Clearwater Analytics, LLC

Report on Description of System and Controls for Financial Reporting Services

For the Period January 1, 2017 through December 31, 2017

The information contained herein including concepts, strategies, system specifications, designs, plans, drawings, or process techniques is considered Confidential Information and is covered under the Contractual Agreement and/or Confidentiality Agreement.

©Clearwater Analytics, LLC 2016

Table of Contents

THE ORGANIZATION 3

SECTION ONE—*Independent Service Auditor's Report* 4

SECTION TWO—*Management Assertion* 8

SECTION THREE—*Description of System*

Control Environment 11
- Risk Assessment 13
- Monitoring 14

Information and Communication 14
- Investment Analytics and Reporting 14
- General Computer Controls 18
- Communication 22

Subservice Organization 22
Client Control Considerations 23

SECTION FOUR—*Control Objectives, Related Controls, and Tests of Operating Effectiveness*

Purpose and Objectives of the Independent Service Auditor's Examination 26
Control Objectives 28
Ethical Behavior 29
Security Processing, Valuation, and Customer Reporting 30
Statutory Reporting 39
Information Technology 41

APPENDIX

Client Defined Accounting Assumptions 55
Reconciliation Process Chart 63

©Clearwater Analytics, LLC 2016

The Organization

Clearwater Analytics, LLC

Clearwater Analytics, LLC provides web-based, fully integrated accounting, compliance, performance, and risk reporting solutions for corporate investors, institutional investors, and investment managers. Highlights and benefits of the Clearwater Analytics solution include:

- Single, comprehensive view of investment-related information across multiple managers, custodians, portals, etc.
- Daily investment information provided for all interested parties; including treasury, accounting, management, tax, audit, and financial reporting departments.
- Complete, reliable outsourced accounting solutions using consistent, audited accounting assumptions.
- Scalable reporting based on the client's fiscal cycle-close schedule.
- Timely calculations and reporting.
- Web-based access to analytics platform (no installed software).
- Independent verification and reconciliation of investment data.

Clearwater provides its investment reporting platform under its own brand or as a private label for custody banks, investment managers, and other financial institutions.

©Clearwater Analytics, LLC 2016

EideBailly®

CPAs & BUSINESS ADVISORS

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls

To the Members of Clearwater Analytics, LLC
777 West Main Street, Suite 900
Boise, Idaho 83702

Scope

We have examined Clearwater Analytics, LLC's description of its Financial Reporting Services (System) for reporting user entities' transactions throughout the period January 1, 2017, to December 31, 2017, (description) and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in Clearwater Analytics, LLC Assertion (assertion). The controls and control objectives included in the description are those that management of Clearwater Analytics, LLC believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Financial Reporting Services that are not likely to be relevant to user entities' internal control over financial reporting.

The information included in The Appendix A "Documents sent to onboarding clients containing a comprehensive list of assumptions that can be applied to the accounting platform" and The Appendix B "Illustration of Clearwater's reconciliation process" is presented by management of Clearwater Analytics, LLC to provide additional information and is not a part of Clearwater Analytics, LLC's description of its Financial Reporting Services system made available to user entities during the period January 1, 2017, to December 31, 2017. Information about Clearwater Analytics, LLC's onboarding and reconciliation process has not been subjected to procedures applied in the examination of the description of the Financial Reporting Services system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the Financial Reporting Services system, and accordingly, we express no opinion on it.

Clearwater Analytics, LLC uses multiple organizations to obtain market prices in support of its operations. Clearwater Analytics, LLC also uses co-location facilities to house the systems critical applications. The description includes only the control objectives and related controls of Clearwater Analytics, LLC and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by Clearwater Analytics, LLC can be achieved only if complementary subservice organizations controls assumed in the design of Clearwater Analytics, LLC's controls are suitably designed and operating effectively, along with the related controls at Clearwater Analytics, LLC. 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 organizations controls.

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 Clearwater Analytics, LLC's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In Section Two of this Report, Clearwater Analytics, LLC has provided an 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. Clearwater Analytics, LLC is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives 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 January 1, 2017, to December 31, 2017. 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 the controls to achieve the related 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 considered necessary to provide reasonable assurance that the related control objectives stated in the description were achieved and evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion in Section Two of this report.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the

presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are presented in the section of our report titled "Control Objectives, Related Controls, and Tests of Operating Effectiveness".

Opinion

In our opinion, in all material respects, based on the criteria described in Clearwater Analytics, LLC's assertion in Section Two:

a. The description fairly presents the Financial Reporting Services system that was designed and implemented throughout the period January 1, 2017, to December 31, 2017.
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 January 1, 2017, to December 31, 2017, and subservice organizations and user entities applied the complementary controls assumed in the design of Clearwater Analytics, LLC's controls throughout the period January 1, 2017, to December 31, 2017.
c. The controls we tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period January 1, 2017, to December 31, 2017, if complementary subservice organizations and user entity controls assumed in the design of Clearwater Analytics, LLC's controls operated effectively throughout the period January 1, 2017, to December 31, 2017.

Restricted Use

This report, including the description of tests of controls and results thereof on Section Four is intended solely for the information and use of management of Clearwater Analytics, LLC, user entities of Clearwater Analytics, LLC's Financial Reporting Services system during some or all of the period January 1, 2017, to December 31, 2017, and their independent auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have 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.

Eide Bailly LLP

Minneapolis, Minnesota
January 12, 2018

clearwater

Section Two

Management Assertion

© Clearwater Analytics, LLC 2016

Management Assertion

We have prepared the description of the financial reporting services of Clearwater Analytics, LLC and its system (the System) for reporting user entities' transactions throughout the period January 1, 2017 to December 31, 2017 (description), for user entities of the system during some or all of the period of January 1, 2017 to December 31, 2017 , and their auditors who audit and report on such user entities' financial statements or internal controls over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities, or user entities themselves, when assessing the risks of material misstatements of user entities' financial statements.

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 Clearwater Analytics, LLC's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

Clearwater Analytics, LLC uses multiple organizations to obtain market prices in support of its operations. Clearwater Analytics, LLC also uses co-location facilities to house the systems critical application. The description includes only the control objectives and related controls of Clearwater Analytics, LLC and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organizations controls assumed in the design of Clearwater Analytics LLC controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organizations.

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

1. The description fairly presents the System made available to user entities during some or all of the period January 1, 2017 to December 31, 2017 for reporting user entities' transactions. The criteria used in making this assertion were that the description:
    a. Presents how the System made available to user entities was designed and implemented to report on relevant user entity transactions, including, if applicable:
        i. The types of services provided including, as appropriate, the classes of transactions reported.
        ii. The procedures, within both automated and manual systems, by which services are provided, including as appropriate, procedures by which transactions are accounted for and transferred to reports and other information prepared for user entities of the System.
        iii. The information used in the performance of the procedures, including, if applicable, related accounting records, when electronic or manual, and supporting information, involved in reporting transactions; this includes the correction of incorrect information and how information is transferred to reports and other information prepared for user entities.
        iv. How the System captures and addresses significant events and conditions, other than transactions.
        v. The process used to prepare reports and other information for user entities.
        vi. Services performed by a subservice organization, if any, including whether the carve-out or the inclusive method has been used in relation to them.
        vii. The specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls.
        viii. Other aspects of our control environment, risk assessment process, information and communication systems (including the related business

©Clearwater Analytics, LLC 2016

processes), control activities, and monitoring activities that are relevant to the service provided.

b. Includes relevant details of changes to the System during the period covered by the description.

