A-LIGN

Derivative Path, Inc.

Type 2 SOC 1

2024

DerivativePATH®

A-LIGN.COM

REPORT ON MANAGEMENT'S DESCRIPTION OF DERIVATIVE PATH, INC.'S SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

Pursuant to Statement on Standards for Attestation Engagements No. 18 (SSAE 18) Type 2

October 1, 2023 to September 30, 2024

Table of Contents

SECTION 1

ASSERTION OF DERIVATIVE PATH, INC.'S MANAGEMENT

ASSERTION OF DERIVATIVE PATH, INC.'S MANAGEMENT

October 7, 2024

We have prepared the description of Derivative Path, Inc.'s ('Derivative Path' or 'the Company') Derivative Trading Platform Services System for processing user entities' transactions entitled "Description of Derivative Path, Inc.'s Derivative Trading Platform Services System throughout the period October 1, 2023 to September 30, 2024", (description) for user entities of the system during some or all of the period October 1, 2023 to September 30, 2024, and their user 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 subservice organizations and user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

Derivative Path uses Amazon Web Services, Inc. (AWS) and Microsoft Azure (Azure) for cloud hosting services, Deposit Trust and Clearance Corporation (DTCC) for swap data repository services, FusionAuth for customer identity and access management (CIAM) services, and SendGrid for transactional and marketing e-mail platform services (collectively, the 'subservice organizations'). The description includes only the control objectives and related controls of Derivative Path and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by Derivative Path in the description can be achieved only if complementary subservice organization controls assumed in the design of Derivative Path's controls are suitably designed and operating effectively, along with the related controls at Derivative Path. The description does not extend to controls of the subservice organizations.

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 Derivative Path 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 Derivative Trading Platform Services System made available to user entities of the system during some or all of the period October 1, 2023 to September 30, 2024, for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

    i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including:

        (1) the types of services provided including, as appropriate, the classes of transactions processed.

        (2) the procedures, within both automated and manual systems, by which services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information prepared for user entities.

        (3) the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

(4) how the system captures significant events and conditions, other than transactions.

(5) the process used to prepare reports and other information for user entities.

(6) services performed by a subservice organization, if any, including whether the inclusive method or the carve-out method has been used in relation to them.

(7) the specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls contemplated in the design of the service organization's controls.

(8) other aspects of our control environment, risk assessment process, information and communication systems (including related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.

ii. includes relevant details of changes to the service organization's system during the period covered by the description.

iii. does not omit or distort information relevant to the scope of the Derivative Trading Platform Services System, while acknowledging that the description is prepared to meet the common needs of broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the Derivative Trading Platform Services System that each individual user entity of the system and its auditor may consider important in its 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, 2023 to September 30, 2024, to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of Derivative Path's controls throughout the period October 1, 2023 to September 30, 2024. The criteria we used in making this assertion were that:

i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization;

ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

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

John Fleming

John Fleming
Chief Operating Officer
Derivative Path, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Derivative Path, Inc.

Scope

We have examined Derivative Path's description of its Derivative Trading Platform Services System for processing user entities' transactions entitled "Description of Derivative Path, Inc.'s Derivative Trading Platform Services System throughout the period October 1, 2023 to September 30, 2024", (description) and the suitability of the design and operating effectiveness of Derivative Path's' controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Assertion of Derivative Path, Inc.'s Management" (assertion). The controls and control objectives included in the description are those that management of Derivative Path believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Derivative Trading Platform Services System that are not likely to be relevant to user entities' internal control over financial reporting.

Derivative Path uses AWS and Azure for cloud hosting services, DTCC for swap data repository services, FusionAuth for CIAM services, and SendGrid for transactional and marketing e-mail platform services. The description includes only the control objectives and related controls of Derivative Path and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by Derivative Path can be achieved only if complementary subservice organization controls assumed in the design of Derivative Path are suitably designed and operating effectively, along with the related controls at Derivative Path. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of Derivative Path'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 and operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In Section 1 of this report, Derivative Path has provided their assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Derivative Path is responsible for preparing the description and their assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

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 to achieve the related control objectives stated in the description, based on our examination.

We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. 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 stated in the description throughout the period October 1, 2023 to September 30, 2024. We believe that the evidence we 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 those controls to achieve the related control objectives stated in the description, based on the criteria in management's 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 stated in the description
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved
- Evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization in their assertion

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

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 errors or omissions in processing or reporting transactions. 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 inadequate or fail.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section 4.

Opinion

In our opinion, in all material respects, based on the criteria described in Derivative Path's assertion,

a. the description fairly presents the Derivative Trading Platform Services System that was designed and implemented throughout the period October 1, 2023 to September 30, 2024.
b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2023 to September 30, 2024 and subservice organizations and user entities applied the complementary user entity controls contemplated in the design of Derivative Path's controls throughout the period October 1, 2023 to September 30, 2024.
c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2023 to September 30, 2024, if complementary subservice organization and user entity controls assume in the design of Derivative Path's controls operated effectively throughout the period October 1, 2023 to September 30, 2024.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4 is intended solely for the information and use of Derivative Path, user entities of Derivative Path's Derivative Trading Platform Services System during some or all of the period October 1, 2023 to September 30, 2024, and the independent auditors of such user entities, who 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.

A-LIGN ASSURANCE

Tampa, Florida
October 7, 2024

SECTION 3

DESCRIPTION OF DERIVATIVE PATH, INC.'S DERIVATIVE TRADING PLATFORM SERVICES SYSTEM

OVERVIEW OF OPERATIONS

Company Background

Established in 2013, Derivative Path is a privately held company with headquarters in Walnut Creek, California and operations in New York and Chicago, assisting financial institutions, buy-side institutions, and commercial end users in executing and managing their over-the-counter interest rate derivative, commodities and foreign exchange transactions. Derivative Path's platform, DerivativeEDGE, helps automate key aspects of clients' operations and the tasks necessary from a trade servicing standpoint.

Derivative Path's platform:

- Is a cloud-based trading platform that focuses on execution and servicing of interest rate and commodity derivatives and foreign exchange, supported by a seasoned front and back-office team
- Tracks and fulfills Dodd-Frank pre-trade compliance requirements, uses a workflow engine tailored to client's approved procedures and access to an independent team of veteran capital markets professionals with current knowledge of Dodd-Frank rules to help drive client marketing / program activities
- Provides access to an independent system and relevant discounted valuations, for example Secured Overnight Financing Rate (SOFR), along with operational support which removes dependence on any one dealer bank
- Provides a variety of reports such as white-labeled resets and Mark-to-market (MTM) statements that can be run on demand or generated automatically
- Connectivity to Depository Trust and Clearing Corporation's (DTCC) Swap Data Repository, end user trades reported by Derivative Path

Description of Services Provided

Program set up activity:

- Establish trading relationships with acceptable dealer counterparties including International Swaps and Derivatives Association (ISDA) and Credit Support Annex (CSA) negotiation
- Help establish credit / risk / ops policies and procedures with considerations around the Volcker Rule
- Help establish client legal loan and swap documents / presentation templates
- Banker training at the onset of the program and annually for lenders (training includes introduction to swaps, application of swaps in commercial lending, credit exposure in derivatives and foreign exchange and information on key operational issues)
- Ongoing support to assist the lending team with all swaps related matters

