate and timely manner, and production processing failures are identified, tracked, recorded and addressed in a complete, accurate and timely manner.

5. Controls provide reasonable assurance that production applications and data are regularly backed up and are available for restoration in the event of processing errors and/or unexpected interruptions.

### Description of EY Tests Performed

The procedures performed to test operating effectiveness are listed next to each of State Street's respective control objectives and control procedures, and are the responsibility of Ernst & Young. Test procedures in connection with determining the operating effectiveness of controls are described below.

#### Test Description

Inspection

Assessed and examined documents and reports that contain an indication of performance of the control. For example, reading documents and reports to determine whether logical access requests are documented and user access is granted as requested.

### Observation

Witnessed on a sample basis, the performance of controls by organizational personnel. For example, viewing the functionality of applications to determine whether a valid user ID and password is required.

### Inquiry

Interviewed applicable State Street personnel about the relevant control descriptions, processes and procedures.

Information technology general controls administered by State Street are listed below. Unless otherwise specified, these controls apply to the applications, operating system and database environments listed in the *Application Listing* in Section III B.

### Information Produced by the Entity

When using information produced by the entity ("IPE"), EY evaluated whether the information was sufficiently reliable for our purposes, including, as necessary, obtaining evidence about the completeness and accuracy of the information and evaluating whether the information was sufficiently precise and detailed for our purposes (e.g., controls requiring system-generated populations for sample-based testing and reports used by management in the performance of controls). These test procedures were performed as a component of evaluation and testing the controls identified by State Street. The types of information produced by State Street that EY obtained as evidence may have included, but was not limited to:

- Standard reports that are configured within an application
- Parameter-driven reports generated by an application
- Reports generated to facilitate testing of control populations
- Custom reports that are not configured within the application (i.e., scripts, report writers and queries)
- Spreadsheets that include information utilized for the performance or testing of a control
- Analyses, schedules or other evidence manually prepared

EY performs a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used:

1) Inspect the source of the IPE;

2) Inspect the query, script, or parameters used to generate the IPE;

3) Compare/agree data between the IPE and the source; and/or

4) Inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity.

## Control Objective 1

Controls provide reasonable assurance that physical access to data centers and computer rooms is restricted to authorized personnel based on business need.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| **Policies and Procedures** | | |
| 1.1 State Street has developed and implemented written policies and procedures to guide personnel through the process of requesting and granting access to facilities, including data centers and computer rooms for permanent employees and contingent workers. | Inquired with Global Security personnel and inspected written policies and procedures including revision history to determine whether current documentation existed to guide personnel through the process of requesting and granting access to facilities, including data centers and computer rooms. | No deviations noted. |
| **Physical Security Administration** | | |
| 1.2 Requests for access to data centers and computer rooms must be submitted to designated IT personnel. Designated Data Center Operations personnel are authorized to approve access requests to data centers and computer rooms based on the business need for the access requested. Global Security will process approved access requests. | For a sample of permanent employees and contingent workers granted access to data centers and computer rooms, inspected access request documentation to determine whether the access request was approved by designated Data Center Operations personnel and processed by Global Security Personnel. | No deviations noted. |
| | Inspected queries/parameters used to generate the data center and computer room access listings used to select the testing sample in order to determine whether the queries/parameters included appropriate selection criteria for user access and their entitlements. | No deviations noted. |
| 1.3 Global Security personnel are notified of a permanent employee's or contingent worker's termination status in a timely manner. The Human Resources Management System ("HRMS") application sends a file to the physical security management tool, used to assign and manage access card information to data centers and computer rooms globally. Through automated job schedules (North America and Asia Pacific) or through an automated workflow process (Europe), the HRMS file automatically updates the terminated permanent employee's or contingent worker's expiration date in the access card record with the earliest of the termination date, agency end date or last date worked from the HRMS file. This file is sent daily, except for weekends and holidays. | Inspected job schedule configuration settings to determine whether the HRMS data was sent to the physical security management tools used to assign and manage access card information to data centers and computer rooms.<br>See Control Objective 4 for information about testing performed on job scheduling processes and controls. | No deviations noted. |
| | For a sample of terminated permanent employees and contingent workers with access to data centers and computer rooms, inspected the access card record to determine whether the expiration date matched the earliest of the termination date, agency end date or last date worked in the HRMS file. | No deviations noted. |
| | Inspected queries/parameters used to generate the data center and computer room access listings used to select the testing sample to determine whether queries/parameters used included the appropriate selection criteria for users, including the appropriate date selection criteria. | No deviations noted. |
| 1.4 Upon termination, a permanent employee's or contingent worker's access card is automatically disabled based on the expiration date in the access card record. | Inspected the access log and video surveillance of the disablement of a permanent employee's or a contingent worker's access card and subsequent attempt to gain access to facilities to determine whether the access was denied. | No deviations noted. |

## Control Objective 1

Controls provide reasonable assurance that physical access to data centers and computer rooms is restricted to authorized personnel based on business need.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| 1.5 Update access to physical security management tools is restricted to designated Global Security personnel based on job responsibilities. | Inspected a listing of user IDs with update access to physical security management tools to determine whether access was restricted to designated Global Security personnel based on job responsibilities. | No deviations noted. |
| | Inspected queries/parameters used to generate the physical security management tool update access list used in testing to determine whether queries/parameters used included the appropriate selection criteria for users. | No deviations noted. |
| 1.6 Access to data centers and computer rooms is restricted to designated permanent employees and contingent workers and reviewed at least annually by designated IT personnel to determine whether existing access remains appropriate based on job responsibility. Modifications to data center and computer room access privileges are communicated to Global Security personnel for processing. | Inspected access recertification documentation for in-scope data centers and computer rooms to determine whether the access of permanent employees and contingent workers was reviewed by designated IT personnel. | No deviations noted. |
| | For a sample of permanent employees and contingent workers identified in the data center and computer room access review as needing their access modified or revoked, inspected current data center and computer room listings to determine whether the adjustment requested by IT personnel was processed as requested. | No deviations noted. |
| | Inspected queries/parameters used to generate the access listings used in testing to determine whether the queries/parameters used included the appropriate selection criteria for users and their entitlements. | No deviations noted. |
| **Physical Access Controls** | | |
| 1.7 Access to data centers and computer rooms is secured with access cards, keypad readers and/or biometric devices. | For a sample of data centers and computer rooms, inquired and observed entry points to determine whether access cards, keypad readers and/or biometric devices were required to gain entry. | No deviations noted. |
| 1.8 Physical security management tools record access to data center and computer room entry points. Video cameras record access to data center entry and exit points. Global Security personnel monitor and respond to unauthorized activity at data centers and computer rooms. | For a sample of data centers and computer rooms, inquired with Global Security personnel and observed access card activity recorded by physical security management tools and video camera surveillance tapes to determine whether access to data centers and computer rooms was recorded, monitored and corrective action taken for unauthorized activity. | No deviations noted. |

## Control Objective 2

Controls provide reasonable assurance that logical access to production applications, databases and operating systems, including the corporate network, is restricted to authorized personnel based on business need.

| State Street Controls | EY Tests | EY Test Results |
| --- | --- | --- |
| **Policy, Standards and Procedures** | | |
| 2.1 The Global Cybersecurity ("GCS") group has developed the GCS Policy and implemented written information security standards to guide personnel through the process of managing and monitoring access to production applications, databases and operating systems, and the corporate network for permanent employees and contingent workers. | Inquired with GCS and Security Administration personnel and inspected written standards and procedures to determine whether documentation existed to guide personnel through the process of managing and monitoring access to production applications, databases, operating systems and the corporate network. | No deviations noted. |
| **User ID and Password Management** | | |
| 2.2 Permanent employees and contingent workers are required to access State Street's corporate network prior to authenticating at the application, database, and/or operating system-level through the use of a valid Local Area Network ("LAN") user ID and password combination. When accessing the network remotely, users are required to use multi-factor authentication. | Observed a permanent employee and a contingent worker log on to the corporate network to determine whether a valid LAN user ID and password was required to authenticate the users. | No deviations noted. |
| | Inquired with management and inspected system configuration evidence to determine whether connection to the internal network systematically required the use of two-factor authentication methods (e.g., SecurID token) for remote users. | No deviations noted. |
| 2.3 Authentication standards have been established by the GCS group and include single factor using a password or multi-factor leveraging a Secure ID Token with a password and/or PIN. Password and PIN standards have been established by the GCS group and require production applications, databases, and operating systems be configured by designated personnel (where technically feasible) to adhere to minimum requirements. A process exists for management to review password settings for production applications, databases and operating systems that do not comply with GCS standards and evaluate the potential risks and mitigating controls associated with the current password settings. | Inquired with GCS personnel and inspected the GCS Program requirements to determine whether single-factor password standards included password complexity, periodic password change, minimum password length and password history and multi-factor password standards included minimum PIN length and Secure ID token authentication systems. | No deviations noted. |
| | For production applications with application-level authentication, inspected password settings to determine whether password settings complied with the GCS password standards or obtained the review and evaluation to determine whether the potential risks and mitigating controls were identified for samples that did not comply with GCS standards. | No deviations noted. |
| | For databases and operating systems, including the corporate network and applications with database or operating system-level authentication, inspected password settings to determine whether password settings complied with the GCS password standards or obtained the review and evaluation to determine whether the potential risks and mitigating controls were identified for databases and operating systems that did not comply with GCS standards. | No deviations noted. |
| | Inquired with GCS personnel to determine whether a process is in place for management to review password settings that do not comply with the GCS standards. | No deviations noted. |

## Control Objective 2

Controls provide reasonable assurance that logical access to production applications, databases and operating systems, including the corporate network, is restricted to authorized personnel based on business need.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| 2.4 Security settings for operating systems have been configured by IT personnel to allow for a limited number of invalid access attempts before the account is locked. A time delay is in place for all disabled LAN user IDs before the user ID owner can re-authenticate to the system. A permanent employee or contingent worker who has locked their account is required to either contact the Help Desk or access an on-line self-service tool and provide at least two forms of identification to unlock their account. | Inspected operating system, including the corporate network, security settings to determine whether password and account lockout settings had been configured by IT personnel in accordance with GCS password standards to allow for a limited number of invalid access attempts before the account is locked. | No deviations noted. |
| | Inquired with Help Desk personnel and observed a user access the on-line self-service tool to determine whether two forms of identification were required to unlock an account. | No deviations noted. |
| **Access Administration** | | |
| 2.5 Access requests are documented and approved by designated personnel who are authorized to approve access requests to production applications, databases, operating systems and/or the corporate network. | For samples of new and modified permanent employees and contingent worker access, inspected access request documentation to determine whether the access request was documented and was approved by designated personnel who were authorized to approve access requests to production applications, databases, operating systems, and/or the corporate network. | For samples of 342 State Street new and modified permanent employees and contingent workers selected for testing across multiple access administration processes, EY identified the following deviation where access was granted without authorized approval:<br>• 1 of 16 users selected for testing with access to the Tax Efficient Lot Selector ("iTELS") and Automated Wash Sales ("AWS") applications<br>No deviations were noted for other access administration processes.<br>**Management Response**<br>Management acknowledges that although iTELS and AWS application gateway access was appropriately requested and approved for a new application support employee, the functional entitlements were separately provisioned by mirroring an existing application support employee's profile, without documented approval. Management has reiterated the requirement to document the request and approval for each entitlement. No changes to the entitlements were required as they were appropriate for the employee's job responsibilities.<br>Management further notes this is a unique access administration process specific to iTELS and AWS entitlements and there were no deviations noted for the other access administration processes as documented in Section III B. |