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

2. The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period January 1, 2017 to December 31, 2017 to achieve those control objectives if subservice organizations and user entities or user entities applied the complementary controls assumed in the design of Clearwater Analytics, LLC's controls throughout the period of January 1, 2017 to December 31, 2017. The criteria we used in making this assertion were:

   a. The risks that threaten the achievement of the control objectives stated in the description have been identified by management of Clearwater Analytics LLC;

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

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

David Boren
Chief Executive Officer
1/12/2017

Scott Erickson
Chief Operating Officer
1/12/2017

James Price
Chief Technology Officer
1/12/2017

Ryan Arave
VP of Finance and Accounting
1/12/2017

©Clearwater Analytics, LLC 2016

clearwater

Section Three

Description of System

©Clearwater Analytics, LLC 2016

SCOPE OF THIS REPORT

This description of controls highlights the services provided by Clearwater Analytics, LLC (the Company) and focuses on key control objectives as they may be relevant to the internal control environment of Clearwater clients. Clearwater Analytics, LLC uses a co-location facility to house the System's critical applications. This description includes only the controls and related control objectives of Clearwater Analytics, LLC. This description does not include the control objectives and related controls of the co-location facility. This report, when coupled with an understanding of the internal controls in place at user organizations, is intended to assist in the assessment of the internal controls surrounding financial information generated by the Company. It is designed to provide information for use by clients and their independent accountants who audit the financial statements of an entity that used the Company as a service organization. The document was prepared using the following categories from the COSO Framework:

- Control Environment
- Risk Assessment
- Monitoring
- Information and Communication
- Control Activities

CONTROL ENVIRONMENT

The Company's control environment reflects the position taken by management, its Principals, and others concerning the importance of internal controls and the emphasis given to implement and monitor its policies, procedures, methods, and organizational structure. An entity's control environment represents the collective effect of various factors on establishing and enhancing the effectiveness of specific control activities (outlined within Section Three). Consistent with the guidance contained in the AICPA SSAE No. 18, such factors include the following:

- Integrity and ethical values
- Commitment to competence
- Board of Directors
- Management's philosophy and operating style
- Organizational structure
- Human Resources ("HR") policies and practices

Integrity and Ethical Values

Management seeks to convey the message that integrity and ethical values cannot be compromised, and it seeks to continually demonstrate, through words and actions, a commitment to high ethical standards, as highlighted below:

- The Company's Code of Ethics establishes parameters regarding the way in which employees of the Company are to perform their duties. Every employee is expected to remain informed about and to comply with the Code of Ethics and regulatory and legal requirements. These principles are reviewed and communicated at new associate orientation. Additionally, upon implementation of any updates to this policy, all employees are required to review and sign the revised document.
- The Code of Ethics addresses a variety of business and personal conduct issues and sets forth the acceptable conduct required of all employees, including the following:
  - Compliance with laws, rules, and regulations
  - Individual responsibilities over the protection of Company assets, including intellectual property
  - Communication and confidentiality standards
- Additional procedures include:
  - Executives ("management"), supervisors, and HR representatives are responsive in taking appropriate disciplinary action when the Company's policies and procedures are violated.
  - Management communicates formally, on at least an annual basis, its overall commitment to integrity and ethical values in all business relationships. The Company switched this communication from quarterly to annual in the first quarter of 2017.

©Clearwater Analytics, LLC 2016

Commitment to Competence

Management seeks to specify the level of competence needed for particular jobs and translate the desired levels of competence into requisite knowledge and skills. Relevant procedures include:

- Several hiring assessment tests exist to assist management in determining the qualifications and aptitude of personnel.
- Various levels of Company personnel are involved in the interview process to ensure the desired level of competence exists.
- All new employees are subject to a third-party criminal background check.
- Internal background checks can include review of personal references and contact with prior employers.

Board of Directors

The control environment and "tone at the top" are influenced significantly by the entity's Board of Directors. Factors include the Board's experience and stature of its members, extent of its involvement, and scrutiny of activities and the appropriateness of its actions. The Company has the following procedures in place to address this element of the control environment:

1. An executive committee is comprised of Chief Executive Office, Chief Financial Officer, and Chief Operating Officer.

2. The Board meets at least quarterly to review financial and operational results with formalized minutes generated at each of these meetings.

Management's Philosophy and Operating Style

The philosophy and operating styles of management normally have a pervasive effect on an entity. This philosophy and related style are evident as follows:

- A relatively simple organizational structure exists to facilitate communication between the executive management and personnel.
- Frequent meetings are held by management to communicate the Company's risk tolerance policies, including the proper approval channels upon executing transactions involving risk.
- Business risks associated with market changes, competition, and other outside forces are considered in strategy sessions held weekly and/or monthly.

The Company has designated a Chief Compliance Officer who is responsible for:

- Enforcing the Code of Ethics, Employee Non-Disclosure Agreement ("NDA"), and personal trading policy for Company employees.
- Defining and enforcing the segregation of duties.
- Developing and updating procedures to ensure:
  - Completeness of records
  - Appropriate procedures for limiting and addressing the potential for conflicts of interest
  - Adequate employee training
  - Appropriate handling of employee or client complaints

In an effort to ensure that the Company and its employees are functioning in compliance with company-wide policies, the Chief Compliance Officer:

- Explains Company processes and procedures to staff.
- Provides regular updates to reflect changes in applicable legislation and Company operations or procedures to staff.
- Requires staff to acknowledge in writing that they have read and understood the Company policies and procedures.

Organizational Structure

The organizational structure has been sufficiently designed to adequately monitor the enterprise's activities, encourage the free flow of information, and ensure the appropriate segregation of incompatible duties. The Company has the following procedures in place:

- Limited layers of management exist between executive management and other personnel. This is an advantage relative to the flow of information. An "open door" policy exists and executives receive timely feedback from employees.

©Clearwater Analytics, LLC 2016

- Management has been historically conservative in expanding the organizational structure. Changes are reviewed at the highest level and are made when deemed necessary.
- Given the size of the Company and the number of personnel in the corporate office, sufficient supervisory and management staff exists in the key areas. An assessment on staffing needs is performed periodically.

HR Policies and Practices

HR policies are central to recruiting and retaining competent people to enable the Company's goals and objectives to be carried out.