Pre-Trade Execution Tasks:

- Initial evaluation of client's eligibility, suitability, and credit appetite
- Create client swap presentation and help present to client either in-person or on the phone
- ISDA docs and client regulatory questionnaire created, negotiated, and signed (with the support of Counsel)
- Client Legal Entity Identified (LEI) / Global Market Entity Identifier (GMEI) setup

Trade Execution Tasks:

- Ensure all trade requisites are satisfied (end user eligibility met, credit approved, client presentation made, LEI / GMEI set, and swap docs signed)
- Create and deliver term sheet to Swap Dealer(s)
- Coordinate trade execution timing
- Execute trade with client and Swap Dealer(s)

Post-Trade Execution Tasks:

- Swap Data Repository reporting upload and end-user exception reporting
- Review and match Swap Dealer transaction confirm to client trade details
- Create client confirmations
- Track return of signed client confirmations
- Create client settlement / payment notices
- Create client MTM statements
- Do periodic reviews of client swap positions for new hedging needs
- Assist with swap amendment / termination / credit events
- Assist with margin calls on swap positions
- On-going client trade documentation retention and recordkeeping requirements

Transactions Processing and Reporting

Supported products:

- Interest Rate Swaps
- Swaps with embedded Cap or Floor
- Caps and Floors
- Swaptions
- Cancelable Swaps
- Collars
- Corridors
- Debt
- Debt with Option
- Callable Debt
- Foreign Exchange (FX) Spot
- FX Forwards
- FX Windows
- FX Swaps
- FX Non-Deliverable Forwards
- FX Options
- Commodity Swaps
- Commodity Puts and Calls
- Commodity Collars

New trades executed by the sales team or client are reviewed by the operations team for accuracy and moved to a Validated trade status. Trades are submitted to the Global Trade Repository. Confirmations are received from Dealers and compared to trade terms for accuracy, prior to being sent to the customer for execution. On a daily basis the portfolio is evaluated for all trades requiring floating rate resets and reset notices generated. Reset notices are automatically matched to dealer reset notices and exceptions examined and resolved. Reset notices are then distributed to clients. The portfolio is marked to market using closing curves on each business day. At month end, mark to market reports, 610 / 611 Legal Lending Limit reports, CVA, PFE etc. reports are generated and stored in the document repository.

Significant Events

Derivative Path has implemented automated and manual procedures to capture and address significant event and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with detailed information that impacts the Trading Platform Services system. Please see the procedures, monitoring, and risk assessment procedures described in the relevant sections of this report for further details.

Functional Areas of Operation

The Derivative Path staff provides support for the above services in each of the following functional areas:

- Executive management - provides general oversight and strategic planning of operations
- Sales and Structuring team - provide support to full-service clients; marketing derivative products to end users, executing transactions and related hedges
- Operations team - provides post trade support for trade validation, confirmations, reporting and month end valuations
- Hedge Accounting team - provides support for hedge accounting documentation and reporting
- Development team - responsible for delivering a responsive system that fully complies with the functional specification
- Quality assurance team - verifies that the system complies with the functional specification through functional testing procedures
- System administrators - responsible for effective provisioning, installation / configuration, operation, and maintenance of systems hardware and software relevant to the system
- Customer Support - serves customers by providing product and service information that includes resolving product and service issues
- Audit and Compliance - performs regularly scheduled audits relative to defined standards, provides continuous improvement feedback, and assesses legal and regulatory requirements

Boundaries of the System

The scope of this report includes the Derivative Trading Platform Services System performed in the Walnut Creek, California; Chicago, Illinois; and New York, New York facilities.

This report does not include the cloud hosting services provided by AWS and Azure at the Oregon and Northern Virginia facilities; the swap data repository services provided by DTCC; the CIAM services provided by FusionAuth; and the transactional and marketing e-mail platform services provided by SendGrid, at multiple facilities, respectively.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS and Azure at the Oregon and Northern Virginia facilities; the swap data repository services provided by DTCC; the CIAM services provided by FusionAuth; and the transactional and marketing e-mail platform services provided by SendGrid, at multiple facilities, respectively.

Subservice Description of Services

AWS and Azure provide cloud hosting services for the servers used to store data along with other network components. AWS & Azure is responsible for the physical security of the data centers hosting the cloud infrastructure, including the network equipment at the Oregon and Norther Virginia facilities.

DTCC provides swap data repository services to allow Derivate to fulfill their regulatory reporting obligations under Dodd-Frank.

FusionAuth provides CIAM services. FusionAuth delivers secure single-sign-on (SSO), multi-factor authentication (MFA), and user management capabilities to a wide range of applications.

SendGrid provides a customer communication platform for transactional and marketing e-mail. SendGrid outsources its physical facility security to Steadfast data center. SendGrid ensures that Steadfast has sufficient availability and security controls in place and monitors adherence to those processes and procedures.

Complementary Subservice Organization Controls

Derivative Path's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the Control Objectives related to Derivative Path's services to be solely achieved by Derivative Path control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Derivative Path.

The following subservice organization controls should be implemented by AWS, Azure, DTCC, FusionAuth, and SendGrid to provide additional assurance that the Control Objectives described within this report are met:

Subservice Organization - AWS	
Control Objective	**Control**
CO 2 - Physical Security	Physical access to data centers is approved by an authorized individual.
	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
	Physical access to data centers is reviewed for appropriateness.
	Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
	Physical access points to server locations are managed by electronic access control devices.
	Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
CO 3 - Computer Operations	S3 performs continuous integrity checks of the data at rest. Objects are continuously validated against their checksums to prevent object corruption.
	When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.
	Objects are stored redundantly across multiple fault-isolated facilities.
	If enabled by the customer, Relational Database Services (RDS) backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.
CO 5 - Information Security	Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
	Incidents are logged within a ticketing system, assigned severity rating, and tracked to resolution.
	Access attempts to recovery key materials are reviewed by authorized operators on a cadence defined in team processes.

Subservice Organization Controls - Azure	
Control Objective	**Control**
CO 2 - Physical Security	Security verification and check-in for personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors are required.
	Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
	Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
	The datacenter facility is monitored 24x7 by security personnel.
	Datacenter Management team maintains and tests datacenter management environmental equipment within the facility according to documented policy and maintenance procedures.
CO-3 Computer Operations	Backups of key service components are performed regularly and stored in fault tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately.
	Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.
	Customer data is automatically replicated within Azure to minimize isolated faults.
	Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately.
	Backup restoration procedures are defined, and backup data integrity checks are performed through standard restoration activities.
	Offsite backups are tracked and managed to maintain accuracy of the inventory information.
	Production data is encrypted on backup media.
	Azure services are configured to automatically restore customer services upon detection of hardware and system failures.
	Microsoft operating system updates for virtual machines are made available through Microsoft Security Response Center (MSRC) site and Windows Update.
CO 5 - Information Security	External traffic to the customer VM(s) is restricted to customer - enabled ports and protocols.
	Azure network is segregated to separate customer traffic from management traffic.
	Each Online Service’s customer’s data is segregated from other Online Services’ customers’ data, either logically or physically.