## Control Objective 2

Controls provide reasonable assurance that logical access to production applications, databases and operating systems, including the corporate network, is restricted to authorized personnel based on business need.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| (See previous page.) | For applications onboarded to SailPoint, inspected documentation for a sample of one to determine whether access administered outside of SailPoint was identified and approved. | No deviations noted. |
| | Inspected queries/parameters used to generate the listings used to select samples to determine whether the listings included the appropriate selection criteria for users, including the appropriate date selection criteria. | No deviations noted. |
| | For system-generated approver listings, inspected queries/parameters used to generate the listings to determine whether the queries/parameters used included the appropriate criteria. For manually maintained approver listings, inspected the Human Resource listing for job titles and performed inquiries to determine whether the approvers were designated personnel. | No deviations noted. |
| 2.6 Access is granted by dedicated Security Administration groups according to the access privileges specified in the access request. | For the samples of new and modified permanent employee and contingent worker access selected above for control 2.5, inspected access listings and/or system evidence to determine whether access was granted by dedicated Security Administration groups as requested. | No deviations noted. |
| | Inspected queries/parameters used to generate the listings used to select samples to determine whether the listings included the appropriate selection criteria for users, including the appropriate date selection criteria. | No deviations noted. |
| 2.7 Designated individuals who approve requests for new or modified access to production applications, databases, operating systems and the corporate network are reviewed on a periodic basis and at least once every calendar year by designated personnel (e.g., SVPs, IT designees or business units designees).<br>Access administration processes for select applications follow organizational hierarchy for authorization of access requests and no periodic review is required. In such cases, access requests must be authorized and approved by a manager. Please refer to Section III B for the list of applications. | For access approver recertifications performed during the period, inspected access approver recertification documentation for samples of designated individuals who approve requests for new or modified access to production applications, databases, operating systems and the corporate network to determine whether authorized access request approvers were reviewed on a periodic basis and at least once every calendar year by designated State Street personnel. | No deviations noted. |
| | Inspected queries/parameters used to generate the access approver listings used to select samples, and the post-review listing, and/or compared source system data against approver recertification documentation, as applicable, to determine whether the recertification was inclusive of the approvers. | No deviations noted. |
| | See control 2.5 for information about testing performed on access request authorization controls. | |
| | For samples of amendment requests resulting from the approver recertifications, inspected post-review approver listings to determine whether amendments were actioned appropriately. | No deviations noted. |

## Control Objective 2

Controls provide reasonable assurance that logical access to production applications, databases and operating systems, including the corporate network, is restricted to authorized personnel based on business need.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| 2.8 For access requests submitted through access request tools, these tools have been configured to enforce segregation of duties between access requestors and access approvers. For access requests submitted through the Help Desk or dedicated Security Administration personnel, Security Administration personnel manually check that the access approver is not the same individual for whom the access is being requested. Security Administration personnel responsible for processing an access request are not involved in the approval of that same access request. | For access requests submitted through certain access request tools, observed personnel submit an access request through the tools and attempt to approve their own access request to determine whether the tools systematically enforced segregation of duties between access requestors and access approvers. | No deviations noted. |
| | For access requests submitted through the Help Desk or dedicated Security Administration personnel, inquired with Security Administration personnel to determine whether manual checks were performed to enforce segregation of duties between access requestors and access approvers. | No deviations noted. |
| | For the samples of new and modified permanent employee and contingent worker access selected above for control 2.5, inspected access request documentation to determine whether the individual approving the access is not the same individual for whom the access is being requested and that Security Administration personnel responsible for processing an access request are not involved in the approval of that same access request. | For samples of 342 State Street new and modified permanent employees and contingent workers selected for testing across multiple access administration processes, EY identified the following deviations where a segregation of duties between access requestor, approver, and/or Security Administration personnel was not enforced:<br>• 1 of 12 for the Oracle Financials application<br>• 2 of 17 for the FundSuite ARC (EMEA) application<br>• 1 of 25 for the AIS IT access administration process<br>No deviations were noted for other access administration processes.<br>**Management Response**<br>For Oracle Financials and AIS IT, management acknowledges a bulk access request form for members of a fund services team was submitted by an authorized approver, which also included the approver on the form. Access was subsequently granted.<br>For FundSuite ARC (EMEA), the access request was approved and processed by the same access administrator.<br>Management confirmed all access was appropriate and reiterated the importance of enforcing an independent approval for all requested access. Management notes that the deviations resulted from unique access administration process specific to the |

## Control Objective 2

Controls provide reasonable assurance that logical access to production applications, databases and operating systems, including the corporate network, is restricted to authorized personnel based on business need.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| (See previous page.) | (See previous page.) | FundSuite ARC (EMEA) application and Oracle Financials/AIS IT and there were no deviations noted for other access administration processes as documented in Section III B. |
| | Inspected queries/parameters used to generate the listings used to select the samples to determine whether the queries/parameters used included the appropriate selection criteria for users, including the appropriate date selection criteria. | No deviations noted. |
| 2.9 Daily, an automated feed containing terminated permanent employee or contingent worker status from the HRMS application is sent to security administration tools for access revocation. | Inspected job schedule configurations to determine whether HRMS sends an automated feed daily to security administration tools used by Security Administration personnel to revoke access for terminated permanent employees or contingent workers. | No deviations noted. |
| | For a sample of terminated permanent employees and contingent workers, inspected the SailPoint Leavers workflow log and the HRMS application user profile to determine whether the reported termination date matched the earliest of the termination date or agency end date from the HRMS file. | No deviations noted. |
| 2.10 A permanent employee's or contingent worker's LAN user ID is disabled or deleted, either automatically through the security administration tool or manually by Security Administration personnel, based on the reported termination date in the GHR automated feed.<br>For permanent employees and contingent workers whose termination request was revoked more than five business days post-termination date, GHR and Contingent Labor Support, respectively, perform a monthly review of logical and physical access to determine whether access was used post-termination date. Access usage, if any, is documented and analyzed for potential impact and tracked to resolution. | For a sample of terminated permanent employees and contingent workers, inquired with Security Administration personnel and inspected the activity log in security administration tools or Active Directory audit tools to determine whether the LAN user ID was disabled or deleted. | No deviations noted. |
| | Inspected the queries/parameters used to generate the HRMS list used to select the sample to determine whether queries/parameters used included the appropriate user criteria. | No deviations noted. |
| | For a sample of months, inspected termination monitoring documentation to determine whether contingent workers/permanent employees whose access was revoked more than five business days post-termination date were identified, documented, analyzed and tracked to resolution. | No deviations noted. |
| | Inspected the queries/parameters used to generate the listings for the termination review to determine whether the listings included the appropriate selection criteria, including the appropriate date selection criteria. | No deviations noted. |

## Control Objective 2

Controls provide reasonable assurance that logical access to production applications, databases and operating systems, including the corporate network, is restricted to authorized personnel based on business need.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| **Automated Recertifications** | | |
| 2.11 At least once every calendar year, user entitlements for each application, database, and operating system are collected into the recertification tools and reviewed for completeness. User entitlements not collected are researched, corrected by designated State Street personnel, or manually recertified as necessary. | For a sample of recertifications and for one SSGA application with programmatically collected entitlements, inspected job schedule configurations and inquired with IT personnel to determine whether the collection of users and entitlements into the recertification tool was complete and accurate. | No deviations noted. |
| | For a sample of recertifications with manually collected entitlements, inspected queries/parameters used to generate manual listings and inquired with IT personnel to determine whether the collection of users and entitlements into the recertification tool was complete and accurate. | No deviations noted. |
| | Inspected recertification evidence to determine whether user entitlements for each relevant application, database, and operating system were collected into automated recertification tools at least once every calendar year and subject to review. | No deviations noted. |
| | For a sample of recertifications, reperformed and/or inspected evidence of management's review for completeness and inquired with Security Administration personnel, ISOs and/or platform SMEs to determine whether user IDs and/or entitlements identified as not collected into the tool excluded from the recertification or not matched to an employee record or recertifying manager were researched and corrected or manually recertified. | For 1 of 8 SailPoint Infrastructure Access recertifications selected for testing across 91,196 user entitlements, EY identified the following deviation where Management's review did not identify that user entitlements were incorrectly excluded from the recertification:<br>• 12 of 7,998 user entitlements with access to MS SQL databases<br>As a result, the corresponding user entitlements were not recertified.<br>No deviations were noted for other automated recertification processes.<br>**Management Response**<br>Management acknowledges that from a total of 7,998 MS SQL user entitlements, 12 entitlements for 3 users with read-only access were not included in the recertification. Although Management identified the missing entitlements during the QC process, the required manual review protocol was not clearly communicated to the responsible team to action. Management has updated documentation and reiterated the procedures for recertifying omitted entitlements. Additionally, the 12 entitlements have since been recertified. |

## Control Objective 2

Controls provide reasonable assurance that logical access to production applications, databases and operating systems, including the corporate network, is restricted to authorized personnel based on business need.

| State Street Controls | EY Tests | EY Test Results |
| --- | --- | --- |
| (See previous page.) | For one SSGA application with manually collected entitlements, inspected source application listings and recertification tool listings to determine whether the users and entitlements within the recertification tool were complete and accurate. | No deviations noted. |
| 2.12 The recertification tools send a notification to each user's hierarchical manager who is required to approve/retain or revoke the access. For privileged access reviews, a second elevated review within the recertification tool is also required. The recertification tools automatically enforce segregation of duties, preventing users from recertifying their own access. | For a sample of recertifications and for SSGA users, inspected access recertification documentation to determine whether users and entitlements were reviewed by hierarchical managers on a periodic basis and at least once every calendar year. | No deviations noted. |
| | For a sample of infrastructure and business privileged access recertifications and for SSGA Privileged Access recertifications, inspected access recertification documentation to determine whether users and entitlements were reviewed by hierarchical managers and the hierarchical manager's business unit senior manager or above on a periodic basis and at least once every calendar year. | No deviations noted. |
| | For a sample of users recertified above, inspected access entitlements and/or inquired with management to determine whether access was appropriate based on job responsibilities. | No deviations noted. |
| | Observed State Street IT personnel access the recertification tools to determine whether the tool settings have been configured to enforce segregation of duties, preventing a user from recertifying their own access. | No deviations noted. |
| | For recertification tools that are not configured to enforce segregation of duties, inspected access recertification documentation to determine whether a segregation of duties was present. | No deviations noted. |
| | Inspected job schedule configuration and inquired with IT personnel to determine whether the collection of hierarchical employee information into the recertification tool was complete and accurate. | No deviations noted. |
| | For two hierarchical managers performing a recertification, inspected recertification evidence to determine if the recertification tool identified the correct manager based on the HRMS record. | No deviations noted. |
| | For infrastructure and business privileged access recertifications and SSGA Privileged Access recertifications, inspected the queries/parameters used to generate the listings of reviews on the recertification tool used to select the sample to determine whether queries/parameters included the appropriate selection criteria. | No deviations noted. |