- Policies and procedures exist for key HR functions.
- Hiring standards exist for all employees (see *Commitment to Competence* for additional details).
- Any departure from established policies and procedures is dealt with by the executive management team. Management balances the needs of associates with the goals and responsibilities of the Company. Where possible, counselling is performed with employees, and when certain lines have been crossed, terminations occur to sever the employment relationship in order to protect other employees, clients, the Company, and its assets.
- As part of a formalized HR process, communication is initiated to notify appropriate departments of status changes and terminations. The Company ensures employees' access to computer systems is removed upon termination.
- Personnel are made aware of their job responsibilities and Company's expectations and are evaluated on their performance at least annually.
- HR maintains a signed NDA on file for each employee.
- HR maintains a signed Code of Ethics on file for each employee (see *Integrity and Ethical Values* above for additional details).
- The Company has established a privacy policy to govern the actions of the Company, its employees, and its representatives as they relate to the collection, use, retention, and disclosure of client information. Each Company employee and representative must abide by the Company's commitment to privacy in the handling of client information.
- The Company adheres to the following principles when dealing with client information:
  - Protection of privacy and confidentiality
  - Maintenance of accurate records
  - Compliance with applicable laws and regulations in jurisdictions where the Company transacts business

Risk Assessment

To identify and manage risk, management has placed into operation entity-wide and activity-level controls. The risk assessment process also considers external and internal factors that could impact achievement of the Company's objectives, analyzes the risks, and provides a basis for managing risks. Economic, industry, and regulatory environments change and entities' activities evolve. The Company has established the following risk assessment procedures:

- Executive management provides the direction on an overall entity-level strategic plan. The plan is used as a basis for judging departmental achievement. The overall results are reviewed formally by executive management on at least a quarterly basis.
- Frequent (e.g., weekly, monthly, etc.) meetings are held between the executive team and personnel to review how the Company manages risk.
- All significant capital expenditures receive approval from the VP of Finance and Accounting.
- Executive management monitors monthly expense reports and approves all staffing expenditures.
- Regular communication occurs between executive management and accounting personnel. An accounting team in Client Services communicates to executive management any significant changes that may have an impact on accounting practices in a timely manner. In the event that the change has an effect on systems, the accounting team meets with the Development Committee to obtain approval on any significant changes. The

©Clearwater Analytics, LLC 2016

Committee reviews and prioritizes all proposed system changes.

- Business risks associated with market changes, competition, and other outside forces are considered in strategy sessions held weekly and/or monthly.
- Insurance is maintained by the Company to provide coverage against major risks. Coverage provided by insurance companies is reviewed by the Principals and is maintained at levels that they believe is reasonable given the size and scope of the Company's operations.

Monitoring

Management monitors controls to consider whether they are operating as intended and that the controls are modified appropriately for changes in condition. The Company has the following monitoring procedures in place:

- Monitoring activities are performed by the Company's internal audit group and by each department to continually assess the quality of internal controls over time.
- Necessary corrective actions are taken as required to correct deviations from policies and procedures.
- Employee control activities and related adherence to policies and procedures are reviewed through ongoing monitoring procedures and/or separate independent evaluations.
- Entity-level (e.g., Code of Ethics, etc.) and process-level controls (e.g., reconciliations, etc.) are reviewed for reasonableness and monitoring controls (e.g., review of financial reports by executive management) are in place to detect and act when controls are circumvented.
- Principals engage independent consultants to review and evaluate key entity-level and process-level controls.

Executive management proactively responds to external auditors, independent consultants, and/or client auditors and where applicable, implements recommendations as a means to strengthen internal controls.

INFORMATION AND COMMUNICATION

Investment Analytics and Reporting

Reconciliation Procedures

Both the automated system and Client Services personnel perform daily reconciliation and other validation procedures over the following:

Daily Account Reconciliation. Reconciliation takes place between the client's custodian[1] data and the Company's internal reporting system. The company predicts principal and income, cash and positions, amortization and market value. Any differences between custody data and company predictions are identified through hundreds of automated and manual comparisons. Extracts of custodian data sources are systematically downloaded and aligned with Clearwater data. Client Services personnel utilize a systematic report to reconcile and resolve identified discrepancies around. Accounts are reviewed on a daily basis by Client Services personnel to ensure the systematic extracts, downloads, and related reconciliations are performed properly. Client Services personnel perform regular follow-up with the appropriate internal and external parties until issues are resolved. See Appendix B for an illustration of the daily reconciliation process.

Custody Accounting Information. These reconciliation procedures take place between the Company's calculated figures – including total accrued (when there is no third-party data available) and market value – and custodian data where available. A systematic comparison is performed between custodian and Clearwater data. Systematic reconciliations are reviewed by Client Services personnel and any identified discrepancies are resolved.

Tri-party. These reconciliation procedures take place between the Company's calculated figures, custody data, and data from the investment manager's trading system. A systematic comparison is performed between the three data sources. Systematic reconciliations are reviewed by Client Services and any discrepancies are resolved.

[1] The term "custodian" throughout this document refers to the data source from which Clearwater receives core transaction and portfolio holding information. These data sources include client custody banks, safekeeping institutions, brokerage accounts, internal systems, or other sources.

©Clearwater Analytics, LLC 2016

Task List. An automated program is run by the Company to identify potential issues with the reconciliation process. Unusual items (e.g., zero coupons, zero yields) are noted as exceptions and these items are reviewed and resolved by Client Services or Data Team personnel.

Pricing Tasks. On a daily basis, third-party prices are systematically downloaded, and pricing errors resulting from third parties' downloads are monitored and resolved in a timely manner. Daily, prices obtained from third party sources are systematically compared to prices assigned to selected client accounts. Daily tasks are run by the pricing team and Client Services to check for large pricing changes. Any identified issues are resolved with the pricing source. Clearwater Analytics, LLC no longer monitors stale pricing daily. Clearwater performs a stale pricing check every thirty days for Standard and Poors and Thomson Reuters and notifies the pricing provider of any stale prices identified.

Compliance. The Company also has an automated system that identifies activity that is out of compliance with client guidelines (see additional details and controls within the Compliance section below). Client Services personnel review potential new violations and new contributors to existing violations daily for reasonableness and/or recalculation. Accounts aren't marked as "reconciled" until after the compliance review is performed.

Security Pricing Method

Hierarchical Pricing. Each security's price comes from the highest-priority pricing source possible within each client's selected pricing source hierarchy. Remaining pricing sources are used for price comparisons. The default hierarchical order starts with any client-provided pricing overrides. Calculated pricing on select security types is then applied. S&P Capital IQ pricing is then assigned to the remaining securities, with Account Source pricing being the final source. The pricing hierarchy is customizable, can be applied at the individual account level, and can include any of the pricing sources described below.

- **Pricing Overrides**. Some clients hold distressed, illiquid, or alternative investment types and choose to provide Clearwater with prices for these securities. Pricing overrides can be provided periodically, and these override values will remain static until the next pricing update is provided. Pricing overrides will be used in favor of any sources or calculated prices.