Subservice Organization - DTCC	
Control Objective	**Control Expected to be Implemented**
CO 7 - Valuation Validation Procedures	DTCC is expected to implement controls for accurately validating data, reporting derivative transactions, and reporting any deviations or identified issues.

Subservice Organization - FusionAuth	
Control Objective	**Control**
CO-3 Computer Operations	Data in transit over the public Internet is encrypted with industry-standard algorithms.
	Customer data is securely disposed of after its retention period passes, and any retained data is sanitized and anonymized.
	Managed data stores such as RDS are configured with encryption turned on.
	External users are provided with a support channel for reporting systems failures, incidents, concerns, and other complaints to appropriate personnel.

Subservice Organization - SendGrid	
Control Objective	**Control**
CO 6 - Data Communications	Data backups housing customer data are encrypted at rest.
	Customer passwords and application programming interface (API) keys are individually salted and hashed while stored.
	Secure data transmission protocols are used to encrypted confidential and sensitive data when transmitted over public networks.

Derivative Path management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant Control Objectives through written contracts, such as service level agreements. In addition, Derivative Path performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing the applicable attestation reports over services provided by subservice organizations at least annually.
- Reviewing and reconciling output reports and security documents provided by DTCC.
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organizations.

Significant Changes Since the Last Review

On January 1, 2024, Derivative Path introduced a new business offering, commodities, that provides clients to trade over the-counter commodities. The controls specific to this offering were implemented beginning on January 1, 2024.

CONTROL ENVIRONMENT

Integrity and Ethical Values

Derivative Path has implemented, maintained, and regularly communicated a code of conduct and other policies regarding acceptable business practices, guidance on conflicts of interest, and expected standards of ethical and moral behavior. Derivative Path's management conducts business dealings with personnel, vendors, clients, investors, creditors, competitors, and auditors on a high ethical plane and insists others have similar business practices. These business practices are enforced by requiring personnel to acknowledge the employee handbook at the beginning of employment indicating that they will adhere to the code of conduct and other policies regarding acceptable business practices.

Commitment to Competence

Derivative Path's team consists of experienced professionals that provide formal mentoring to newly hired personnel during the initial period of employment and continual hands-on and formal training to ensure that the requisite skill sets are developed by the personnel for their assigned job responsibilities. Training is a focal point for all personnel and is driven and supported by the management team. Training is reinforced by maintaining job descriptions that contain requirements of knowledge and skills needed to perform each job adequately and successfully.

Management's Philosophy and Operating Style

Derivative Path's leadership takes a relatively conservative approach regarding the security of information and risk associated with business processes and practices.

Organizational Structure and Assignment of Authority and Responsibility

The responsibilities of key positions within Derivative Path are clearly defined and communicated. Individuals that hold key positions are experienced, knowledgeable, and have lengthy tenure with the company or industry. Derivative Path's organizational structure supports communication of information both up to leadership as well as down to support staff.

Derivative Path has well-defined and clear communication channels to disseminate information within the organization; this enables Derivative Path's management to react to market and regulation changes and to successfully achieve its goals and objectives. Derivative Path is appropriately staffed to support its operations, particularly with respect to critical areas such as application change management, data processing and information technology system support.

Human Resources Policies and Practices

Derivative Path maintains job descriptions that contain requirements of knowledge and skills needed to adequately perform key positions within the organization. An employee handbook is communicated to personnel to illustrate expected level of performance, information technology skill set and employee behavior. Mentoring programs are utilized to communicate the expected level of performance, required skill sets and employee behavior. All personnel handling client data are vetted and trained in proper handling of data privacy and confidentiality.

RISK ASSESSMENT

Derivative Path has placed into operations a risk assessment process to identify and manage risks that could affect the organization's ability to provide accurate and reliable reporting to clients relevant to trading and execution services. This process requires management to identify significant risks inherent in the reporting on derivative trade information that affect financial transactions for clients and to implement appropriate measures to monitor and manage these risks.

This process has identified risks resulting from the nature of the services provided by Derivative Path and management has implemented various instruments designed to manage these risks. Derivative Path's risk assessment includes the significant impacts to its clients' financial information for services provided. The following is a list of factors considered during Derivative Path's risk assessment process:

- Operational risk associated with computerized information systems, manual processes involved in transaction processing and external systems
- Changes in the operating environment
- Fiduciary risk associated with acting on behalf of clients
- Outsourcing IT functions to third-parties
- New personnel
- Rapid growth
- New or revamped information systems
- New technology
- New business models, products, or activities
- Government regulations
- Other privacy and processing rules and regulations

CONTROL OBJECTIVE AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

Along with assessing risks, Derivative Path has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of those objectives.

Selection and Development of Control Activities Specified by the Service Organization

Control activities are a part of the process by which Derivative Path strives to achieve its business objectives. Derivative Path has applied a risk management approach to the organization in order to select and develop control activities. After relevant risk have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved when necessary to meet the overall objectives of the organization.

Derivative Path's Control Objectives and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the Control Objectives and related control activities are included in Section 4, they are, nevertheless, an integral part of Derivative Path's description of the Derivative Trading Platform system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, adjacent to the service organization's description of control activities. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

MONITORING

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Derivative Path's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Vendor management procedures have been defined to review the services provided by external providers. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Derivative Path's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Derivative Path's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Derivative Path's personnel.

Vendor Management

Derivative Path has defined the following activities to oversee controls performed by vendors that could impact the Derivative Trading Platform system:

- Reviewing attestation reports over services provided by vendors and subservice organizations at least annually

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

INFORMATION AND COMMUNICATION SYSTEMS

Information Systems

Derivative Path has implemented mechanisms to track and record operational data to make strategic decisions and ensure objectives are consistently achieved. Information gathered from systems enable Derivative Path to understand business trends in order to maximize efforts and provide optimal services.