## Control Objective 2

Controls provide reasonable assurance that logical access to production applications, databases and operating systems, including the corporate network, is restricted to authorized personnel based on business need.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| 2.13 The recertification is reviewed by the IAM Centralized Certification or SSGA ISO team for completeness to confirm all user entitlements were marked with the appropriate access recertification decision. Any revocations resulting from the recertification are either revoked automatically or submitted to Security Administration for processing. Upon completion of revocation processing, a Reconciliation Validation report is run to verify that all access marked for revocation has been processed accurately. Any differences are escalated for resolution. | For a sample of recertifications and SSGA users selected above for control 2.12, inspected the final recertification report to determine whether all user entitlements for the selected recertifications were marked as maintain or revoke. | No deviations noted. |
| | Except SSGA, for a sample of recertifications selected above for control 2.12, inspected the Validation report to determine whether access revocation requests were processed. | For 1 of 17 recertifications selected for testing following the SailPoint general user access recertification process, EY identified that 2 of 15,038 entitlements requested to be revoked were not processed timely, impacting the Transaction Lifecycle Premium application.<br><br>No deviations were noted for other automated recertification processes.<br><br>**Management Response**<br>Management acknowledges that from a total of 15,038 entitlements marked for revocation, 2 entitlements for 1 user were retained for the Transaction Lifecycle Premium application. The access is appropriate and the user's manager certified the access as appropriate during the Q3 certification. Management has reiterated the importance of maintaining appropriate documentation related to retained access. |
| | For one SailPoint recertification, compared the Revocation Validation report against the post-recertification access listing to determine whether user entitlements marked for revocation were completely and accurately processed. | No deviations noted. |
| | For a sample of SSGA users selected above for control 2.11, inspected post-review user listings to determine whether access revocation requests for a sample of access amendments were processed. | No deviations noted. |
| **Manual Access Recertifications – Applications** | | |
| 2.14 Access to production applications is restricted to designated personnel based on job responsibilities and is reviewed on a periodic basis by designated business and/or IT personnel at least once every calendar year. Manual access recertifications are performed at the application level or by management chain (e.g., application users in a specific region). Where necessary, the ID(s) requiring modification/deletion are communicated to Security Administration personnel for processing. | For manual access reviews, inspected access recertification documentation for a sample of reviewers to determine whether the listings of application users and entitlements were reviewed on a periodic basis and at least once every calendar year by designated business and/or IT personnel. | No deviations noted. |

## Control Objective 2

Controls provide reasonable assurance that logical access to production applications, databases and operating systems, including the corporate network, is restricted to authorized personnel based on business need.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| (See previous page.) | For manual access reviews, inspected recertification summary documentation and/or email correspondences to determine whether the recertification was distributed to the recertifying managers. | No deviations noted. |
| | For a sample of users recertified above, inspected access entitlements and inquired with management to determine if access was appropriate based on job responsibilities. | No deviations noted. |
| | For samples of access amendment requests resulting from the access recertifications above, inspected a post-review application listing to determine whether amendments were actioned appropriately. | No deviations noted. |
| | For manual access reviews, inspected queries/parameters used to generate the listings used in the recertification, and the post-review listing, and inquired with State Street personnel to determine whether the recertification was inclusive of the users and entitlements. | No deviations noted. |
| | For the FundSuiteArc (U.S. Instance) user access recertification, inspected documentation to determine whether the recertification was performed in the prior period and inquired with management to determine the current status of the review for the 2023 calendar year. | No deviations noted. |
| **Manual Access Recertifications – Administrator IDs**<br>*Applicable to Administrator IDs not recertified through the infrastructure and business privileged recertification or general access recertification described within the Automated Application Recertification Tool section above* | | |
| 2.15 Administrator IDs with access to databases, operating systems and the corporate network are restricted to designated IT personnel based on job responsibilities and are reviewed on a periodic basis and at least once every calendar year by designated IT managers at the SVP level or above.<br>Administrator IDs with the ability to grant access to production applications, databases and operating systems, and the corporate network are restricted to designated Security Administration personnel and are reviewed on a periodic basis and at least once every calendar year by designated IT or business managers, or are restricted to designated business and/or IT personnel through the Firecall ID process. | For a sample of IT managers at the SVP level or above designated to review Administrator IDs with access to databases, operating systems and the corporate network, inspected access recertification documentation to determine whether Administrator IDs were reviewed on a periodic basis and at least once every calendar year. | No deviations noted. |
| | For manual Administrator ID recertifications, for a sample of reviewers designated to recertify Administrator IDs with the ability to grant access to production applications, databases and operating systems, inquired with management and inspected access recertification documentation to determine whether access was reviewed on a periodic basis and at least once every calendar year by designated IT or business managers. | No deviations noted. |

## Control Objective 2

Controls provide reasonable assurance that logical access to production applications, databases and operating systems, including the corporate network, is restricted to authorized personnel based on business need.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| (See previous page.) | For samples of applications, inspected privileged access entitlements and/or inquired with management to determine whether the access was appropriate based on users' job responsibilities.<br><br>See tests below for information about Production Data testing performed for Firecall ID access. | No deviations noted. |
| | For samples of access amendment requests resulting from the access recertifications above, inspected a post-review application listing to determine whether amendments were actioned appropriately. | No deviations noted. |
| | For Administrator ID recertifications noted above, inspected queries/parameters used to generate the listings used in the recertification, and the post-review listing and/or compared source system data against manual recertification documentation, as applicable, to determine whether the recertification was inclusive of the users and entitlements. | No deviations noted. |
| 2.16 Upon daily notification of movers from the HRMS application, for certain applications on SailPoint, the user's access is automatically taken "back to birthright" or a notification is sent to the employee and their manager to review the access remains appropriate based on the employee's current job responsibilities. | For a sample of permanent employees identified by the HRMS applications as movers, inspected evidence of their access taken "back to birthright" or recertified by the user's new manager. | For 1 of 40 movers selected for testing, the user's access was automatically taken "back to birthright". However, 1 of the 125 entitlements was not automatically revoked through that process.<br><br>**Management Response**<br><br>Management acknowledges that 1 of 125 entitlements was configured to be excluded from the automated revocation process in error. However, the entitlement alone does not provide access to data without a complementary entitlement, which was configured to be automatically revoked through the mover process. Therefore, although the entitlement was not automatically revoked, it would not allow access to data. Management has removed the exclusion so it will be subject to automated revocation. Additionally, Management implemented a report to identify changes to configurations. |
| | Inspected queries/parameters used to generate the listings used to select samples to determine whether the listings included the appropriate selection criteria for users, including the appropriate date selection criteria. | No deviations noted. |

## Control Objective 2

Controls provide reasonable assurance that logical access to production applications, databases and operating systems, including the corporate network, is restricted to authorized personnel based on business need.

| State Street Controls | EY Tests | EY Test Results |
| --- | --- | --- |
| **Network Security** | | |
| 2.17 Internet firewall rules are reviewed on a quarterly basis by designated IT personnel. | For a sample of quarters, inspected firewall review documentation to determine whether internet firewall rules were reviewed quarterly by designated IT personnel. | No deviations noted. |
| | Observed IT personnel generate the internet firewall rules report to determine whether the report included firewalls supporting the in-scope applications. | No deviations noted. |
| | For a sample of firewall rules, observed internet firewall configurations to determine whether they were appropriately included in the internet firewall rules report. | No deviations noted. |
| **Production Data Access** | | |
| 2.18 Firecall ID access requests are documented and submitted through Firecall access request tools or email. Firecall ID access is approved by designated personnel and granted for a specified period of time. For SSGA, Firecall IDs are pre-approved by an MD or above and access is activated by the Help Desk once Firecall requester/user is authenticated. | For samples of Firecall ID access requests, inspected access request documentation to determine whether Firecall ID access requests were approved by designated personnel in compliance with Firecall policy. | No deviations noted. |
| | For SSGA IT applications, inquired with State Street IT personnel to determine whether Firecall IDs were pre-approved by an MD or above and access was activated once Firecall requester/user is authenticated. | No deviations noted. |
| | For a sample of SSGA Firecall access requests, inspected Help Desk tickets to determine whether a ticket was created prior to an individual's access being granted. | No deviations noted. |
| | Inspected queries/parameters used to generate the Firecall ID requests listing used to select the sample to determine whether queries/parameters used included the appropriate Firecall ID access request selection criteria, including date selection criteria. | No deviations noted. |
| 2.19 Firecall ID access request approvers are reviewed on an annual basis by designated personnel. For SSGA, Firecall ID owners are recertified through their annual recertification process and approved by an MD or above. | For samples of Firecall ID access request approvers, inquired with designated personnel and inspected access recertification documentation to determine whether Firecall ID access request approvers were reviewed on an annual basis by designated personnel. | No deviations noted. |
| | Inspected queries/parameters used to generate the Firecall ID access approver listing used to select samples, and the post-review listing, to determine whether queries/parameters included the appropriate Firecall ID access approver selection criteria. | No deviations noted. |
| | For a sample of SSGA Firecall ID owners, inspected access approver recertification documentation to determine whether Firecall ID owners were reviewed on an annual basis by an MD or above. | No deviations noted. |
| | For a sample of Firecall ID approver and SSGA Firecall ID owner amendment requests resulting from the access request approver recertifications, inspected post-review listings to determine whether amendments were actioned appropriately. | No deviations noted. |

## Control Objective 2

Controls provide reasonable assurance that logical access to production applications, databases and operating systems, including the corporate network, is restricted to authorized personnel based on business need.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| 2.20 For Firecall ID access requests managed by designated personnel and SAS (submitted through request form), Security Administration personnel manually check that the Firecall ID access request approver is not the same individual for whom the Firecall ID access is being requested, as applicable.<br>For Firecall ID access requests managed by SAS (submitted through ServiceNow) and TPEO, ServiceNow and the Firecall access request tools have been configured to enforce segregation of duties between Firecall ID access requestors and approvers. | For samples of Firecall ID access requests managed by designated personnel and SAS Firecall ID access requests, inspected access request documentation to determine whether access requestors and approvers were different individuals. | No deviations noted. |
| | Inspected queries/parameters used to generate the Firecall ID request listing used to select the sample to determine whether queries/parameters used included the appropriate Firecall ID access request selection criteria, including date selection criteria. | No deviations noted. |
| | For Firecall ID access requests managed by TPEO, observed State Street IT personnel submit Firecall ID access requests through the tools and attempt to approve their own access request to determine whether the tools systematically enforced segregation of duties between Firecall ID access requestors and access approvers. | No deviations noted. |
| 2.21 Firecall IDs are deactivated based upon specified time parameters. | For the samples of Firecall ID access requests, inquired with Security Administration personnel and inspected Firecall ID activity logs or Firecall ID password logs to determine whether Firecall IDs were deactivated based upon specified time parameters. | For samples of 134 State Street Firecall ID access requests selected for testing across multiple Firecall administration processes, EY identified the following deviation where the Firecall ID was not deactivated within the specified timeframe:<br>• 2 of 40 Firecall ID access requests following the SAS Manual Firecall ID process<br>No deviations noted for the other Firecall ID processes.<br>**Management Response**<br>Management acknowledges that the Firecall IDs noted were appropriately requested, authorized, granted and activities were logged and monitored as supported by controls 2.18, 2.19, 2.20 and 2.22. |
| | Inspected queries/parameters used to generate the Firecall ID access request listings used to select the samples, and Firecall ID activity logs to determine whether queries/parameters used included the appropriate user and activity selection criteria, including date selection criteria. | No deviations noted. |
| | Inspected the queries/parameters used to generate the listing for the daily Firecall review to determine whether the listing included the appropriate selection criteria, including the appropriate date selection criteria. | No deviations noted. |