- **Calculated Prices**. Securities with short maturities and infrequent secondary market trades are typically priced via mathematical calculations. For example, in the case of a certain issue of commercial paper (CP), Clearwater will accrete from purchase price at trade date to face value at maturity to calculate a daily price. In the event that another transaction is observed for the same security within the account, the price on that subsequent transaction clearly reflects the market price on that day and Clearwater will adjust the price in the account to the observed transaction price and follow a revised accretion schedule to determine the daily price. Calculated Pricing applies to the following security types:

  - CP and Certificates of Deposit (CD) – market price follows amortization/ accretion schedule from purchase to maturity
  - Repurchase Agreements and Auction Rate Securities – priced at par
  - Money Market Funds that are not institutional prime funds – priced at $1

- **S&P Capital IQ**. S&P Capital IQ is a business line of The McGraw-Hill Companies; S&P Capital IQ's Valuation Service provides prices for global equity and fixed-income securities and hard-to-price instruments using both market approach and model valuation methods. Its coverage includes global equity, corporate, government, mortgage-backed, asset-backed, agency, and U.S. Municipal securities. Security types include bills, bonds, debentures, derivatives, equities, mortgages, and medium-term notes. S&P Capital IQ offers visibility to the trade data used to create its valuations.

- **Thomson Reuters.** Thomson Reuters, a business unit of Thomson Reuters Corporation, provides evaluated prices on over 2.4 million securities. Coverage includes sovereign debt, corporate debt, convertible securities, bank debt, mortgage backed securities, asset backed securities, municipal securities, derivatives, and structured notes. Pricing methodologies incorporate bond

©Clearwater Analytics, LLC 2016

terms and conditions, current performance data, proprietary pricing models, real-time quotes from contributing dealers, trade prices, and other market data.

- **iMoneyNet.** Provides prices for institutional prime money market funds. iMoneyNet is part of the Business Intelligence Division of Informa PLC, a leading provider of money market mutual fund and enhanced cash information.

- **Interactive Data.** Interactive Data Corporation, a portion of ICE Data Services, provides evaluated prices representing approximately 135 countries and over 50 different currencies for approximately 2.7 million financial instruments. Interactive data is made available for an additional fee and can be selected for daily or monthly use. If used monthly, the pricing hierarchy will incorporate the additional source at month end.

- **IHS Markit.** IHS Markit is a world leader in critical information for major industries and markets, including pricing data for specific security types such as bank loans that are not as well supported by other 3rd party pricing sources. Markit Pricing Data is available for bank loan pricing for an additional fee.

- **NAIC.** NAIC Automated Valuation Service pricing is available to insurance clients. The AVS provides market values that regulators will use in their examination process. Insurance clients who choose to use AVS pricing will need to execute an independent contract with the NAIC and designate Clearwater as a third-party administrator.

- **Account Source.** Account Source pricing is the pricing received in the daily feed sent to Clearwater by the client's custodian or other financial institution.

Security Characteristics

At least daily, the Company uploads dynamic security characteristic information (e.g., credit rating, factor, variable-rate, etc.) into the system using several independent security characteristic sources. Static security characteristics (e.g., day count, first coupon, etc.) are uploaded into the system upon initial security creation using independent security characteristic sources.

In cases where there are securities without readily discernible and independent pricing or characteristics (e.g., the structured product markets), the Company uses its best efforts to ascertain accurate security information. Lack of independent and accurate sources for security pricing and characteristics may result in imprecise portfolio accounting, risk, compliance, and performance information.

Corporate Actions

The Company is notified of daily actions through the portfolio data feed from the custodian. Corporate actions are updated via the daily security characteristic upload process (described above under *Security Characteristics).* The Company may confirm corporate actions via various independent sources and also through the daily reconciliation process performed by Client Services personnel.

Accounting

Overview. The Accounting platform is designed to provide the client with a suite of daily accounting reports and tools to account for the portfolio timely and accurately. The accounting platform provides various reports and tools, including statutory ("STAT") reports, balance sheet, income statement, cash flow statement, impairment report, transactions report, cash flow forecast, tax lots report, automated General Ledger Upload, NAIC Upload (for STAT clients), and Cycle-Close Packet.

Accounting Calculations and Assumptions. The foundation of the accounting platform is the set of assumptions that are applied to the data to calculate and report the accounting information. Upon client inception, these assumptions are input into the reporting platform according to the client's selection. See Appendix A for the document sent to onboarding clients containing a comprehensive list of assumptions that can be applied to the accounting platform.

Accounting Reporting. The Accounting platform provides accounting information at the aggregate financial-statement level and provides drill-down capabilities into the individual securities that comprise the aggregate financial information. Through the use of the accounting assumptions, security characteristics, and pricing process discussed previously in this report, the processed and

©Clearwater Analytics, LLC 2016

calculated data is mapped to the reports in the Accounting platform that are used for financial statement-generation purposes.

Access to Enter Writedowns. Clients may write down securities they have deemed other-than-temporarily impaired, by either requesting Client Services to make the change or entering the writedown themselves. The client's users with access to this function must be authorized by the client.

Cycle-Close Packets and General Ledger Upload. To assist organizations close their books in an accurate and timely manner, the Company can provide the following functionality:

- **Legacy System Cycle-Close Packets**. The Company produces cycle-close packets which can provide several reports from the accounting module, including income statement, balance sheet, statement of cash flows, income detail, balance sheet detail, and more.
- **General Ledger Upload**. The Company provides a cycle-close general ledger file according to the client's GL codes and in a format the client has selected to best fit their journal entry creation needs. Supporting documentation on the entries is also provided.
- **NAIC Upload**. The Company provides the schedules required by the National Association of Insurance Commissioners (NAIC) for Quarterly and Annual filings. These schedules are generated in the format accepted by NAIC-approved Annual Filing Software providers for direct upload.

The automated System performs checks to ensure that the data being reported is accurate and internally consistent. If discrepancies are identified, they are investigated and corrected by Client Services personnel.

The ability to modify and implement changes to the source code driving the report generation process, as well as the ability to access the application database, is limited to appropriate and authorized members of the development team.

The System uses the most current data available to calculate cycle-close information. Adjustments needed to previously-locked down periods are systematically identified by the accounting values generator and entered in the current period. They are labeled as Adjusting Entries in the GL report files.

Compliance

The Company's compliance platform provides access to portfolio compliance status, automated change in compliance notification, and day-by-day compliance history by individual investment mandate.

The Client Services team obtains a copy of the client's investment policy to implement rules in the System to monitor compliance with the client's policy. Client Services personnel convene with the client to discuss the investment policy mandate and benchmark, including any specific mandate parameters that may be narrower than the stated investment policy parameters. The portfolio investment policy parameters are recorded in the automated Clearwater Investment Guidelines compliance-monitoring template. The automated compliance system monitors overall trading activity and market movements and identifies portfolio compliance violations (see *Security Characteristics* for additional details).

Client investment guideline changes (e.g., adjustment to the percentage of portfolio that can be invested in a specific security) are made through the single mode of access for all client users, the web-based client interface. Access to edit client investment guidelines is available only to client users designated by the primary client contact. A secure log file is maintained to track user activity. The log stores the user, guideline parameter change (guideline affected and old and new values), and time of occurrence.

Calculations and/or code associated with the compliance platform are sufficiently tested and approved before being implemented into production. The ability to make modifications is strictly limited to appropriate members of the application development team.

In the case of a compliance violation, a non-compliant flag will appear on the website and the compliance email functionality can be set to notify the client of the specific offending account and violation. The Violations section of the compliance platform records the details of each violation, noting the investment policy guideline broken and the offending securities.