Infrastructure

Primary infrastructure used to provide Derivative Path's Derivative Trading Platform Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Active Directory	Microsoft Windows	Internal Directory services
Derivative Path leverages a variety of AWS services for cloud hosting. Information on the listed services can be found on AWS website https://aws.amazon.com/products/		
AWS - Virtual Private Cloud (VPC), Elastic Block Store (EBS), Elastic Load Balancer (ELB), Web Application Firewall (WAF), etc.	Cloud	Provides the infrastructure and platform to host the SaaS solution

Software

Primary software used to provide Derivative Path's Derivative Trading Platform Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
VNS3	Linux	Virtual Private Network (VPN) appliance for site-to-site partner integration
Tomcat	Linux	Web Services
IBM Messaging and Queuing Middleware (MQ)	Linux	Synchronous messaging between product and the Depository Trust & Clearing Corporation (DTCC)
Microsoft Internet Information Services (IIS)	Windows Server 2019	Provide web services for the customer facing portal
Numerix	Windows Server 2019	Perform analytics against gathered data on behalf of clients
MS SQL	Windows Server 2019	Database
MySQL	Linux	Database
PostgreSQL	Linux	Database
Coralogix	Windows / Linux	Monitoring of all system operations
OpsGenie	Proprietary	Alerting of events that require action to be taken
FusionAuth	Proprietary	Authentication and authorization service to access the DerivativeEdge Application

Primary Software		
Software	**Operating System**	**Purpose**
SendGrid	Proprietary	Communication platform for transactional and marketing e-mail
Atlassian	Proprietary	Jira and Bitbucket- source code repository
Split.IO	Proprietary	Continuous Integration/development (CI/CD) and full stack experimentation
Rapid7	Windows / Linux	Vulnerability management of all systems
Sophos Intercept X	Windows / Linux	Real time centrally managed antivirus scanning, EDR, and reporting
Zscaler	Windows / Linux	Zscaler Private Access (ZPA) delivers a zero trust model for employee VPN access

Communication Systems

Throughout the organization, Derivative Path conducts frequent meetings to identify and address moderate and significant issues affecting the company's operations. Defined corporate policies and procedures are used as the established vehicles for addressing and monitoring activities, accomplishments, and issues. Management meetings provide the platform for owners and senior management to communicate and respond to operational tasks and issues. At all levels, the company has established communication channels to promote and distribute information up and down the defined organizational structure.

COMPLEMENTARY USER ENTITY CONTROLS

Derivative Path's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Control Objectives related to Derivative Path's services to be solely achieved by Derivative Path control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Derivative Path.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Control Objectives described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

Control Objective 1 - Control Environment

1. User entities are responsible for determining whether Derivative Path's security infrastructure is appropriate for its needs and for notifying the service organization of any required modifications.
2. User entities are responsible for understanding and complying with their contractual obligations to Derivative Path.
3. User entities are responsible for notifying Derivative Path, in a timely manner, when changes are made to technical, billing, or administrative contact information.

Control Objective 2 - Physical Security

1. User entities are responsible for determining whether Derivative Path's security infrastructure is appropriate for its needs and for notifying the service organization of any required modifications.

Control Objective 3 - Computer Operations

1. User entities are responsible for determining whether Derivative Path's security infrastructure is appropriate for its needs and for notifying the service organization of any required modifications.
2. User entities are responsible for immediately notifying Derivative Path of any actual or suspected information security breaches, including compromised user accounts.
3. User entities are responsible for understanding and complying with their contractual obligations to Derivative Path.
4. User entities are responsible for defining any encryption methodology utilized in relation to Derivative Path's systems or service(s).
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address their inability to access or utilize Derivative Path's services.
6. Other than DerivativeEDGE, which is maintained by Derivative Path, user entities are responsible for maintaining their own internal systems of record.

Control Objective 5 - Information Security

1. User entities are responsible for immediately notifying Derivative Path of any actual or suspected information security breaches, including compromised user accounts.
2. User entities are responsible for ensuring the confidentiality of any user accounts and passwords assigned to them for use with Derivative Path's systems.
3. User entities are responsible for ensuring that Derivative Path is notified of any required user account maintenance in a timely manner.
4. User entities are responsible for securing the method to request and remove access to ensure that appropriate users are requesting access to Derivative Path's systems.
5. User entities are responsible for ensuring that user IDs and passwords are assigned only to authorized individuals and that the roles assigned to the user account are appropriate.
6. User entities are responsible for determining whether Derivative Path's security infrastructure is appropriate for its needs and for notifying the service organization of any required modifications.
7. User entities are responsible for immediately notifying Derivative Path of any actual or suspected information security breaches, including compromised user accounts.
8. User entities are responsible for notifying Derivative Path, in a timely manner, when changes are made to technical, billing, or administrative contact information.
9. User entities are responsible for defining any encryption methodology utilized in relation to Derivative Path's systems or service(s).
10. User entities are responsible for ensuring the confidentiality of any user accounts and passwords assigned to them for use with Derivative Path's systems.
11. User entities are responsible for securing the method to request and remove access to ensure that appropriate users are requesting access to Derivative Path's systems.
12. User entities are responsible for defining the communications method utilized to connect to Derivative Path's system (e.g., direct connections, over public networks, etc.).

SECTION 4

DESCRIPTION OF DERIVATIVE PATH, INC.'S CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

GUIDANCE REGARDING DESCRIPTION OF DERIVATIVE PATH, INC.'S CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

A-LIGN ASSURANCE's examination of the controls of Derivative Path was limited to the control objectives and related control activities specified by the management of Derivative Path and did not encompass all aspects of Derivative Path's operations or operations at user organizations. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 18 (SSAE 18).

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether a SSAE 18 report meets the user auditor's objectives, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the processing of the user organization's transactions
- Understand the flow of significant transactions through the service organization
- Determine whether the control objectives are relevant to the user organization's financial statement assertions
- Determine whether the service organization's controls are suitably designed to prevent or detect processing errors that could result in material misstatements in the user organization's financial statements and determine whether they have been implemented

CONTROL AREA 1 **CONTROL ENVIRONMENT**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that management's tone influences the control consciousness of its personnel and provides discipline, structure and security to the organization, and management monitors the subservice organizations to ensure controls are in place to achieve the organization's service level commitments.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.1	An employee handbook of policies and procedures that includes the organization's code of business ethics and conduct is documented and available to guide personnel in the performance of their job responsibilities.	Inspected the employee handbook, the code of ethics and the entity's SharePoint site to determine that an employee handbook of policies and procedures that includes the organization's code of business ethics and conduct was documented and available to guide personnel in the performance of their job responsibilities.	No exceptions noted.
1.2	Personnel are required to sign an acknowledgement form indicating that they have received the employee handbook, and have read, understand, and agree to adhere to the policies and procedures contained within the handbook.	Inspected the signed handbook acknowledgement for a sample of new hires to determine that personnel were required to sign an acknowledgement form indicating that they have received the employee handbook, and have read, understand, and agree to adhere to the policies and procedures contained within the handbook.	No exceptions noted.
1.3	Personnel are required to sign a confidentiality agreement during the onboarding process that contains a statement indicating that they will protect the confidentiality of client data.	Inspected the signed confidentiality agreement for a sample of new hires to determine that personnel were required to sign a confidentiality agreement during the onboarding process that contains a statement indicating that they will protect the confidentiality of client data.	No exceptions noted.
1.4	Personnel and contractors are subjected to screening procedures as a component of the onboarding process.	Inspected the completed background check documentation, the candidate evaluation form, and interview notes for a sample of new hires to determine that personnel and contractors were subjected to screening procedures as a component of the onboarding process.	No exceptions noted.