## Control Objective 2

Controls provide reasonable assurance that logical access to production applications, databases and operating systems, including the corporate network, is restricted to authorized personnel based on business need.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| **Security Monitoring** | | |
| 2.22 Privileged access activities are captured through the SIEM tools. Alerts are generated through these tools to cover specific privileged access activities. Alerts are reviewed within 2 business days by GCS personnel and escalated to designated IT personnel as necessary for further action. | For a sample of days for the UNIX and Linux platforms, inspected documentation to determine whether alerts for the selected days were reviewed within 2 business days by GCS personnel and escalated to designated IT personnel as necessary for further action. | For 3 of 25 days selected for testing, the applicable alerts were generated, but not reviewed by GCS personnel within 2 business days.<br>**Management Response**<br>Management acknowledges that the documentation of resolution was not readily available and not consistently performed subsequent to the transition period of responsibilities and technologies. Management notes that the identified items are related to activities performed by privileged users, however, additional security monitoring controls are in place to detect and monitor abnormal activities performed throughout the environment (i.e., 2.24, 2.25, 2.26). The Privileged Access Management program continues to mature its processes to refine and enhance its playbooks, detection and reporting capabilities to reduce false positives and response protocols across the enterprise, enabled via a centralized privileged access management solution. |
| | For a sample of days for the OpenVMS, Mainframe, Tandem, and Windows platforms, inspected documentation to determine whether alerts for the selected days were reviewed within 2 business days by GCS personnel and escalated to designated IT personnel as necessary for further action. | For 8 of 28 days selected for testing, the applicable alerts were generated, but not reviewed by GCS personnel within 2 business days.<br>**Management Response**<br>Refer to above response within 2.22. |
| | Inspected parameters in the SIEM tool to determine whether alerts are created as a result of the documented predefined alert criteria. | No deviations noted. |
| | Inspected scripts and configurations for the OpenVMS, Linux, Mainframe, Tandem, UNIX and Windows platforms and inquired with IT personnel to determine whether the collection of activity logs from source platforms into the SIEM tool was complete and accurate. | No deviations noted. |

## Control Objective 2

Controls provide reasonable assurance that logical access to production applications, databases and operating systems, including the corporate network, is restricted to authorized personnel based on business need.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| 2.23 On a weekly basis, GCS hosts the SIEM Review Board ("SRB") to review and track all proposed changes to the SIEM. Items may include the addition or removal of connectors, tuning of an alert, addition or removal of an alert or rule, prioritization of content creation, maintenance approval or addition of new content for a new log source. These meetings are hosted by State Street and minutes are kept of each meeting that include the proposed items as well as approvals or denials. | For a sample of weeks, inquired with management and inspected meeting materials to determine whether governance activities conducted during the SIEM review Board meeting were documented. | No deviations noted. |
| 2.24 On a daily basis, the Cyber Defense Center ("CDC") publishes a report of notable cyber threat events and incidents that occurred during the previous 24 hours to GCS leadership. | For a sample of days, inspected the CDC Daily Pulse Report documentation to determine whether a report of notable cyber threat events and incidents for the past 24 hours was sent to GCS leadership. | No deviations noted. |
| | For each selected day, inquired with management and inspected and observed the underlying data included in the CDC Daily Pulse Report to determine whether the queries/parameters used included the appropriate criteria, including date selection criteria. | No deviations noted. |
| 2.25 On an ongoing basis, CDC monitors and triages security events to determine prioritization and remediation activities. | For a sample of severities of notable events, inquired with management and inspected evidence of investigation documented in the ticket to determine whether events were classified and triaged by the CDC. | No deviations noted. |
| | Inspected parameters used to generate the listing of notable events used for selection of samples to determine whether the parameters included the appropriate selection criteria for notable events. | No deviations noted. |
| | See control 2.24 for additional testing relevant to ongoing monitoring and triage of security events. | |
| 2.26 The CDC receives and analyzes incident notifications to ensure that incidents are classified, contained, escalated, eradicated, reported, and reviewed post-closure in accordance with the Cyber Security Incident Response Plan ("CSIRP"). | Inquired with CDC personnel and inspected the CSIRP, including revision history, to determine whether current documentation existed to guide CDC personnel through the lifecycle of incident identification, incident management and incident response activities. | No deviations noted. |
| | For a sample of cyber incidents, inquired with management and inspected evidence of classification, containment, escalation, eradication, reporting, and post-closure review documented in the ticket to determine whether incidents were investigated in accordance with CSIRP. | No deviations noted. |
| | Inspected parameters used to generate the listing of cyber incidents used for selection of samples to determine whether the parameters included the appropriate selection criteria for cyber incidents. | No deviations noted. |

## Control Objective 3

Controls provide reasonable assurance that a Systems Development Lifecycle ("SDLC") process is followed for the development of production applications, and changes to production applications, databases and operating systems follow a documented change management process that requires changes be tested, approved and implemented by authorized personnel to support the effective functioning of application controls and to result in the complete, accurate and timely processing and reporting of transactions and balances.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| **Policies and Procedures** | | |
| 3.1 State Street has developed and implemented written policies and procedures to guide personnel through the development of production applications and the process of making changes to existing production applications, databases and operating systems. | Inquired with State Street personnel and inspected written policies and procedures to determine whether documentation existed to guide personnel through the development of production applications and the process of making changes to existing production applications, databases and operating systems. | No deviations noted. |
| **Systems Development Lifecycle** | | |
| 3.2 Project documentation is developed in accordance with written SDLC policies and procedures for application development projects. | For samples of projects, inspected documentation to determine whether project documentation was created in accordance with written SDLC policies and procedures. | No deviations noted. |
| | Inquired with IT personnel and observed the process for compiling the population of projects used to select the samples to determine whether the population was inclusive of the appropriate projects and date selections. | No deviations noted. |
| **Change Management Process** | | |
| 3.3 Application functional and technical changes are tested, where technically feasible, by designated personnel in a user acceptance testing ("UAT") environment. | For samples of application functional and technical changes, including emergency changes, inspected test plans/cases, test results (where deemed technically feasible) and/or sign-offs included in change request documentation to determine whether application changes were tested by designated personnel. | No deviations noted. |
| | Inspected the queries/parameters used to generate the change listings used to select samples to determine whether the queries/parameters used included the appropriate criteria for application functional change records and date selections. | No deviations noted. |
| | Inquired with IT personnel to determine whether testing was performed within the UAT environment.<br>See control 3.8 for information about testing performed on separate environments. | No deviations noted. |

## Control Objective 3

Controls provide reasonable assurance that a Systems Development Lifecycle ("SDLC") process is followed for the development of production applications, and changes to production applications, databases and operating systems follow a documented change management process that requires changes be tested, approved and implemented by authorized personnel to support the effective functioning of application controls and to result in the complete, accurate and timely processing and reporting of transactions and balances.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| 3.4 Designated personnel approve application changes prior to change implementation. | For samples of application functional and technical changes, including emergency changes, inspected change request tickets to determine whether approvals were obtained from designated personnel prior to change implementation. | No deviations noted. |
| | Inspected queries/parameters used to generate the change listings used to select the samples to determine whether the queries/ parameters used included the appropriate criteria for application functional and technical change records and date selections. | No deviations noted. |
| | For a sample of modified application production files selected from the source systems, inquired with IT personnel and inspected change request tickets to tie out application file modifications to corresponding change tickets. | No deviations noted. |
| | For system-generated approver listings, inspected queries/parameters used to generate the listings for completeness of the approvers and to determine whether the queries/parameters used included the appropriate criteria. For manually maintained approver listings, inspected the Human Resource listing for job titles and performed inquiries to determine whether the change approvers were designated personnel. | No deviations noted. |
| 3.5 Database and operating system changes are tested, as required and technically feasible, by designated IT personnel. | For samples of database changes, including emergency changes, inspected test plans/cases, test results (where deemed to be required and/or technically feasible) and/or sign-offs included in change request documentation to determine whether database changes were tested by designated IT personnel. | No deviations noted. |
| | For samples of operating system changes, including emergency changes, inspected test plans/cases, test results (where deemed to be required and/or technically feasible) and/or sign-offs included in change request documentation to determine whether operating system changes were tested by designated IT personnel. | No deviations noted. |
| | Inspected queries/parameters used to generate the operating system and database change listings to determine whether the queries/ parameters included the appropriate criteria for operating system and database change tickets, including the appropriate date selection criteria. | No deviations noted. |

## Control Objective 3

Controls provide reasonable assurance that a Systems Development Lifecycle ("SDLC") process is followed for the development of production applications, and changes to production applications, databases and operating systems follow a documented change management process that requires changes be tested, approved and implemented by authorized personnel to support the effective functioning of application controls and to result in the complete, accurate and timely processing and reporting of transactions and balances.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| 3.6 Designated IT personnel approve database and operating system changes prior to change implementation. | For database changes, including emergency changes, selected in the sample above, inspected change request tickets to determine whether approvals were obtained from designated IT personnel prior to change implementation. | No deviations noted. |
| | Inspected queries/parameters used to generate the database change listing used to select samples to determine whether the queries/parameters used included the appropriate criteria for database change records and date selections. | No deviations noted. |
| | For a sample of modified stored procedures selected from the source system traced file modifications to corresponding database change tickets. | No deviations noted. |
| | For system generated approver listings, inspected queries/parameters used to generate the listings for completeness of the approvers and to determine whether the queries/parameters used included the appropriate criteria. For manually maintained approver listings, inspected the Human Resource listing for job titles and performed inquiries to determine whether the change approvers were designated State Street personnel. | No deviations noted. |
| 3.7 At least weekly, the Change Advisory Board ("CAB") evaluates changes ready for production of a certain risk value to determine the readiness for implementation considering, but not limited to, successful development testing, completeness of supporting change documentation and evaluation of potential change risks. The decisions to approve, reject or return the change for further information are formally documented and maintained within the ticketing tool. | *Applicable for applications hosted in APAC and EMEA*<br>For a sample of weeks, inspected evidence of the weekly Change Advisory Board ("CAB") meeting to determine whether changes were approved, rejected or returned for further information and the decision was formally documented and maintained within the ticketing tool. | No deviations noted. |
| | *Applicable for applications hosted in North America and SSGA IT applications*<br>For a sample of days, inspected evidence of the daily Change Advisory Board ("CAB") meeting to determine whether changes were approved, rejected or returned for further information and the decision was formally documented and maintained within the ticketing tool. | No deviations noted. |
| | For one change, inspected evidence of the CAB meeting minutes and change ticket documentation to determine that approvals were captured timely following the meeting. | No deviations noted. |
| **Segregation of Duties** | | |
| 3.8 A separate UAT and production environment exist to segregate application testing and change implementation activities. | For a sample of applications, observed IT personnel log on to the UAT and production environments and inspected library management tools to determine whether separate environments existed for UAT and production. | No deviations noted. |