©Clearwater Analytics, LLC 2016

Compliance violations are recorded daily for audit purposes and are available by date or rule for up to two years in Compliance History. Compliance history modification rights are limited to Development System Administrators. Compliance History records violations as part of the reconciliation process, and the automatic email notification is sent to the client when all accounts a user has access to are reconciled and checked for compliance. Client Services personnel review compliance violations as part of the daily reconciliation and validation process.

Access to Edit Compliance Guidelines. Client (external) access to edit Compliance Guideline parameters is determined by the client through formal documentation as part of the account administration process. Company (internal) access to edit client Investment Guidelines is restricted to the Client Services Team and Systems Development Manager. A secure log file is maintained in the system to track Investment Guideline parameter changes (e.g., change made, external user, and time of occurrence).

Account Administration

The Client Services team is responsible for guiding a new client through a comprehensive documentation process entitled the Implementation Process. When the Client Services team initiates a new account, a Company representative follows processes outlined in the Implementation Process document. The Implementation Process document outlines the required documentation, portfolio accounting and compliance assumptions, and timelines.

The Client Services team transmits information received from the client about the portfolio custodian, fiscal calendar, authorized users, investment policy, reporting requirements, and reconciliation tolerances to the relevant internal parties.

For account closures, the Client Services personnel receive written notification from the client to close an account and ensure execution of the client direction and cease reporting.

General Computer Controls

General computer controls establish the control environment in which application systems are developed and operated. Therefore, the general computer control environment has an impact on the effectiveness of controls in application systems, including the reporting platform provided by Clearwater.

The following areas describe the general controls supporting the reporting platform:

- *Application System Development and Change Management*
- *Logical Access*
- *Physical Access*
- *Environmental Controls*
- *Data Backup and Recovery*
- *Network Security*

Application System Development and Change Management

The application development group is responsible for the development and maintenance activities supporting the Clearwater application. A Systems Development Lifecycle ("SDLC") has been established and is leveraged by development teams based on the size and scope of a particular project. Product Management and Development leadership are responsible for assigning development and maintenance projects to staff developers or project teams with their associated tasks, objectives, and due dates. Meetings among the development team are held regularly to ensure project deadlines are being met and that development results are in line with management's expectations. Regular meetings are also held between development leadership and business management to set development priorities and ensure development efforts are aligned with management's goals and objectives.

The phases of the development approach are described at a high level below:

1. *Blueprint*: The project team defines the business and technology requirements for the application. The team examines the current business process and identifies opportunities for improvement. These requirements are translated into functional specifications with assistance and approval from the business sponsors.
2. *Design*: The requirements and specifications are interpreted into the technical infrastructure and application designs.

©Clearwater Analytics, LLC 2016

3. *Development*: The application software components are programmed, unit tested, system tested, and integration tested.
4. *Implementation*: The business functionality is tested, accepted, and approved for production use.
5. *Testing*: There are multiple points of testing during the development and implementation stages, including test plans; test cases; problem prioritization, tracking, and resolution; and re-testing.
6. *Deployment*: The application is deployed, and the development team assesses the results of the project.

Client Development Requests. In addition to internally driven changes initiated by the Company, the Development team also works on modifications requested by its clients. For significant client-driven changes, the Development team will work closely with the requesting client to establish a statement of work detailing the specific requirements and scope of the change. Before development, the team requires approvals from both the client and management affirming the accuracy of the requirements. Clients are often included in the end-user testing before the change is introduced into production.

Source Code Maintenance and Restrictions. To create and maintain code, developers make use of a code repository, which tracks all changes to source code files, including what change was made, when the change was made, and who made the change. Only authorized developers have access to the code repository. Once the code is committed to the repository, the system automatically compiles both the source code and the unit tests code into binaries, executes the unit tests, and runs static code analysis. If the compilation, unit testing, and analysis are successful, the system deploys the binaries to the testing environment for additional automated testing.

Quality Assurance. All projects require sufficient oversight and testing activities to ensure the quality of the development effort. As part of these quality assurance ("QA") activities, the Company utilizes a testing platform where all newly developed or modified code is reviewed and tested.

The QA stage of development also includes the development and/or preparation of the necessary test scripts. Key application security elements are also tested. Integrated code undergoes testing to ensure proper functionality and to identify any unexpected differences in calculations.

Once code passes these tests, it is identified as being a candidate for release. It is then moved into the next test environment. Here the testing is on the functionality of new features in a production-like environment. If this testing is successful, the code is tagged for release.

The code is then moved into the staging environment, where deployment testing occurs. Deployment tests are standardized, mostly manual tests exercising a number of usage scenarios with the new, integrated code. If these final tests pass, the code is ready for deployment.

Deployment. Compiled binaries are only versioned when all required tests pass. Only versioned binaries can be deployed. Versioned binaries cannot be modified. Only a limited number of staff are authorized to deploy versioned binaries to the production environment and no developers have this ability.

Post-Deployment Monitoring. In addition to the testing of code in development, QA also tests code in production to ensure production code is functioning as expected and client data passes consistency checks. Other Clearwater teams perform multiple daily processes to ensure the Clearwater application calculates and reports information accurately and completely. Any problems or issues are reported immediately to the Development team for correction.

Request Tracking. To address feature enhancement requests and identify bugs associated with the application, Clearwater maintains a tracking tool where all issues and requests are recorded and prioritized. The team leads review all reported issues, determine which need development involvement to address, and assign a developer to implement a fix. Once the issue has been addressed, the tracking tool is updated accordingly.

Emergency Changes. Emergency changes (also known as "hot fixes") must be compiled into binaries, unit tested, analyzed, QA tested, and versioned before they can be deployed by an authorized deployer. The QA testing for hot fixes focuses on the functionality of the fix, and the code undergoes integration testing in all future releases of code.

©Clearwater Analytics, LLC 2016

The Version section discusses the security of the highest version of the TLS protocol your client supports. (Formerly, TLS was known as "SSL".) TLS **1.2** is latest version of TLS

Application Security Te ce
of se
appli
to en
secur
script
validated and range checked.

How AIG is m password cha is the Passwo AIG Policy

Who is the primary client contact from AIG : HR?

Logical Access

Application Authentication. The single mode of interactive access for all client users is the web-based interface to the system. Access to the system through this interface is obtained by authenticating to the site using a username and password unique to each user. All transmissions between client and server are encrypted ing TLS, including the transmission of the session during the user's session.

Is AIG re

Following a successful log-in, continuous authentication is performed using the us s ID and unique session ID for each page requeste during that session. A session begins when the er logs into the system and ends when the user logs out, by either explicitly using the logout link or by closing the browser, or when the session times out. The only way to obtain a valid session ID provide a valid username and password at the point of log-in to the site. Without a valid user/session ID combination, a request for a g page on the server will be denied.

Is AIG going to use SSO?

The application does not allow concurrent log Only one session per user can be active at any given time.

Single Sign-on. The Company employs multiple single sign-on solutions for portals wishing to integrate the Clearwater website. These solutions include a client SSL certificate proxy-based approach, a SAML 2.0 protocol, and a SiteMinder affiliate agent.