CONTROL AREA 1 **CONTROL ENVIRONMENT**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that management's tone influences the control consciousness of its personnel and provides discipline, structure and security to the organization, and management monitors the subservice organizations to ensure controls are in place to achieve the organization's service level commitments.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.5	Personnel training programs are provided to new hire personnel to protect clients' personally identifiable information (PII) and provide guidance on the performance of job responsibilities.	Inspected the training materials and the completed training tracking tool for a sample of new hires to determine that personnel training programs were provided to new hire personnel to protect clients' PII and provide guidance on the performance of job responsibilities.	No exceptions noted.
1.6	Formal information security training is performed on an annual basis for current employees.	Inspected the completed information security training tracking tool for a sample of current employees to determine that formal information security training was performed on an annual basis for current employees.	No exceptions noted.
1.7	The board of directors meet at a minimum bi- annually to discuss organizational operations and goals.	Inspected the board of directors meeting minutes to determine that the board of directors met at a minimum bi-annually to discuss organizational operations and goals.	No exceptions noted.
1.8	Formal employee performance evaluations are completed and documented annually to provide personnel insights on accomplishments and required changes in role or skill sets.	Inspected the completed performance evaluation form for a sample of current employees to determine that formal employee performance evaluations were completed and documented annually to provide personnel insights on accomplishments and required changes in role or skill sets.	No exceptions noted.
1.9	An employee/consultant onboarding checklist is utilized to document activities that facilitate the onboarding process.	Inspected the completed onboarding checklist for a sample of new hires to determine that an employee/consultant onboarding checklist was utilized to document activities that facilitate the onboarding process.	No exceptions noted.
1.10	An employee/consultant departure checklist is utilized to document activities that facilitate the offboarding process.	Inspected the completed termination checklist for a sample of terminated employees to determine that an employee/consultant departure checklist was utilized to document activities that facilitate the offboarding process.	No exceptions noted.

CONTROL AREA 1 **CONTROL ENVIRONMENT**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that management's tone influences the control consciousness of its personnel and provides discipline, structure and security to the organization, and management monitors the subservice organizations to ensure controls are in place to achieve the organization's service level commitments.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.11	The subservice organizations are monitored and managed to ensure controls are in place to achieve the organization's service level commitments.	Inspected the completed attestation report and vendor review for a sample of subservice organizations to determine that the subservice organizations were monitored and managed to ensure controls were in place to achieve the organization's service level commitments.	No exceptions noted.

CONTROL AREA 2 **PHYSICAL SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that physical access to the business premises and information systems is restricted to properly authorized individuals.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.1	Physical access security policies and procedures are documented that provide guidance to personnel on the performance of job responsibilities.	Inspected the information security policy to determine that physical access security policies and procedures were documented that provide guidance to personnel on the performance of job responsibilities.	No exceptions noted.
2.2	A card key access system restricts access to the perimeter door of the corporate office.	Inspected the badge access user listing and zone definitions to determine that a card key access system restricted access to the perimeter door of the corporate office.	No exceptions noted.
2.3	Card key access requests require an approved access request checklist.	Inspected the badge access user listing and the completed onboarding checklist for a sample of new hires to determine that a card key access request required an approved access request checklist.	No exceptions noted.
2.4	Access to administer the card key access system is restricted to personnel based on their job responsibilities.	Inquired of the Information Security Officer, regarding administrative access to the key card system to determine that access to administer the card key access system was restricted to personnel based on their job responsibilities.	No exceptions noted.
		Inspected the card key administrative user access listing and access rights to determine that access to administer the card key access system was restricted to personnel based on their job responsibilities.	No exceptions noted.
2.5	Access to the corporate office is reviewed monthly to identify suspicious activity.	Inquired of the Information Security Officer, regarding the physical user access review process to determine that access to the corporate office was reviewed monthly to identify suspicious activity.	No exceptions noted.
		Inspected the completed physical user access review for a sample of months to determine that access to the corporate office was reviewed monthly to identify suspicious activity.	No exceptions noted.

CONTROL AREA 2 **PHYSICAL SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that physical access to the business premises and information systems is restricted to properly authorized individuals.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.6	Physical keys are utilized to access the corporate office if the card key access system is inoperable. Keys are restricted to a limited number of officers and tracked and monitored via a physical key inventory listing.	Inquired of the Information Security Officer, regarding physical access to the building facilities to determine that physical keys were utilized to access the corporate office, if the card key access system was inoperable, and that keys were restricted to a limited number of officers and tracked and monitored via a physical key inventory listing.	No exceptions noted.
		Inspected the key inventory listing to determine that physical keys were utilized to access the corporate office, if the card key access system was inoperable, and that keys were restricted to a limited number of officers and tracked and monitored via a physical key inventory listing.	No exceptions noted.
2.7	Personnel card key access privileges are revoked as a component of the offboarding process.	Inquired of the Information Security Officer, regarding physical access termination procedures to determine that personnel card key access privileges were revoked as a component of the offboarding process.	No exceptions noted.
		Inspected the bade system user access listing and the supporting termination checklist for a sample of terminated employees to determine that personnel card key access privileges were revoked as a component of the offboarding process.	No exceptions noted.
2.8	Card key access is reviewed monthly to confirm that terminated personnel access rights have been revoked.	Inspected the badge system user access listing and the completed physical user access review for a sample of months to determine that card key access was reviewed monthly to confirm that terminated personnel access rights were revoked.	No exceptions noted.

CONTROL AREA 3 **COMPUTER OPERATIONS**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that system deviations, problems and errors are identified, tracked, recorded, and resolved in a complete, accurate and timely manner. System data is regularly backed up, backups are encrypted and restricted to authorized personnel.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.1	A help desk ticketing system is utilized to track and respond to reported incidents.	Inspected the supporting incident ticket for a sample of incidents to determine that a help desk ticketing system was utilized to track and respond to reported incidents.	No exceptions noted.
3.2	A patch management and release system are utilized to monitor and release new security patches to production servers.	Inspected the patch management and release system and the patch update applied to the system for a sample of months to determine that a patch management and release system was utilized to monitor and release new security patches to production servers.	No exceptions noted.
3.3	Production servers and workstations are equipped with antivirus software to detect and prevent the transmission of data or files that contain certain virus signatures.	Inspected the centrally managed antivirus software configurations, the threat protection base policy and an example server and workstation to determine that production servers and workstations were equipped with antivirus software to detect and prevent the transmission of data or files that contain certain virus signatures.	No exceptions noted.
3.4	Antivirus software automatically updates virus signatures on production servers when updates are made available from the manufacturer and weekly for workstations.	Inspected the centrally managed antivirus software configurations, the threat protection base policy and an example server and workstation to determine that antivirus software automatically updated virus signatures on production servers when updates were made available from the manufacturer and weekly for workstations.	No exceptions noted.
3.5	Antivirus software performs scans on production servers in real-time, performs a full system scan for virus signatures weekly and performs a full system scan for virus signatures daily for workstations.	Inspected the centrally managed antivirus software configurations, the threat protection base policy and an example server and workstation to determine that antivirus software performed scans on production servers in real-time, performed a full system scan for virus signatures weekly and performed a full system scan for virus signatures daily for workstations.	No exceptions noted.