## Control Objective 3

Controls provide reasonable assurance that a Systems Development Lifecycle ("SDLC") process is followed for the development of production applications, and changes to production applications, databases and operating systems follow a documented change management process that requires changes be tested, approved and implemented by authorized personnel to support the effective functioning of application controls and to result in the complete, accurate and timely processing and reporting of transactions and balances.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| 3.9 IT personnel with the responsibility to develop application changes are segregated from IT personnel with change implementation responsibilities. Access privileges for application development and change implementation activities are enforced through library management tools, file system security permissions or through eSF access entitlement tools. | *Applicable to all applications residing on OpenVMS and Tandem operating systems and the Alpha Frontier, Caliber™, Enterprise Reporting Platform, Investment General Ledger System, Investor Services System and Wall Street Office (Alternatives) applications*<br>For samples of user IDs with access to library management tools, inspected access privileges to determine whether access was restricted to designated IT personnel based on job responsibilities. | No deviations noted. |
| | Inspected queries/parameters used to generate the library management tool access listings used to select the sample to determine whether the queries/parameters used included the appropriate criteria for users and their entitlements. | No deviations noted. |
| | *Applicable to all applications residing on Linux, Mainframe, Private Cloud, UNIX, and Windows operating systems other than Alpha Frontier, Caliber™, Enterprise Reporting Platform, Investment General Ledger System, Investor Services System and Wall Street Office (Alternatives) applications*<br>Inspected library management tool configuration settings to determine whether tools were configured to enforce segregation of application development and change implementation activities. | No deviations noted. |
| | For a sample of applications, inspected user IDs with update access to critical files and production directories, inquired with Security Administration personnel and inspected file system security permissions to determine whether update access privileges were restricted from application development personnel. | No deviations noted.<br>However, State Street Management self-identified a process account with update access on the Windows and Linux production servers that was set to allow interactive (human) login, and the password, which did not comply with GCS password standards, was known to members of the application support teams with development responsibilities. The account was not used during the period to interactively log into Windows production servers. The account was used during the period to interactively log directly into Linux production servers supporting 7 out of the 141 in-scope applications. Management analyzed the broader risk of potential user entity financial statement misstatements and noted the following compensating controls that would reasonably limit and/or detect unauthorized user activity: 2.22, 2.24, 2.25, 2.26, 4.5 and 4.6. |

## Control Objective 3

Controls provide reasonable assurance that a Systems Development Lifecycle ("SDLC") process is followed for the development of production applications, and changes to production applications, databases and operating systems follow a documented change management process that requires changes be tested, approved and implemented by authorized personnel to support the effective functioning of application controls and to result in the complete, accurate and timely processing and reporting of transactions and balances.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| (See previous page.) | (See previous page.) | In addition to noting the compensating controls above as well as subsequently changing the process account password and disabling interactive logins to Windows and Linux production servers, Management analyzed the process account activity and confirmed:<br>• The access was used by personnel who were functionally responsible for performing production support and/or infrastructure support and/or already had named user IDs to production, and<br>• No known application production data or functionality was modified by the process account for the servers where interactive logins were noted.<br>**Additional Procedures Performed by EY:**<br>Inspected State Street Management's analysis of the self-identified deviation, including relevant supporting documentation and no additional deviations were identified. |
| | Inspected queries/parameters used to generate the critical file and production directories access listings used to select the sample to determine whether the queries/parameters used included the appropriate criteria for users and their entitlements. | No deviations noted. |
| **Development of Macros** | | |
| 3.10 Requests for new macros or modifications to existing macros are submitted using the Global Macro Automation Services ("GMAS") websites and are tested by business users. | For a sample of macro requests, inspected requests to determine whether requests were submitted using the website and were tested by business users. | No deviations noted. |
| | Inspected queries/parameters used to generate the new and modified macros listing to determine whether the queries/parameters included the appropriate criteria for new and modified macros and appropriate date selections. | No deviations noted. |

## Control Objective 3

Controls provide reasonable assurance that a Systems Development Lifecycle ("SDLC") process is followed for the development of production applications, and changes to production applications, databases and operating systems follow a documented change management process that requires changes be tested, approved and implemented by authorized personnel to support the effective functioning of application controls and to result in the complete, accurate and timely processing and reporting of transactions and balances.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| 3.11 New macros and modifications to existing macros are approved by business users before being implemented to the production environment by designated GMAS personnel. | For a sample of new and modified macro requests, inspected requests to determine whether macros were approved by business users before being implemented to the production environment by designated GMAS personnel. | No deviations noted. |
| | Inspected the queries/parameters used to generate the new and modified macros listing used to select the sample to determine whether the queries/parameters used included the appropriate criteria for new and modified macros and date selections. | No deviations noted. |
| | Inspected the Human Resource listing for job titles and performed inquiries to determine whether the change approvers were designated business users. | No deviations noted. |

## Control Objective 4

Controls provide reasonable assurance that processing of production applications, databases and operating systems is authorized and executed in a complete, accurate and timely manner, and production processing failures are identified, tracked, recorded and addressed in a complete, accurate and timely manner.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| **Policies and Procedures** | | |
| 4.1 State Street has developed and implemented written policies and procedures to guide personnel through production processing activities, including making changes to job schedules in the production environment and monitoring and responding to incidents. | Inquired with IT personnel and inspected written policies and procedures to determine whether documentation existed to guide personnel through production processing activities, including scheduling and updating batch jobs in the production environments and monitoring and responding to incidents. | No deviations noted. |
| **Job Scheduling** | | |
| 4.2 Changes to job schedules are approved by authorized personnel prior to implementation in the production environment. | *Applicable to applications residing on the Mainframe, OpenVMS, Linux, UNIX and Windows operating systems other than Alpha Frontier, Caliber™, Enterprise Reporting Platform, Investment General Ledger System, Investor Services System, Mosiki, NAV Collection, PAM for Investments, PAM for Mortgages and Wall Street Office (Alternatives) and SSGA IT applications* | |
| | For a sample of job schedule change requests, inspected job schedule request documentation to determine whether the change request was approved by an authorized approver. | No deviations noted. |
| | *Applicable to NAV Collection, PAM for Investments and PAM for Mortgages applications* | |
| | For a sample of job schedule changes, inspected job schedule request documentation to determine whether the change request was approved by an authorized approver. | For the NAV Collection, PAM for Investments and PAM for Mortgages applications, 4 of 25 scheduling changes selected for testing, evidence of approval was not readily available.<br>**Management Response**<br>Management acknowledges that the job scheduling changes were performed in order to resolve documented problem tickets. However, approval for the job schedule changes was not formally documented. Management reiterated the requirement to obtain approval for all job schedule changes to demonstrate the appropriateness and acceptance of the issue resolution. |
| | Inspected queries/parameters used to generate the job schedule change listing used to select samples to determine whether the queries/parameters used included the appropriate criteria for job schedule change records and date selections. | No deviations noted. |
| | For a sample of modified production jobs selected from the source systems, inquired with IT personnel and inspected job scheduling change request tickets to tie out production job modifications to corresponding change tickets. | No deviations noted. |

## Control Objective 4

Controls provide reasonable assurance that processing of production applications, databases and operating systems is authorized and executed in a complete, accurate and timely manner, and production processing failures are identified, tracked, recorded and addressed in a complete, accurate and timely manner.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| (See previous page.) | *Applicable to applications residing on the Tandem operating system, applications running in the Private Cloud and the following applications: Alpha Frontier, Caliber™, Enterprise Reporting Platform, Investment General Ledger System, Investor Services System, Mosiki and Wall Street Office (Alternatives) and SSGA IT applications*<br>See Control Objective 3 for information about change management testing as changes to job schedules follow the change management process. | |
| 4.3 Job schedule change approvers for application residing on the OpenVMS operating system are reviewed on an annual basis by designated IT personnel. | For a sample of job schedule change approvers for applications residing on the OpenVMS operating system, inspected recertification documentation to determine whether change requestors were reviewed annually by designated IT personnel. | No deviations noted. |
| | For a sample of job schedule change approver amendments resulting from the recertifications, inspected documentation to determine whether amendments were actioned appropriately. | No deviations noted. |
| | Inspected queries/parameters used to generate the listings used to select the sample, and the post-review listing, to determine whether the queries/parameters used included the appropriate selection criteria for users and entitlements. | No deviations noted. |
| **Incident Management** | | |
| 4.4 Production jobs are monitored by designated IT personnel for successful completion through the use of event monitoring tools. Failed jobs are configured to automatically create a service request ticket or email which results in an alert to designated IT personnel. Alerts are tracked, prioritized and addressed by designated IT personnel in a timely manner. | Observed and inquired with designated IT personnel to determine whether event monitoring tools were used to identify and monitor production job failures in a timely manner. | No deviations noted. |
| | *Applicable to all applications other than Cash Portal, Market Data Framework, Market Effect System, Participant Record Keeping System, Recon Portal and Sentinel*<br>For samples of production job alerts, inspected incident management tickets or email correspondence to determine whether alerts were generated, communicated and addressed by designated IT personnel. | No deviations noted. |
| | Inspected queries/parameters used to generate the listings used to select the sample and inquired with IT personnel to determine whether the queries/parameters used included the appropriate selection criteria. | No deviations noted. |
| | *Applicable to Cash Portal, Market Data Framework, Market Effect System, Participant Record Keeping System, Recon Portal and Sentinel*<br>For a sample of production jobs and dates, inspected activity logs to determine whether the jobs ran successfully, and processing errors were addressed, as necessary, by designated SSGA IT personnel. | No deviations noted. |
| | Inspected queries/parameters used to generate the activity logs from the job scheduling tool to determine whether activity logs were complete and accurate. | No deviations noted. |

## Control Objective 4

Controls provide reasonable assurance that processing of production applications, databases and operating systems is authorized and executed in a complete, accurate and timely manner, and production processing failures are identified, tracked, recorded and addressed in a complete, accurate and timely manner.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| 4.5 Incident management meetings are held and documented on a daily basis by IT and/or business management to review major incidents on data center status, daily processing, availability and outages. | For a sample of days, inspected Daily Processing reports to determine whether incidents were being tracked and communicated to State Street Executive Management. | No deviations noted. |
| | Inquired with IT personnel and inspected a sample of incident management reports to determine whether incidents being tracked were communicated to IT and/or business management and discussed during periodic incident management meetings. | No deviations noted. |
| 4.6 The Problem Management team performs formal Root Cause Analysis following incident/event resolution to identify the source of performance and operational issues so that remediating action can be taken, if necessary. Problem Management also provides metrics and reporting to Senior Management. | Inquired with management and inspected policies and procedures to determine whether the process for Root Cause Analysis was documented. | No deviations noted. |
| | For a sample of incidents requiring Root Cause Analysis, inspected tickets to determine whether Root Cause Analysis was performed to identify the source of performance and operational issues so that remediating action can be taken, if necessary. | No deviations noted. |
| | Inspected queries/parameters used to generate the listing of incidents requiring Root Cause Analysis used to select the testing sample in order to determine whether the queries/parameters used included the appropriate selection criteria for these incidents. | No deviations noted. |
| | Inspected a sample of monthly Technology Stability Reports to determine whether metrics of problem management KPIs and trends were reported to Senior Management. | No deviations noted. |