Passwords. Each private label can establish its own private-label policy. The default policy requires a password have a minimum length of characters, and must include one number and one special character. Subject to those criteria, users are able to control their passwords and change them whenever they choose or as mandated by their specific password policy. Passwords are stored in the database after being double hashed using unique salt and encrypted, random long strings, and the recommended digest algorithm and cannot be discovered by the System Administrator.

User Termination Process. When a user is no longer authorized to access the application, his/her log-in is disabled by flagging the user within the database. This will prevent any attempts to access the application. Permissions can be restored by request of the primary client contact.

The primary client contact determines which client employees may access the application and what information they will be allowed to see. Clients are responsible for notifying the Company if a user account should be terminated. The Company terminates unauthorized user access immediately upon client notification and confirms the termination with the client.

Clearwater Employee Access. Clearwater employees are given access only to the systems necessary for performing their job functions. When a candidate is hired, the hiring manager requests HR to start the new-hire process. HR sends a request to IT requesting the new employee be granted access based on their department and job title. The employee's access is granted based on pre-defined and approved templates for the job title.

When an employee terminates, HR sends a request to IT, who removes the employee's access to Clearwater systems.

Physical Access

is AIG asking any report that focuses and related to security, availability, processing integrity, confidentiality, and privacy of the system as per Clearwater uses third-party co-location facility.
doesn't mention if AIG have access to the location
SEE PG 23 showing a SOC1 was reviewed by clearwater
SEE PAG 49 showing Controls

Clearwater utilizes a third-party co-location house its critical applications *(see note rega subservice organization on page 21)*. Acces facility is available to the Company 24/7 an select IT staff. The facility requires authent through a keycard and iris scan to gain acce center.

Clearwater equipment is segregated from t configurations of other co-location custome data center by being secured in a locked se Access to the cabinet is restricted to Clearw administrators.

Security cameras with a digital archive are employed to monitor sensitive locations and ensure sufficient surveillance of visitor activities in the data center.

Environmental Controls

©Clearwater Analytics, LLC 2016

To ensure the protection of its customers' hardware and data assets, the co-location facility utilizes the following industry-standard environmental controls:

- Redundant ventilation and cooling units, with sufficient capacity to handle reasonable fluctuations, maintain constant temperature and humidity within the data center.
- Fire detection equipment and a fire suppression system ensure fires are quickly detected and extinguished.
- Uninterruptible power supply ("UPS") equipment, further supported by a diesel generator, provides continuous power in the event of an outage.
- Redundant power distribution units ("PDU") and mechanical support equipment ensure consistent power to racks and application servers.

Each critical system is properly maintained and regularly tested by the facility to ensure it is functioning properly.

Full daily backup nothing reference to incremental backup

Data Backup and Recovery

Critical application data is backed up a[illegible] from the co-location facility to a geographically separate backup site on a regular and consistent basis. The DBA staff has created an automated job that runs on a daily basis and initiates a full backup of the application's SQL database at the co-location facility to disk. This data is then replicated to disk at the backup site. Upon completion of the daily full backup, transaction logs are then backed up at least hourly and also replicated to the backup site, ensuring that any potential loss of data due to a system crash would be limited to no more than one hour.

Access to the backed up data at both locations is limited to key members of the DBA and IT staff. The DBA staff restores the data from disk on a weekly basis, at a minimum, ensuring recoverability.

Network Security

Clearwater has designed and implemented their network to protect client data and ensure secure client communication with the reporting platform. The primary network components are located at the co-location facility, along with the application and database servers, and are supported by the Company's IT department.

The Company utilizes a firewall to scan incoming/ outgoing traffic. The firewall is configured to deny anything that is not explicitly allowed. The ability to access and modify firewall configurations is limited to key IT personnel.

Web hosts are located in a Demilitarized Zone ("DMZ") behind the firewall and hardened to prevent exploitation by third-party attacks.

The firewall, web hosts, application, and database servers are all clustered to ensure redundancy and provide high availability. Access to the web, database, and domain controller servers is limited to appropriate IT staff. Additionally, DBA privileges are sufficiently limited to appropriate staff. Strong passwords, with required length and complexity, are employed to prevent unauthorized access.

Patching and Security Audits. Operating system security patches are performed, at a minimum, on a monthly basis as released by the operating system vendor. All security patches are installed and tested in a testing environment before they are applied to production servers.

To ensure the firewall and web hosts are properly secured and that potential vulnerabilities are identified and addressed, the Company also utilizes an industry-standard, third-party security tool to audit the external-facing platforms daily. The scanning tool leverages the Common Vulnerabilities and Exposures ("CVE") standard, an index of publicly known information security vulnerabilities. Any weaknesses detected during the scan are discussed with management and addressed in a timely manner.

Anti-Virus Software. Anti-virus software is installed on all hosts within the organization. Definition updates are automated and executed twice a day or as needed based on the availability of patches from the vendor.

Application Monitoring. To track user activity and identify potentially malicious behavior, Clearwater maintains an activity log that records user actions within the application. User events such as failed log-in attempts, successful log-ins/log-outs, passwords changes, compliance parameter changes, etc., are all recorded and time stamped. A subset of critical events, such as multiple failed log-in attempts, are flagged as potential security threats, at which point an email alert is sent to

©Clearwater Analytics, LLC 2016

is AIG having access to the Penetration Testing Reports?

appropriate IT personnel for follow up. Web logs are also maintained and reviewed as required.

Network/Platform Monitoring. To ensure service errors, host availability issues, and network events are quickly identified and addressed in a timely manner, the Company leverages a monitoring tool configured to alert the System Administrators by sending both email and SMS messages detailing the incident.

Penetration Testing. Independent third-party penetration testing is performed annually. Any significant issues identified by these tests are addressed in a timely manner.

Remote Access. Remote access to the co-location facility is limited to appropriate and authorized users.

Business Continuity Management. The Company currently has a disaster recovery strategy for reestablishing the reporting platform and client data after a significant disruption. The Company has an off-site hosting facility, which includes redundant high-speed internet connections and redundant power, including generator power, if required. Web servers are part of a high-availability cluster with fail-over to other machines in the cluster if any individual machine fails. Database files are backed up every hour to off-site servers, which are backed up daily. The redundant site can accommodate all critical functions and systems. Disaster recovery procedures are tested quarterly.

Communication

Effective communication ensures that key messages regarding internal control and executive tone at the top are shared with relevant internal parties across the organization. Additionally, employees should have means to communicate significant control information and report suspected improprieties to management. Relevant procedures include:

- The Company's organizational structure allows for the timely communication of information across the organization when necessary.
- Executive management maintains an open-door policy that allows not only employees but also customers to present questions and concerns as they are deemed necessary.
- Each member of executive management has the responsibility of communicating duties and control responsibilities to those supervised, and they do this via regular committee meetings, initial new associate orientation, and ongoing monitoring of the personnel.
- Formal policies and procedures exist to encourage employees to report suspected improprieties to executive management.
- Management formally communicates its overall commitment to integrity and ethical values in all business relationships.
- Frequent meetings are held by management to communicate the Company's risk tolerance policies, including the proper approval channels upon executing transactions involving risk. Executive management has frequent meetings with the Board.
- Regular communication occurs between executive management and Client Services personnel. An accounting team in Client Services communicates to executive management any significant changes that may have an impact on accounting practices in a timely manner. In the event that the change has an effect on systems, the accounting team meets with the Development Committee to obtain approval on any significant changes. The Committee reviews and prioritizes all proposed system changes. This communication helps ensure that the accounting team is aware of and is involved in any significant changes.