CONTROL AREA 3 **COMPUTER OPERATIONS**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that system deviations, problems and errors are identified, tracked, recorded, and resolved in a complete, accurate and timely manner. System data is regularly backed up, backups are encrypted and restricted to authorized personnel.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.6	The backup system is configured to encrypt backed up data as a component of the backup process.	Inspected the backup system encryption configuration to determine that the backup system was configured to encrypt backed up data as a component of the backup process.	No exceptions noted.
3.7	Backups are replicated to a separate availability zone for redundancy in real-time.	Inspected the automated backup replication configuration and an example of a successful backup replication log to determine that backups were replicated to a separate availability zone for redundancy in real-time.	No exceptions noted.
3.8	Access to backed up data is restricted to personnel based on their job responsibilities.	Inquired of the Information Security Officer, regarding access to backed up data to determine that access to backed up data was restricted to personnel based on their job responsibilities.	No exceptions noted.
		Inspected the listing of users with access to the backup system to determine that access to backed up data was restricted to personnel based on their job responsibilities.	No exceptions noted.

CONTROL AREA 4 **APPLICATION CHANGE MANAGEMENT**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that application software is developed to effectively support application functionality and reporting requirements, and that changes are authorized and tested prior to production migration.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.1	Software development life cycle (SDLC) policies and procedures are documented and available to guide personnel through the development and change management process.	Inspected the SDLC and source code policies and procedures to determine that software development life cycle policies and procedures were documented and available to guide personnel through the development and change management process.	No exceptions noted.
4.2	A change management ticketing system is utilized to record and track application change requests.	Inspected the change management ticketing system and the supporting change ticket for a sample of application changes to determine that a change management ticketing system was utilized to record and track application change requests.	No exceptions noted.
4.3	Application change requests submitted to the development group includes a description of change, prioritization, and management's approval to begin development.	Inspected the supporting change ticket for a sample of application changes to determine that application change requests submitted to the development group included a description of change, prioritization, and management's approval to begin development.	No exceptions noted.
4.4	Application development and testing efforts are performed in environments that are logically and physically separated from the production environment.	Inspected the separate staging, development, and production environments and network diagram to determine that application development and testing efforts were performed in environments that were logically and physically separated from the production environment.	No exceptions noted.
4.5	Version control software is utilized to centrally maintain application source code versions.	Inspected the version control software dashboard to determine that software was utilized to centrally maintain application source code versions.	No exceptions noted.
4.6	Access to the version control software is restricted to personnel based on their job responsibilities.	Inquired of the Information Security Officer, regarding version control access to determine that access to the version control software was restricted to personnel based on their job responsibilities.	No exceptions noted.

CONTROL AREA 4 **APPLICATION CHANGE MANAGEMENT**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that application software is developed to effectively support application functionality and reporting requirements, and that changes are authorized and tested prior to production migration.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the version control software user access listing to determine that access to the version control software was restricted to personnel based on their job responsibilities.	No exceptions noted.
4.7	Developer testing is completed prior to promoting to quality assurance testing.	Inspected the SDLC policies and procedures and the supporting change ticket for a sample of application changes to determine that developer testing was completed prior to promoting to quality assurance testing.	No exceptions noted.
4.8	Quality assurance testing is completed, documented, and approved prior to scheduling migration to the production environment.	Inspected the SDLC policies and procedures and the supporting change ticket for a sample of application changes to determine that quality assurance testing was completed, documented, and approved prior to scheduling migration to the production environment.	No exceptions noted.
4.9	Application vulnerability testing is performed prior to scheduling the migration of a new application version release to the production environment.	Inspected the supporting change ticket for a sample of application changes to determine that application vulnerability testing was performed prior to scheduling the migration of a new application version release to the production environment.	No exceptions noted.
4.10	Application changes are approved prior to migration to the production environment.	Inspected the supporting change ticket for a sample of application changes to determine that application changes were approved prior to migration to the production environment.	No exceptions noted.
4.11	The ability to migrate changes to the production environment is restricted to personnel based on their job responsibilities.	Inquired of the Chief Technology Officer regarding change migration to determine that the ability to migrate changes to the production environment was restricted to personnel based on their job responsibilities.	No exceptions noted.

CONTROL AREA 4 **APPLICATION CHANGE MANAGEMENT**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that application software is developed to effectively support application functionality and reporting requirements, and that changes are authorized and tested prior to production migration.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the production user access listing to determine that the ability to migrate changes to the production environment was restricted to personnel based on their job responsibilities.	No exceptions noted.

CONTROL AREA 5 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	General		
5.1	Information security policies and procedures are documented to establish organizational system and information security standards.	Inspected the organizational and information security policies and procedures to determine that information security policies and procedures were documented to establish organizational system and information security standards.	No exceptions noted.
5.2	An information technology (IT) access request is approved prior to granting access to the internal network and production systems.	Inspected the information security and the system access control policies and procedures, the in-scope user listings and the supporting user access request ticket for a sample of new hires to determine that an IT access request was approved prior to granting access to the internal network and production systems.	No exceptions noted.
5.3	System access is revoked as a component of the termination process.	Inspected the information security and the system access control policies and procedures, the in-scope user listings, and the supporting user access revocation ticket and check list for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
5.4	External vulnerability scans are performed by third-party providers monthly on the production system to identify potential system vulnerabilities, evaluate results, and take appropriate actions if necessary.	Inspected the completed vulnerability scan test results for a sample of months to determine that external vulnerability scans were performed by third-party providers monthly on the production system to identify potential system vulnerabilities, evaluate results, and take appropriate actions if necessary.	No exceptions noted.
5.5	Penetration tests are performed by a third-party on an annual basis.	Inspected the completed third-party penetration test report to determine that penetration tests were performed by a third-party on an annual basis.	No exceptions noted.

CONTROL AREA 5 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.6	Internal penetration tests are performed by company personnel on a quarterly basis.	Inspected the completed internal penetration test report for a sample of quarters to determine that internal penetration tests were performed by company personnel on a quarterly basis.	No exceptions noted.
	Production Network - AWS Identity and Access Management (IAM)		
5.7	Production network users are authenticated via individually assigned user accounts and passwords. The production network is configured to enforce password requirements that include: • Password history • Maximum password age • Password length • Complexity • MFA	Inquired of the Information Security Officer, regarding production network authentication to determine that production network users were authenticated via individually assigned user accounts and passwords. The production network was configured to enforce password requirements that included: • Password history • Maximum password age • Password length • Complexity • MFA	No exceptions noted.
		Observed the authentication of a user to the production network to determine that production network users were authenticated via individually assigned user accounts and passwords. The production network was configured to enforce password requirements that included: • Password history • Maximum password age • Password length • Complexity	No exceptions noted.

CONTROL AREA 5 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the production network user listing and password configurations to determine that production network users were authenticated via individually assigned user accounts and passwords. The production network was configured to enforce password requirements that included: • Password history • Maximum password age • Password length • Complexity	No exceptions noted.
5.8	Administrative access to the production network is restricted to personnel with administrative job responsibilities.	Inquired of the Information Security Officer, regarding administrative access to the production network to determine that administrative access to the production network was restricted to personnel with administrative job responsibilities.	No exceptions noted.
		Inspected the production network administrator user listing and access roles to determine that administrative access to the production network was restricted to personnel with administrative job responsibilities.	No exceptions noted.
5.9	Production network audit policy configurations are in place that include: • Management Events • Data Events • Insight Events	Inspected the production network audit logging configurations and an example production network audit log extract to determine that production network audit policy configurations were in place that included: • Management Events • Data Events • Insight Events	No exceptions noted.