## Control Objective 5

Controls provide reasonable assurance that production applications and data are regularly backed up and are available for restoration in the event of processing errors and/or unexpected interruptions.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| **Policies and Procedures** | | |
| 5.1 State Street has developed and implemented written policies and procedures to guide personnel through the process of performing backups of applications and data, sending backups off-site and processing data restore requests. | Inquired with IT personnel and inspected written policies and procedures to determine whether documentation existed to guide personnel through the process of performing backups of applications and data, sending backups off-site and processing data restore requests. | No deviations noted. |
| **Backup Management Process** | | |
| 5.2 Applications servers and databases are backed up on a periodic basis using automated backup management tools and in accordance with written backup policies and procedures. Backups failures are researched and resolved by appropriate IT personnel. | For a sample of applications and related databases, inquired with IT personnel and inspected screenshots of the job schedule definitions and backup management tool configurations to determine whether the backup frequency and type of backup was scheduled to occur in accordance with written backup policies and procedures. | No deviations noted. |
| | For a sample of backup jobs and configurations, inquired with IT personnel and inspected the corresponding activity logs to determine whether applications and data were backed up as defined by the job schedule definitions. | No deviations noted. |
| | Inquired with IT personnel to determine whether backups were monitored for successful completion and failures were researched and resolved by IT personnel. | No deviations noted. |
| 5.3 Backup data is sent or replicated virtually to an off-site facility on a periodic basis. The tape inventory maintained by the off-site vendor is reconciled through the vendor's on-line reporting tool. | For a sample of days, inspected the tape shipping manifest to determine whether backups for applications except for Investor Services System, JARS, Livewire, Phoenix, Record Keeping System (Japan), NAV Collection and PAM applications, were sent to an off-site facility on a periodic basis by IT personnel. | No deviations noted. |
| | Inquired with IT personnel to determine that a reconciliation of backup tapes sent to the off-site facility is performed. | No deviations noted. |

## Control Objective 5

Controls provide reasonable assurance that production applications and data are regularly backed up and are available for restoration in the event of processing errors and/or unexpected interruptions.

| State Street Controls | EY Tests | EY Test Results |
|---|---|---|
| 5.4 Update access to backup management tools is restricted to designated IT personnel based on job responsibilities and is reviewed on a periodic basis and at least once every calendar year by the State Street ISO or designated business or IT manager. | *Applicable to applications residing on operating systems other than the Mainframe, OpenVMS or Tandem*<br>For a sample of user IDs with update access to backup management tools inspected annual access recertifications and/or State Street organizational diagrams to determine whether access was restricted to designated IT personnel and was reviewed on a periodic basis by ISOs or designated IT senior manager or above based on job responsibilities. | No deviations noted. |
| | For a sample of access revocation requests resulting from the access recertifications, inspected documentation to determine whether amendments were actioned appropriately. | No deviations noted. |
| | Inspected queries/parameters used to generate the listings used in the recertification to determine whether queries/parameters used included the appropriate selection criteria for users and backup management tools entitlements. | No deviations noted. |
| | *Applicable to applications residing on the Mainframe, OpenVMS and Tandem operating systems*<br>See Control Objective 2 for information about operating system access recertification testing performed, as backup management tool access is managed through operating system access privileges. | |
| **Data Restore** | | |
| 5.5 A service request ticket is created for data restore requests submitted through e-mail, the Help Desk, or service request tools. Once the data restore has been performed by IT personnel, the business user who made the request is notified that the data restore has been completed. The service request tool is configured to request confirmation from the business user that the restore was completed as requested. | For a sample of data restore requests, inspected service request tickets to determine whether IT personnel performed the data restore as requested and notified the business user through the service request ticket. | No deviations noted. |
| | Inspected queries/parameters used to generate the data restore request ticket listing used to select the sample to determine whether the queries/parameters included the appropriate data restore request parameters and date selection criteria. | No deviations noted. |

## B. Additional Information Provided by the Independent Service Auditor

### Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. In addition to the tests of specific control procedures described below, our procedures included tests of, or consideration of, the relevant elements of State Street's control environment, including:

- State Street's organizational structure and approach to segregation of duties;
- The functioning of the Board of Directors;
- Management control methods;
- Personnel policies and practices;
- Corporate Audit; and
- Regulatory oversight of State Street.

Our tests of the control environment included the following procedures to the extent we considered necessary: (a) a review of State Street's organizational structure, including the segregation of functional responsibilities, policy statements, accounting and processing manuals, personnel policies, procedures and reports; (b) discussions with management, operations, administrative and other personnel who are responsible for developing, ascertaining adherence to and applying controls; (c) observations of personnel in the performance of their assigned duties; and (d) a review of State Street's actions taken in response to recommendations to improve controls made by Corporate Audit and regulators having supervisory oversight over State Street's fiduciary activities.

### Test of Controls

The control environment was considered in determining the nature, timing and extent of testing of the operating effectiveness of controls relevant to the achievement of the control objectives.

Our tests of the operating effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, is sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the period from October 1, 2022 to September 30, 2023. Our tests of the operational effectiveness of controls were designed to cover a representative number of instances of the controls throughout the period from October 1, 2022 to September 30, 2023, for each of the controls listed in the description in Section IV. Our tests did not include tests of controls in respect of any particular client of State Street. The testing procedures performed and results are the responsibility of EY. In selecting particular tests of the operational effectiveness of controls, we considered: (a) the nature of the items being tested, including if they are part of a common process; (b) the types and sufficiency of available evidential matter; (c) the nature of the audit objectives to be achieved; and (d) the expected efficiency and effectiveness of the test. Additionally, EY considered the applications that follow a common process and aggregated the populations where appropriate. EY has determined the nature, timing and extent of testing performed to obtain evidence about the effectiveness of State Street's control procedures in meeting the identified control objectives during the period from October 1, 2022 to September 30, 2023.

## C. Deviation Summary by Complementary State Street Report

Not all controls, processes or test results described in this report are applicable to each in-scope application and/or complementary State Street business control report. The chart below identifies which controls with test deviations noted in Section IV are relevant to each complementary State Street SOC 1® business process reports.

| | Report Reference Letter | 2.5 | 2.8 | 2.11 | 2.13 | 2.16 | 2.21 | 2.22 | 3.9 | 4.2 |
|---|---|---|---|---|---|---|---|---|---|---|
| Alternatives – Hedge | A | | ✔ | ✔ | ✔ | ✔ | | ✔ | ✔ | |
| Alternatives – Private Markets | B | | ✔ | ✔ | ✔ | ✔ | | ✔ | ✔ | |
| French Fund Accounting | C | | | ✔ | ✔ | ✔ | | ✔ | ✔ | |
| Global Fund Accounting and Custody | D | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | |
| Global Services – Taxation Services Australia | E | | | ✔ | ✔ | ✔ | | ✔ | ✔ | |
| Global Services – Unit Registry Australia | F | | | ✔ | ✔ | ✔ | | ✔ | ✔ | |
| Institutional Transfer Agent | G | | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | |
| Investment Manager Services – Enterprise | H | | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | |
| Kansas City Insurance Services | I | | | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ |
| State Street GmbH-KVG Fund Accounting In-sourcing | J | | | ✔ | ✔ | ✔ | | ✔ | ✔ | |
| State Street GmbH Succursale Italia's Fund Administration, Depositary Bank and Local Custody | K | | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | |
| State Street Global Advisors | L | | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | |
| SSTB Co., Ltd. Japan – Investment Manager and Insurance Outsourcing Services | M | | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | |
| State Street Retiree Services | N | | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | |

A Alternatives – Hedge
B Alternatives – Private Markets
C French Fund Accounting
D Global Fund Accounting and Custody
E Global Services – Taxation Services Australia
F Global Services – Unit Registry Australia
G Institutional Transfer Agent
H Investment Manager Services – Enterprise
I Kansas City Insurance Services
J State Street GmbH-KVG Fund Accounting In-sourcing
K State Street GmbH Succursale Italia's Fund Administration, Depositary Bank and Local Custody
L State Street Global Advisors
M SSTB Co., Ltd. Japan – Investment Manager and Insurance Outsourcing Services
N State Street Retiree Services
O State Street Transfer Agency – Hong Kong and Singapore
P State Street Transfer Agency – Ireland
Q SSTB Co., Ltd. Japan – Trust and Standing Proxy Business
R U.S. Investment Services

| | Report Reference Letter | 2.5 | 2.8 | 2.11 | 2.13 | 2.16 | 2.21 | 2.22 | 3.9 | 4.2 |
|---|---|---|---|---|---|---|---|---|---|---|
| State Street Transfer Agency – Hong Kong and Singapore | O | | | ✔ | ✔ | ✔ | | ✔ | ✔ | |
| State Street Transfer Agency – Ireland | P | | | ✔ | ✔ | ✔ | | ✔ | ✔ | |
| SSTB Co., Ltd. Japan – Trust and Standing Proxy Business | Q | | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | |
| U.S. Investment Services | R | | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | |

*See following chart for detailed explanation of Controls, Tests, Deviations, and Management Responses.