SUBSERVICE ORGANIZATIONS

Pricing Providers - Clearwater Analytics, LLC uses multiple subservice organizations to obtain market prices in support of its operations. The description above under Security Pricing Method includes only policies, procedures and control objectives at the Company and does not include policies, procedures and control objectives of the subservice organizations that provide market price information. The examination of the independent service auditors did not extend to the policies and procedures at these subservice organizations (carve-out method). The following are subservice organizations that provide market price information to Clearwater Analytics, LLC;

©Clearwater Analytics, LLC 2016

- S&P Capital IQ
- Thomson Reuters
- iMoneynet
- Interactive Data
- IHS Markit
- NAIC
- Account Source

Co-location Facilities - Clearwater Analytics, LLC also utilizes subservice organizations to house the System's critical applications. Clearwater Analytics, LLC monitors these subservice organizations and reviews the SOC 1 reports of the subservice organizations. The most recent subservice organization reports received from the subservice organizations were for the periods ended March 31, 2017 and September 30, 2017. Clearwater Analytics, LLC reviewed the subservice organizations' SOC 1 user control considerations as it relates to Clearwater Analytics, LLC's responsibilities and Clearwater Analytics, LLC has applicable controls in place to address the applicable user control considerations. Clearwater Analytics, LLC obtained a letter from the subservice organizations indicating that, since March 31, 2017 and September 30, 2017, the subservice organizations have maintained the underlying design, operational processes, personnel and policies that support the related control objectives included in their SOC I type II report. In addition, based on Clearwater Analytics, LLC's monitoring of the subservice organizations since March 31, 2017 and September 30, 2017 (control objectives 8 and 9), no changes were noted in controls at the subservice organizations. The description above under Physical Access and Environmental Controls includes only policies, procedures, and control objectives at the Company and does not include policies, procedures, and control objectives of the co-location facilities. The examination of the independent service auditors did not extend to policies and procedures at these subservice organizations.

The achievement of certain Company control objectives, however, is dependent upon whether applicable controls at the subservice organizations were suitably designed and operating effectively throughout the period. As such, the regular due diligence the Company performs to confirm the subservice organization is performing the responsibilities is outlined in objectives 3 their related activities.

what about the confidentially of the client account information?

Control Objective 3

- Controls provide reasonable assurance that client account information is calculated, reconciled, and reported accurately and completely.

Control Objectives 8 and 9

- The Company relies on the subservice organization to help ensure physical security standards safeguard critical systems.
- The Company relies on the subservice organization to help ensure environmental standards safeguard critical systems.

what this mean?

CLIENT CONTROL CONSIDERATIONS

The Company's controls are only a portion of the overall internal controls of each client. Clients also need to implement and maintain effective internal controls. Each client's internal controls depend upon the nature of the process, the degree of interaction of controls, and the terms of agreement with the Company. This section highlights some of the controls the Company believes each client should consider for implementation ("User Controls"). The Company has considered User Controls in developing the controls that are described in this report. Each client must evaluate its own internal controls to determine if the following procedures are in place:

- Clients should provide instructions and information in accordance with the provisions of the agreement in effect between the Company and the client. (Control Objectives 2 & 7)
- Clients should provide authorized instructions and information to the Company using data transmission delivery methods in accordance with the Company's security standards. Instructions and information provided to the Company using methods not in accordance with Company security standards may be less secure. (Control Objectives 2 & 7)

©Clearwater Analytics, LLC 2016

- Clients should notify the Company in writing of new accounts or account closures. (Control Objectives 2 & 3)
- Clients should review the accuracy and completeness of the setup of new accounts in the analytics platform. (Control Objective 2)
- Clients who have had data back-loaded onto the analytics platform should note that this data may not be subject to the processes detailed in this report. (Control Objective 5)
- Clients should notify the Company immediately of terminated or transferred employees with access to the Company's computer systems whose access should be removed or modified by the Company. (Control Objective 7)
- Clients should establish, monitor, and maintain effective controls over access to the Company's analytics and reports via terminals at client locations. (Control Objectives 7 & 8)
- Clients should notify the Company immediately of changes to individuals authorized to instruct the Company on a client's behalf. (Control Objective 7)
- Clients should maintain effective controls to ensure compliance parameter changes submitted to the Company are appropriately authorized. (Control Objective 4)
- Clients should review the established guidelines within the Company's compliance platform to determine the completeness and accuracy of the investment policy guidelines. (Control Objective 4)
- Clients should notify the Company in writing of portfolio accounting policies, including accounting assumptions and/or indices, as well as changes thereto. (Control Objectives 2, 3, 4, & 5)
- Clients should verify the accounting assumptions employed by the Company's accounting platform agree to the client's documented assumptions. (Control Objectives 2, 3, & 5)
- Clients are responsible for the fair presentation in the financial statements of financial position, results of operations, cash flows, changes in net assets, financial highlights, and STAT reports in conformity with generally accepted accounting principles ("GAAP"), statements of statutory accounting principles ("SSAP"), or any regulatory agency requirements. (Control Objectives 3 & 5)
- Clients should maintain effective controls over the accuracy and completeness of the investment policy, portfolio guidelines, and/or other information provided to the Company. (Control Objectives 2, 3, 4, & 5)
- Clients are responsible for selecting pricing sources for the valuation of securities. (Control Objective 3)
- Clients are responsible for reviewing default tolerable error thresholds (dollar and/or percent values) for daily pricing reasonableness tests. Clients are responsible for adjusting those requirements, if necessary. (Control Objective 3)

The list of client control considerations presented above does not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations.

Not clear what is the level of responsability in this paragraph - Which others?

©Clearwater Analytics, LLC 2016

clearwater

Section Four

Control Objectives, Related Controls, and Tests of Operating Effectiveness

©Clearwater Analytics, LLC 2016

Purpose and Objectives of the Independent Service Auditor's Examination

This report on the controls placed in operation and tests of operating effectiveness applicable to Clearwater Analytics, LLC is intended to provide interested parties with information sufficient to obtain an understanding of those aspects of Clearwater Analytics, LLC's controls that may be relevant to a user organization's internal control over financial reporting. This report, when coupled with an understanding of the controls in place at user entities, is intended to assist in the assessment of the internal controls applicable to the reporting provided by Clearwater Analytics, LLC for user entities.

Our examination was restricted to the selected services, control objectives and related procedures specified by Clearwater Analytics, LLC in the controls and testing in Section IV, and was not extended to procedures in effect at user entities and outsourced vendor organizations, or other controls that may be described in Section III but not listed in Section IV. Clearwater Analytics, LLC specified its control objectives and is responsible for identifying its controls to meet those objectives.