CONTROL AREA 5 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Operating Systems - Windows, Linux		
5.10	Operating system access is restricted via role-based security privileges defined within the access control system.	Inquired of the Information Security Officer, regarding operating system access to determine that operating system access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Inspected the operating system user listing and access roles to determine that operating system access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
5.11	Administrative access to the operating system is restricted to personnel with administrative job responsibilities.	Inquired of the Information Security Officer, regarding the administrative access to the operating systems to determine that administrative access to the operating system was restricted to personnel with administrative job responsibilities.	No exceptions noted.
		Inspected the operating system administrator user listing and access roles to determine that administrative access to the operating system was restricted to personnel with administrative job responsibilities.	No exceptions noted.
5.12	Windows operating systems are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity	Inspected the Windows operating system authentication configurations to determine that windows operating systems were configured to enforce password requirements that included: • Password history • Password age • Password length • Complexity	No exceptions noted.
5.13	Linux operating systems require users to authenticate via Secure Shell (SSH) keys.	Inquired of the Information Security Officer, regarding Linux operating system authentication to determine that Linux operating systems required users to authenticate via SSH keys.	No exceptions noted.

CONTROL AREA 5 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Observed a privileged user authenticate to the Linux server to determine that Linux operating systems required users to authenticate via SSH keys.	No exceptions noted.
5.14	Windows operating system audit policy configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the Windows operating system audit logging configurations and an example operating system audit log extract to determine that Windows operating system audit policy configurations were in place that include: • Account logon events • Account management • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
	Database - MySQL		
5.15	Database access is restricted via the credentials and group policy settings inherited from the primary domain controller.	Inquired of the Information Security Officer, regarding production database access to determine that database access was restricted via the credentials and group policy settings inherited from the primary domain controller.	No exceptions noted.
		Observed the authentication of a user to the production database to determine that database access was restricted via the credentials and group policy settings inherited from the primary domain controller.	No exceptions noted.
		Inspected the production database user listing and access roles to determine that database access was restricted via the credentials and group policy settings inherited from the primary domain controller.	No exceptions noted.

CONTROL AREA 5 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.16	Access to the databases is restricted to authorized applications and personnel with administrative job responsibilities.	Inquired of the Information Security Officer, regarding administrative access to the production database to determine that access to the database was restricted to authorized applications and personnel with administrative job responsibilities.	No exceptions noted.
		Inspected the production database administrator user listing and access roles and the network domain and group policy settings to determine that access to the database was restricted to authorized applications and personnel with administrative job responsibilities.	No exceptions noted.
5.17	Client data is segregated through code utilizing a parent child hierarchy, with the client being the data isolator.	Inspected the client database schema to determine that client data was segregated through code utilizing a parent child hierarchy, with the client being the data isolator.	No exceptions noted.
5.18	Database audit policy configurations are in place that include user activity and system events.	Inspected the production database audit logging configurations and an example production database audit log extract to determine that database audit policy configurations were in place that included user activity and system events.	No exceptions noted.
	Production Application - DerivativeEdge		
5.19	Production application users are authenticated via individually assigned user accounts and passwords. The production application is configured to enforce password requirements that include: • Password history • Password length • Complexity • MFA	Inquired of the Information Security Officer, regarding production application authentication to determine that production application users were authenticated via individually assigned user accounts and passwords. The production application was configured to enforce password requirements that included: • Password history • Password length • Complexity • MFA	No exceptions noted.

CONTROL AREA 5 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Observed the authentication of a user to the production application to determine that production application users were authenticated via individually assigned user accounts and passwords. The production application was configured to enforce password requirements that included: • Password history • Password length • Complexity • MFA	No exceptions noted.
		Inspected the production application user listing and password configurations to determine that production application users were authenticated via individually assigned user accounts and passwords. The production application was configured to enforce password requirements that included: • Password history • Password length • Complexity • MFA	No exceptions noted.
5.20	Access to administer the application is restricted to personnel based on their job responsibilities.	Inquired of the Information Security Officer, regarding administrative access to the production application to determine that access to administer the application was restricted to personnel based on their job responsibilities.	No exceptions noted.
		Inspected the production application administrator user listing and access roles to determine that access to administer the application was restricted to personnel based on their job responsibilities.	No exceptions noted.

CONTROL AREA 5 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.21	The production application is configured to record specific events and user activities, and alerts personnel via e-mail when specific events are identified.	Inspected the production application audit logging configurations and an example production application audit log extract to determine that the production application was configured to record specific events and user activities, and alerts personnel via e-mail when specific events were identified.	No exceptions noted.
	Zero Trust Access - Zscaler		
5.22	ZPA user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Information Security Officer, regarding ZPA access to determine that ZPA user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Inspected the ZPA user listing to determine that ZPA user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
5.23	The ability to administer ZPA access is restricted to personnel based on their job responsibilities.	Inquired of the Information Security Officer, regarding administrative access to the ZPA to determine that the ability to administer ZPA access was restricted to personnel based on their job responsibilities.	No exceptions noted.
		Inspected the ZPA administrator user listing to determine that the ability to administer ZPA access was restricted to personnel based on their job responsibilities.	No exceptions noted.
5.24	ZPA users are authenticated via MFA prior to being granted remote access to the system.	Inquired of the Information Security Officer, regarding ZPA authentication to determine that ZPA users were authenticated via MFA prior to being granted remote access to the system.	No exceptions noted.
		Observed the authentication of a user to the ZPA to determine that ZPA users were authenticated via MFA prior to being granted remote access to the system.	No exceptions noted.

CONTROL AREA 5 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the ZPA authentication configurations to determine that ZPA users were authenticated via MFA prior to being granted remote access to the system.	No exceptions noted.

CONTROL AREA 6 DATA COMMUNICATIONS

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that data maintains its integrity and security as it is transmitted between third-parties and the service organization.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.1	Firewall rules only allow specific ports and hosts to connect to the entity's environment.	Inspected the firewall rulesets for a sample of production servers to determine that firewall rules only allowed specific ports and hosts to connect to the entity's environment.	No exceptions noted.
6.2	A firewall utilizing stateful inspection packet filtering is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the firewall rulesets for a sample of production servers to determine that a firewall utilizing stateful inspection packet filtering was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
6.3	Network address translation (NAT) is utilized to manage and mask internal IP addresses, and routable IP addresses are not permitted on the internal network.	Inspected the NAT configurations and internal IP address ranges to determine that NAT was utilized to manage and mask internal IP addresses, and routable IP address ranges were not permitted on the internal network.	No exceptions noted.
6.4	Administrative access to the firewall system is authenticated via a unique user account and is restricted to personnel with firewall administrative responsibilities.	Inquired of the Chief Technology Officer, regarding firewall administrative access to determine that administrative access to the firewall system was authenticated via a unique user account and was restricted to personnel with firewall administrative responsibilities.	No exceptions noted.
		Inspected the firewall administrative user access listing to determine that administrative access to the firewall system was authenticated via a unique user account and was restricted to personnel with firewall administrative responsibilities.	No exceptions noted.
6.5	External vulnerability scans are performed by third-party providers monthly on the production system to identify potential system vulnerabilities, evaluate results, and take appropriate actions if necessary.	Inspected the completed vulnerability scan test results for a sample of months to determine that external vulnerability scans were performed by third-party providers monthly on the production system to identify potential system vulnerabilities, evaluate results, and take appropriate actions if necessary.	No exceptions noted.