A Alternatives – Hedge
B Alternatives – Private Markets
C French Fund Accounting
D Global Fund Accounting and Custody
E Global Services – Taxation Services Australia
F Global Services – Unit Registry Australia
G Institutional Transfer Agent
H Investment Manager Services – Enterprise
I Kansas City Insurance Services
J State Street GmbH-KVG Fund Accounting In-sourcing
K State Street GmbH Succursale Italia's Fund Administration, Depositary Bank and Local Custody
L State Street Global Advisors
M SSTB Co., Ltd. Japan – Investment Manager and Insurance Outsourcing Services
N State Street Retiree Services
O State Street Transfer Agency – Hong Kong and Singapore
P State Street Transfer Agency – Ireland
Q SSTB Co., Ltd. Japan – Trust and Standing Proxy Business
R U.S. Investment Services

| Control Number | State Street Control | EY Test | EY Test Results<br>October 1, 2022 to September 30, 2023 | Relevant Report(s)<br>Period Deviation Identified<br>10/1/22–3/31/23 | <br><br>4/1/23–9/30/23 | Management Response<br>October 1, 2022 to September 30, 2023 |
|---|---|---|---|---|---|---|
| 2.5 | Access requests are documented and approved by designated personnel who are authorized to approve access requests to production applications, databases, operating systems and/or the corporate network. | For samples of new and modified permanent employees and contingent worker access, inspected access request documentation to determine whether the access request was documented and was approved by designated personnel who were authorized to approve access requests to production applications, databases, operating systems, and/or the corporate network. | For samples of 342 State Street new and modified permanent employees and contingent workers selected for testing across multiple access administration processes, EY identified the following deviation where access was granted without authorized approval:<br>• 1 of 16 users selected for testing with access to the Tax Efficient Lot Selector ("iTELS") and Automated Wash Sales ("AWS") applications<br>No deviations were noted for other access administration processes. | D<br>✔ | | Management acknowledges that although iTELS and AWS application gateway access was appropriately requested and approved for a new application support employee, the functional entitlements were separately provisioned by mirroring an existing application support employee's profile, without documented approval. Management has reiterated the requirement to document the request and approval for each entitlement. No changes to the entitlements were required as they were appropriate for the employee's job responsibilities.<br>Management further notes this is a unique access administration process specific to iTELS and AWS entitlements and there were no deviations noted for the other access administration processes as documented in Section III B. |

A Alternatives – Hedge
B Alternatives – Private Markets
C French Fund Accounting
D Global Fund Accounting and Custody
E Global Services – Taxation Services Australia
F Global Services – Unit Registry Australia
G Institutional Transfer Agent
H Investment Manager Services – Enterprise
I Kansas City Insurance Services
J State Street GmbH-KVG Fund Accounting In-sourcing
K State Street GmbH Succursale Italia's Fund Administration, Depositary Bank and Local Custody
L State Street Global Advisors
M SSTB Co., Ltd. Japan – Investment Manager and Insurance Outsourcing Services
N State Street Retiree Services
O State Street Transfer Agency – Hong Kong and Singapore
P State Street Transfer Agency – Ireland
Q SSTB Co., Ltd. Japan – Trust and Standing Proxy Business
R U.S. Investment Services

| Control Number | State Street Control | EY Test | EY Test Results October 1, 2022 to September 30, 2023 | Relevant Report(s) | Period Deviation Identified 10/1/22–3/31/23 | Period Deviation Identified 4/1/23–9/30/23 | Management Response October 1, 2022 to September 30, 2023 |
|---|---|---|---|---|---|---|---|
| 2.8 | For access requests submitted through access request tools, these tools have been configured to enforce segregation of duties between access requestors and access approvers. For access requests submitted through the Help Desk or dedicated Security Administration personnel, Security Administration personnel manually check that the access approver is not the same individual for whom the access is being requested. Security Administration personnel responsible for processing an access request are not involved in the approval of that same access request. | For the samples of new and modified permanent employee and contingent worker access selected above for control 2.5, inspected access request documentation to determine whether the individual approving the access is not the same individual for whom the access is being requested and that Security Administration personnel responsible for processing an access request are not involved in the approval of that same access request. | For samples of 342 State Street new and modified permanent employees and contingent workers selected for testing across multiple access administration processes, EY identified the following deviations where a segregation of duties between access requestor, approver, and/or Security Administration personnel was not enforced:<br>• 1 of 12 for the Oracle Financials application | B | ✔ | | For Oracle Financials and AIS IT, management acknowledges a bulk access request form for members of a fund services team was submitted by an authorized approver, which also included the approver on the form. Access was subsequently granted.<br>For FundSuite ARC (EMEA), the access request was approved and processed by the same access administrator.<br>Management confirmed all access was appropriate and reiterated the importance of enforcing an independent approval for all requested access. Management notes that the deviations resulted from unique access administration process specific to the FundSuite ARC (EMEA) application and Oracle Financials/AIS IT and there were no deviations noted for other access administration processes as documented in Section III B. |
| | | | • 2 of 17 for the FundSuite ARC (EMEA) application | D | | ✔ | |
| | | | • 1 of 25 for the AIS IT access administration process<br>No deviations were noted for other access administration processes. | A, B | | ✔ | |

A Alternatives – Hedge
B Alternatives – Private Markets
C French Fund Accounting
D Global Fund Accounting and Custody
E Global Services – Taxation Services Australia
F Global Services – Unit Registry Australia
G Institutional Transfer Agent
H Investment Manager Services – Enterprise
I Kansas City Insurance Services
J State Street GmbH-KVG Fund Accounting In-sourcing
K State Street GmbH Succursale Italia's Fund Administration, Depositary Bank and Local Custody
L State Street Global Advisors
M SSTB Co., Ltd. Japan – Investment Manager and Insurance Outsourcing Services
N State Street Retiree Services
O State Street Transfer Agency – Hong Kong and Singapore
P State Street Transfer Agency – Ireland
Q SSTB Co., Ltd. Japan – Trust and Standing Proxy Business
R U.S. Investment Services

| Control Number | State Street Control | EY Test | EY Test Results October 1, 2022 to September 30, 2023 | Relevant Report(s) Period Deviation Identified 10/1/22–3/31/23 | 4/1/23–9/30/23 | Management Response October 1, 2022 to September 30, 2023 |
|---|---|---|---|---|---|---|
| 2.11 | At least once every calendar year, user entitlements for each application, database and operating system are collected into the recertification tools and reviewed for completeness. User entitlements not collected are researched, corrected by designated State Street personnel, or manually recertified as necessary. | For a sample of recertifications, reperformed and/or inspected evidence of management's review for completeness and inquired with Security Administration personnel, ISOs and/or platform SMEs to determine whether user IDs and/or entitlements identified as not collected into the tool excluded from the recertification or not matched to an employee record or recertifying manager were researched and corrected or manually recertified. | For 1 of 8 SailPoint Infrastructure Access recertifications selected for testing across 91,196 user entitlements, EY identified the following deviation where Management's review did not identify that user entitlements were incorrectly excluded from the recertification:<br>• 12 of 7,998 user entitlements with access to MS SQL databases<br>As a result, the corresponding user entitlements were not recertified.<br>No deviations were noted for other automated recertification processes. | A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R | ✔ | Management acknowledges that from a total of 7,998 MS SQL user entitlements, 12 entitlements for 3 users with read-only access were not included in the recertification. Although Management identified the missing entitlements during the QC process, the required manual review protocol was not clearly communicated to the responsible team to action. Management has updated documentation and reiterated the procedures for recertifying omitted entitlements. Additionally, the 12 entitlements have since been recertified. |
| 2.13 | The recertification is reviewed by the IAM Centralized Certification or SSGA ISO team for completeness to confirm all user entitlements were marked with the appropriate access recertification decision. Any revocations resulting from the recertification are either revoked automatically or submitted to Security Administration for processing. Upon completion of revocation processing, a Reconciliation Validation report is run to verify that all access marked for revocation has been processed accurately. Any differences are escalated for resolution. | Except SSGA, for a sample of recertifications selected above for control 2.12, inspected the Validation report to determine whether access revocation requests were processed. | For 1 of 17 recertifications selected for testing following the SailPoint general user access recertification process, EY identified that 2 of 15,038 entitlements requested to be revoked were not processed timely, impacting the Transaction Lifecycle Premium application.<br>No deviations were noted for other automated recertification processes. | A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R | ✔ | Management acknowledges that from a total of 15,038 entitlements marked for revocation, 2 entitlements for 1 user were retained for the Transaction Lifecycle Premium application. The access is appropriate and the user's manager certified the access as appropriate during the Q3 certification. Management has reiterated the importance of maintaining appropriate documentation related to retained access. |

A Alternatives – Hedge
B Alternatives – Private Markets
C French Fund Accounting
D Global Fund Accounting and Custody
E Global Services – Taxation Services Australia
F Global Services – Unit Registry Australia
G Institutional Transfer Agent
H Investment Manager Services – Enterprise
I Kansas City Insurance Services
J State Street GmbH-KVG Fund Accounting In-sourcing
K State Street GmbH Succursale Italia's Fund Administration, Depositary Bank and Local Custody
L State Street Global Advisors
M SSTB Co., Ltd. Japan – Investment Manager and Insurance Outsourcing Services
N State Street Retiree Services
O State Street Transfer Agency – Hong Kong and Singapore
P State Street Transfer Agency – Ireland
Q SSTB Co., Ltd. Japan – Trust and Standing Proxy Business
R U.S. Investment Services

| Control Number | State Street Control | EY Test | EY Test Results October 1, 2022 to September 30, 2023 | Relevant Report(s) Period Deviation Identified 10/1/22–3/31/23 | Relevant Report(s) Period Deviation Identified 4/1/23–9/30/23 | Management Response October 1, 2022 to September 30, 2023 |
|---|---|---|---|---|---|---|
| 2.16 | Upon daily notification of movers from the HRMS application, for certain applications on SailPoint, the user's access is automatically taken "back to birthright" or a notification is sent to the employee and their manager to review the access remains appropriate based on the employee's current job responsibilities. | For a sample of permanent employees identified by the HRMS applications as movers, inspected evidence of their access taken "back to birthright" or recertified by the user's new manager. | For 1 of 40 movers selected for testing, the user's access was automatically taken "back to birthright". However, 1 of the 125 entitlements was not automatically revoked through that process. | A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R<br>✔ | | Management acknowledges that 1 of 125 entitlements was configured to be excluded from the automated revocation process in error. However, the entitlement alone does not provide access to data without a complementary entitlement, which was configured to be automatically revoked through the mover process. Therefore, although the entitlement was not automatically revoked, it would not allow access to data. Management has removed the exclusion so it will be subject to automated revocation. Additionally, Management implemented a report to identify changes to configurations. |
| 2.21 | Firecall IDs are deactivated based upon specified time parameters. | For the samples of Firecall ID access requests, inquired with Security Administration personnel and inspected Firecall ID activity logs or Firecall ID password logs to determine whether Firecall IDs were deactivated based upon specified time parameters. | For samples of 134 State Street Firecall ID access requests selected for testing across multiple Firecall administration processes, EY identified the following deviation where the Firecall ID was not deactivated within the specified timeframe:<br>• 2 of 40 Firecall ID access requests following the SAS Manual Firecall ID process<br>No deviations noted for the other Firecall ID processes. | D, G, H, K, L, M, N, Q, R<br>✔ | ✔ | Management acknowledges that the Firecall IDs noted were appropriately requested, authorized, granted and activities were logged and monitored as supported by controls 2.18, 2.19, 2.20 and 2.22. |

A Alternatives – Hedge
B Alternatives – Private Markets
C French Fund Accounting
D Global Fund Accounting and Custody
E Global Services – Taxation Services Australia
F Global Services – Unit Registry Australia
G Institutional Transfer Agent
H Investment Manager Services – Enterprise
I Kansas City Insurance Services
J State Street GmbH-KVG Fund Accounting In-sourcing
K State Street GmbH Succursale Italia's Fund Administration, Depositary Bank and Local Custody
L State Street Global Advisors
M SSTB Co., Ltd. Japan – Investment Manager and Insurance Outsourcing Services
N State Street Retiree Services
O State Street Transfer Agency – Hong Kong and Singapore
P State Street Transfer Agency – Ireland
Q SSTB Co., Ltd. Japan – Trust and Standing Proxy Business
R U.S. Investment Services

| Control Number | State Street Control | EY Test | EY Test Results October 1, 2022 to September 30, 2023 | Relevant Report(s) | | Management Response October 1, 2022 to September 30, 2023 |
|---|---|---|---|---|---|---|
| | | | | Period Deviation Identified | | |
| | | | | 10/1/22–3/31/23 | 4/1/23–9/30/23 | |
| 2.22 | Privileged access activities are captured through the SIEM tools. Alerts are generated through these tools to cover specific privileged access activities. Alerts are reviewed within 2 business days by GCS personnel and escalated to designated IT personnel as necessary for further action. | For a sample of days for the UNIX and Linux platforms, inspected documentation to determine whether alerts for the selected days were reviewed within 2 business days by GCS personnel and escalated to designated IT personnel as necessary for further action. | For 3 of 25 days selected for testing, the applicable alerts were generated, but not reviewed by GCS personnel within 2 business days. | A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R | | Management acknowledges that the documentation of resolution was not readily available and not consistently performed subsequent to the transition period of responsibilities and technologies. Management notes that the identified items are related to activities performed by privileged users, however, additional security monitoring controls are in place to detect and monitor abnormal activities performed throughout the environment (i.e., 2.24, 2.25, 2.26). The Privileged Access Management program continues to mature its processes to refine and enhance its playbooks, detection and reporting capabilities to reduce false positives and response protocols across the enterprise, enabled via a centralized privileged access management solution. |
| | | | | | ✔ | |
| | | For a sample of days for the OpenVMS, Mainframe, Tandem, and Windows platforms, inspected documentation to determine whether alerts for the selected days were reviewed within 2 business days by GCS personnel and escalated to designated IT personnel as necessary for further action. | For 8 of 28 days selected for testing, the applicable alerts were generated, but not reviewed by GCS personnel within 2 business days. | A, B, D, G, H, I, K, L, M, N, Q, R | | |
| | | | | ✔ | ✔ | |

A Alternatives – Hedge
B Alternatives – Private Markets
C French Fund Accounting
D Global Fund Accounting and Custody
E Global Services – Taxation Services Australia
F Global Services – Unit Registry Australia
G Institutional Transfer Agent
H Investment Manager Services – Enterprise
I Kansas City Insurance Services
J State Street GmbH-KVG Fund Accounting In-sourcing
K State Street GmbH Succursale Italia's Fund Administration, Depositary Bank and Local Custody
L State Street Global Advisors
M SSTB Co., Ltd. Japan – Investment Manager and Insurance Outsourcing Services
N State Street Retiree Services
O State Street Transfer Agency – Hong Kong and Singapore
P State Street Transfer Agency – Ireland
Q SSTB Co., Ltd. Japan – Trust and Standing Proxy Business
R U.S. Investment Services

| Control Number | State Street Control | EY Test | EY Test Results October 1, 2022 to September 30, 2023 | Relevant Report(s) Period Deviation Identified 10/1/22–3/31/23 | 4/1/23–9/30/23 | Management Response October 1, 2022 to September 30, 2023 |
|---|---|---|---|---|---|---|
| 3.9 | IT personnel with the responsibility to develop application changes are segregated from IT personnel with change implementation responsibilities. Access privileges for application development and change implementation activities are enforced through library management tools, file system security permissions or through eSF access entitlement tools. | For samples of user IDs with update access to critical files and production directories, inquired with Security Administration personnel and inspected file system security permissions to determine whether update access privileges were restricted from application development personnel. | No deviations noted.<br>However, State Street Management self-identified a process account with update access on the Windows and Linux production servers that was set to allow interactive (human) log-in, and the password, which did not comply with GCS password standards, was known to members of the application support teams with development responsibilities. The account was not used during the period to interactively log into Windows production servers. The account was used during the period to interactively log directly into Linux production servers supporting 7 out of the 141 in-scope applications. Management analyzed the broader risk of potential user entity financial statement misstatements and noted the following compensating controls that would reasonably limit and/or detect unauthorized user activity: 2.22, 2.24, 2.25, 2.26, 4.5 and 4.6.<br>(Continued on next page.) | A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R<br>✔ | | Refer to EY Test Results. |

A Alternatives – Hedge
B Alternatives – Private Markets
C French Fund Accounting
D Global Fund Accounting and Custody
E Global Services – Taxation Services Australia
F Global Services – Unit Registry Australia
G Institutional Transfer Agent
H Investment Manager Services – Enterprise
I Kansas City Insurance Services
J State Street GmbH-KVG Fund Accounting In-sourcing
K State Street GmbH Succursale Italia's Fund Administration, Depositary Bank and Local Custody
L State Street Global Advisors
M SSTB Co., Ltd. Japan – Investment Manager and Insurance Outsourcing Services
N State Street Retiree Services
O State Street Transfer Agency – Hong Kong and Singapore
P State Street Transfer Agency – Ireland
Q SSTB Co., Ltd. Japan – Trust and Standing Proxy Business
R U.S. Investment Services

| Control Number | State Street Control | EY Test | EY Test Results October 1, 2022 to September 30, 2023 | Relevant Report(s) Period Deviation Identified 10/1/22–3/31/23 | 4/1/23–9/30/23 | Management Response October 1, 2022 to September 30, 2023 |
|---|---|---|---|---|---|---|
| 3.9 con't. | (See previous page.) | (See previous page.) | In addition to noting the compensating controls above as well as subsequently changing the process account password and disabling interactive logins to Windows and Linux production servers, Management analyzed the process account activity and confirmed:<br>• The access was used by personnel who were functionally responsible for performing production support and/or infrastructure support and/or already had named user IDs to production, and<br>• No known application production data or functionality was modified by the process account for the servers where interactive logins were noted.<br>**Additional Procedures Performed by EY:**<br>Inspected State Street Management's analysis of the self-identified deviation, including relevant supporting documentation and no additional deviations were identified. | (See previous page.) | | (See previous page.) |

A Alternatives – Hedge
B Alternatives – Private Markets
C French Fund Accounting
D Global Fund Accounting and Custody
E Global Services – Taxation Services Australia
F Global Services – Unit Registry Australia
G Institutional Transfer Agent
H Investment Manager Services – Enterprise
I Kansas City Insurance Services
J State Street GmbH-KVG Fund Accounting In-sourcing
K State Street GmbH Succursale Italia's Fund Administration, Depositary Bank and Local Custody
L State Street Global Advisors
M SSTB Co., Ltd. Japan – Investment Manager and Insurance Outsourcing Services
N State Street Retiree Services
O State Street Transfer Agency – Hong Kong and Singapore
P State Street Transfer Agency – Ireland
Q SSTB Co., Ltd. Japan – Trust and Standing Proxy Business
R U.S. Investment Services

| Control Number | State Street Control | EY Test | EY Test Results October 1, 2022 to September 30, 2023 | Relevant Report(s) Period Deviation Identified 10/1/22–3/31/23 | Relevant Report(s) Period Deviation Identified 4/1/23–9/30/23 | Management Response October 1, 2022 to September 30, 2023 |
|---|---|---|---|---|---|---|
| 4.2 | Changes to job schedules are approved by authorized personnel prior to implementation in the production environment. | *Applicable to NAV Collection, PAM for Investments and PAM for Mortgages applications* For a sample of job schedule changes, inspected job schedule request documentation to determine whether the change request was approved by an authorized approver. | For the NAV Collection, PAM for Investments and PAM for Mortgages applications, 4 of 25 scheduling changes selected for testing, evidence of approval was not readily available. | I<br>✔ | | Management acknowledges that the job scheduling changes were performed in order to resolve documented problem tickets. However, approval for the job schedule changes was not formally documented. Management reiterated the requirement to obtain approval for all job schedule changes to demonstrate the appropriateness and acceptance of the issue resolution. |

A Alternatives – Hedge
B Alternatives – Private Markets
C French Fund Accounting
D Global Fund Accounting and Custody
E Global Services – Taxation Services Australia
F Global Services – Unit Registry Australia
G Institutional Transfer Agent
H Investment Manager Services – Enterprise
I Kansas City Insurance Services
J State Street GmbH-KVG Fund Accounting In-sourcing
K State Street GmbH Succursale Italia's Fund Administration, Depositary Bank and Local Custody
L State Street Global Advisors
M SSTB Co., Ltd. Japan – Investment Manager and Insurance Outsourcing Services
N State Street Retiree Services
O State Street Transfer Agency – Hong Kong and Singapore
P State Street Transfer Agency – Ireland
Q SSTB Co., Ltd. Japan – Trust and Standing Proxy Business
R U.S. Investment Services

# Section V

## Other Information Provided by State Street (unaudited)

### A. Business Continuity Planning

State Street's Business Continuity and Disaster Recovery Programs are part of the overall Operational Resilience umbrella. The objective of the Business Continuity program is to reduce the risk to service delivery in the event of a range of disruption scenarios (severe weather, pandemic, widespread power outage, geopolitical events). The program is overseen by Enterprise Continuity Services ("ECS"), a central function that defines program policy and standards that are applicable to all areas of State Street. The standards are designed for business functions and corporate areas to ensure that operational dependencies, including technologies and third parties, maintain an appropriate level of recovery capabilities commensurate with a range of disruption scenarios and that they are in line with overall service delivery and regulatory expectations.

The objective of the Disaster Recovery Program is to help ensure that our technology infrastructure can be recovered from events that impact our premises, infrastructure or data. It governs resilient designs in our architecture, coordinates regular testing of our capabilities and ensures that our recovery procedures meet our stringent requirements for predictability, timeliness and accuracy.

### B. Privacy and Data Protection Program

The Corporate Compliance Oversight Program supports State Street's compliance with laws and regulations that apply to its global business activities and functions. The program cultivates a culture in which compliance is an integral part of State Street's business environment and is recognized and rewarded in evaluating the performance of its business units and its employees.

As part of that effort, State Street has implemented the Global Privacy and Personal Data Protection Standard ("Privacy Standard") to address the practices that must be adhered to by all employees globally in order to comply with regulatory privacy and data protection requirements and best practices. The Privacy Standard has global applicability, and addresses certain jurisdictional implications and details, including, but not limited to, the following:

- The coverage of the policy (processing and controlling of data, including collection of data and data minimization concepts)
- Roles and responsibilities
- Personal data protection principles
- Cross-border data transfers
- Breach management

- Privacy by design
- Data subject rights requests
- Sharing personal data with third parties

Jurisdictional-specific guidance is in place in countries where additional obligations are imposed by law or common practice in the financial services industry.

To support compliance with the Privacy Standard and relevant data protection laws, the Global Privacy Office, as part of State Street Corporate Compliance, is responsible for designing, maintaining, and overseeing the State Street Privacy Program. The Global Privacy Office, led by the Global Head of Data Privacy, consists of global teams providing privacy compliance management.

In addition to the Privacy Standard and the oversight provided by the Global Privacy Office, business units and corporate functions assess privacy risk and the mitigating control environment as part of the annual Risk Control Self-Assessment ("RCSA") process, which takes into account operational and compliance risks. Privacy controls are periodically monitored and tested by Corporate Compliance and Corporate Audit.

STATE STREET

State Street Corporation
State Street Financial Center
1 Congress Street
Boston, Massachusetts 02114-2010
+1 617 786 3000
www.statestreet.com



07-WMS0017-B