CONTROL AREA 6 **DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that data maintains its integrity and security as it is transmitted between third-parties and the service organization.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.6	Penetration tests are performed by a third-party on an annual basis.	Inspected the completed third-party penetration test report to determine that penetration tests were performed by a third-party on an annual basis.	No exceptions noted.
6.7	Internal penetration tests are performed by company personnel on a quarterly basis.	Inspected the completed internal penetration test report for a sample of quarters to determine that internal penetration tests were performed by company personnel on a quarterly basis.	No exceptions noted.
6.8	Customer web sessions are encrypted using 256 RSA encryption and restricted to a specific IP address.	Inspected the customer web session certificate to determine that a valid certificate with 256 RSA encryption was used for web sessions and restricted to a specific IP address.	No exceptions noted.
6.9	A VPN is utilized by personnel for remote access to help ensure the confidentiality and integrity of the data passing over the public network.	Inspected the VPN authentication configurations to determine that a VPN was utilized by personnel for remote access to help ensure the confidentiality and integrity of the data passing over the public network.	No exceptions noted.
6.10	VPN administrative privileges are restricted to network administrative personnel.	Inquired of the Information Security Officer, regarding VPN administrative access to determine that VPN administrative privileges were restricted to network administrative personnel.	No exceptions noted.
		Inspected the VPN administrative user access listing to determine that VPN administrative privileges were restricted to network administrative personnel.	No exceptions noted.
6.11	VPN users are authenticated via MFA prior to being granted remote access to the system.	Inquired of the Information Security Officer, regarding VPN authentication to determine that VPN users were authenticated via MFA prior to being granted remote access to the system.	No exceptions noted.
		Observed the authentication of a user to the VPN to determine that VPN users were authenticated via MFA prior to being granted remote access to the system.	No exceptions noted.

CONTROL AREA 6 **DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that data maintains its integrity and security as it is transmitted between third-parties and the service organization.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the VPN authentication configurations to determine that VPN users were authenticated via MFA prior to being granted remote access to the system.	No exceptions noted.
6.12	An encrypted wireless network is utilized by personnel to help ensure the confidentiality and integrity of the data accessed within the corporate office.	Inspected the wireless network configuration to determine that an encrypted wireless network was utilized by personnel to help ensure the confidentiality and integrity of the data accessed within the corporate office.	No exceptions noted.

CONTROL AREA 7 **VALUATION VALIDATION PROCEDURES**

Control Objective Specified by the Service Organization: Control provides reasonable assurance that valuations and calculations of transactions are verified periodically and in the testing process of the application development change process. An automatic data matching process is utilized to provide reasonable assurance that the calculation of payment amounts is accurate.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.1	Model governance procedures are documented to establish periodic organizational standards to validate application generated valuations.	Inspected the model governance procedures to determine that model governance procedures were documented to establish periodic organizational standards to validate application generated valuations.	No exceptions noted.
7.2	Market data for interest rates is recorded in DerivativeEDGE by the Derivative Path Operations team daily.	Inspected the save closing quotes actions for a sample of days to determine that market data for interest rates was recorded in DerivativeEDGE by the Derivative Path Operations team daily.	No exceptions noted.
7.3	Market data for foreign exchange is recorded in DerivativeEDGE by the Derivative Path Operations team daily.	Inspected the save closing quotes actions for a sample of days to determine that market data for foreign exchange was recorded in DerivativeEDGE by the Derivative Path Operations team daily.	No exceptions noted.
7.4	Effective January 1, 2024, Market data for commodities is recorded in DerivativeEDGE by the Derivative Path Operations team daily.	Inspected the commodity settlements for a sample of days to determine that market data for commodities was recorded in DerivativeEDGE by the Derivative Path Operations team daily.	No exceptions noted.
7.5	Effective January 1, 2024, Commodity settlements require a revaluation of the entire commodity portfolio each commodity business day to calculate the current value of each transaction.	Inspected the commodity market to market report for a sample of days to determine that commodity settlements required a revaluation of the entire commodity portfolio each commodity business day to calculate the current value of each transaction.	No exceptions noted.
7.6	A revaluation of the entire portfolio is performed daily to calculate the current value of each transaction.	Inspected the closing curves for a sample of days to determine that a revaluation of the entire portfolio was performed daily to calculate the current value of each transaction.	No exceptions noted.

CONTROL AREA 7 **VALUATION VALIDATION PROCEDURES**

Control Objective Specified by the Service Organization: Control provides reasonable assurance that valuations and calculations of transactions are verified periodically and in the testing process of the application development change process. An automatic data matching process is utilized to provide reasonable assurance that the calculation of payment amounts is accurate.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.7	A quarterly comparison is performed between the NPV values produced by DerivativeEDGE and a third-party analytics provider for a set of trades. Material differences are investigated, and corrective action is taken.	Inspected the quarterly valuation summary for a sample of quarters to determine that a quarterly comparison was conducted between the NPV values produced by DerivativeEDGE and a third-party analytics provider for a set of trades, and that material differences were investigated, and corrective action was taken.	No exceptions noted.
7.8	Prior to application changes migrated to production, DerivativeEDGE Mark to Market reports in the test environment are compared to the values of the DerivativeEDGE Mark to Market in production for each trade.	Inspected the supporting change ticket for a sample of application changes to determine that prior to application changes migrated to production, DerivativeEDGE Mark to Market reports in the test environment were compared to the values of the DerivativeEDGE Mark to Market in production for each trade.	No exceptions noted.
7.9	Prior to application changes migrated to production, a DerivativeEDGE reset process in the test environment is compared to the DerivativeEDGE reset values in production to evaluate the calculations of Mark to Market values.	Inspected the supporting change ticket for a sample of application changes to determine that prior to application changes migrated to production, a DerivativeEDGE reset process in the test environment was compared to the DerivativeEDGE reset values in production to evaluate the calculations of Mark to Market values.	No exceptions noted.
7.10	DerivativeEDGE utilizes an automatic data matching process to ensure that the reset notices match the dealer notices and that payment amounts being calculated are accurate.	Inspected the DerivativeEDGE Automatch process, a reset notice, and a dealer notice to determine that DerivativeEDGE utilized an automatic data matching process to ensure that the reset notices matched the dealer notices and that payment amounts being calculated were accurate.	No exceptions noted.
7.11	Material model changes will be documented, communicated to client, and an impact analysis will be performed.	Inspected the supporting ticket for a sample of material model changes to determine that material model changes were documented, communicated to client, and an impact analysis was performed.	No exceptions noted.