The examination was conducted in accordance with the Statements on Standards for Attestation Engagements 18 of the American Institute of Certified Public Accountants. It is each interested party's responsibility to evaluate this information in relation to the internal control in place at user organizations to obtain an overall understanding of the internal controls and assess control risk. The user entity and Clearwater Analytics, LLC's portions of the control structure must be evaluated together. If effective user entity internal controls are not in place, Clearwater Analytics, LLC's controls may not compensate for such weaknesses.

A system of internal control is intended to provide reasonable, but not absolute, assurance that the control objectives are achieved. The concept of reasonable assurance recognizes that the cost of a system of internal control should not exceed the benefits expected to be derived and also recognizes that the evaluation of the cost-benefit relationship requires estimates and judgments by management.

Our tests of the effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved throughout the period from January 1, 2017 to December 31, 2017. Our tests of the operational effectiveness of controls were designed to cover a representative number of transactions throughout the period of January 1, 2017 to December 31, 2017 for each of the controls listed in Section IV which are designed to achieve the specific control objectives, also listed in Section IV.

In selecting particular tests of the operational effectiveness of controls, we considered (a) the nature of the items tested, (b) the types and competence of available evidential matter, (c) the nature of the audit objectives to be achieved, (d) the assessed level of control risk and (e) the expected efficiency and effectiveness of the test and (e) the expected efficiency and effectiveness of the test.

©Clearwater Analytics, LLC 2016

Description of Testing Procedures

Test procedures performed in connection with determining the operational effectiveness of controls detailed in the matrices in Section IV are described below:

Test	Description
Inquiry	Inquired of appropriate personnel to ascertain their knowledge and understanding of the compliance of the controls. Inquiries were performed on all controls. However, the test is not listed individually for every control shown in the accompanying matrices.
Observation	Observed application of specific controls.
Inspection	Inspected documents and reports indicating performance of the controls.
Reperformance	Reperformed application of the controls.

Within the testing procedures, sampling refers to non-statistical sampling methods and techniques. Likewise, when referring to a selection of items, such selection was not based on sampling methods and techniques.

Exceptions, if any, noted by Eide Bailly LLP, regarding the adequacy of the controls identified to achieve the stated objective or the level of compliance with the controls are presented in this section under the caption "Results of Testing".

Control considerations that should be exercised by user organizations in order to complement the controls of Clearwater Analytics, LLC are presented in Section III of this report.

©Clearwater Analytics, LLC 2016

Control Objectives

The Company has specified its objectives and identified the controls in place to achieve those objectives for the processing of transactions for its clients in the following matrices. These objectives have been determined by Company management.

The procedures performed to test operating effectiveness and the results of those tests procedures are listed next to each of the Company's respective objectives and controls.

Ethical Behavior

1. Controls provide reasonable assurance that a culture of ethical behavior is communicated and encouraged.

Security Processing, Valuation, and Customer Reporting

2. Controls provide reasonable assurance that critical documentation and instructions for the opening and maintenance of accounts are received, reviewed, and implemented properly.
3. Controls provide reasonable assurance that client account information is calculated, reconciled, and reported accurately and completely.
4. Controls provide reasonable assurance that the compliance platform tracks, reports, and archives client investment guideline information accurately and completely.

Statutory Reporting

5. Controls provide reasonable assurance that Clearwater STAT reports and filing statements meet relevant NAIC procedures and formats.

Information Technology

6. Controls provide reasonable assurance that application development standards are appropriate to ensure proper developmental oversight and that permissions to modify source code and migrate changes into production are properly restricted.
7. Controls provide reasonable assurance that logical access to client account information is restricted and granted only to properly authorized individuals; and information technology security measures exist and are adhered to.
8. Controls provide reasonable assurance that physical security standards are appropriate to safeguard critical systems.
9. Controls provide reasonable assurance that environmental standards are appropriate to safeguard critical systems.
10. Controls provide reasonable assurance that application data is regularly and completely backed-up and stored off-site.
11. Controls provide reasonable assurance that the network design, maintenance, and monitoring activities are appropriate to safeguard critical systems.

See pg.41

©Clearwater Analytics, LLC 2016

Ethical Behavior

Control Objective 1: Controls provide reasonable assurance that a culture of ethical behavior is communicated and encouraged.

Control Number	Controls	Testing performed by Eide Bailly LLP	Results of Tests
1.1	Annually, the Human Resources Department obtains a signed Acknowledgment from each employee certifying compliance with the Code of Ethics.	1. Inspected signed copies of Acknowledgments for a sample of employees to evidence the Human Resources Department obtains a signed Acknowledgment from each employee certifying compliance with the Code of Ethics.	No exceptions noted.
1.2	The Human Resources Department maintains a signed employee NDA on file for each employee.	1. Inspected signed copies of employee NDAs for a sample of employees to evidence the Human Resources Department maintains a signed employee NDA on file for each employee.	No exceptions noted.
1.3	Management communicates formally on an annual basis its overall commitment to integrity and ethical values.	1. Inspected management's communications, annually, to employees regarding its overall commitment to integrity and ethical values to evidence management communicates formally on at least an annual basis its overall commitment to integrity and ethical values.	No exceptions noted.
1.4	The Human Resources Department performs a background check on every new employee.	1. Inspected personnel files for a sample of new employees to evidence the Human Resources Department performs a background check on every new employee.	No exceptions noted.

©Clearwater Analytics, LLC 2016

Security Processing, Valuation, and Customer Reporting

Control Objective 2: Controls provide reasonable assurance that critical documentation and instructions for the opening and maintenance of accounts are received, reviewed, and implemented properly.

Control Number	Controls	Testing performed by Eide Bailly LLP	Results of Tests
2.1	The New Client Checklist is completed to ensure that all necessary activities have been performed to set up a new client.	1. Inspected the completed new client checklist for a sample of new clients to evidence that the New Client Checklist is completed to ensure that all necessary activities have been performed to set up a new client.	No exceptions noted.
2.2	A formal, signed agreement is obtained from the client.	1. Inspected a formal, signed agreement for a sample of new clients to evidence that it is obtained from the client.	No exceptions noted.
2.3	All administrative changes to existing accounts must be requested by the client.	1. Inspected client change requests for a sample of administrative changes to evidence that changes must be requested by the client.	No exceptions noted.
2.4	When loading historical information, Clearwater reconciles loaded historical reports with previously filed reports. Discrepancies identified are evaluated and corrected.	1. Inspected reconciliations of loaded historical reports to previously filed reports and corrections of any noted discrepancies for a sample of new clients to evidence the reconciliation was performed.	No exceptions noted.

©Clearwater Analytics, LLC 2016

Control Objective 3: Controls provide reasonable assurance that client account information is calculated, reconciled, and reported accurately and completely.

Control Number	Controls	Testing performed by Eide Bailly LLP	Results of Tests
3.1	At the appropriate frequency (daily or monthly), extracts of custodian data sources are systematically downloaded.	1. Inspected custodian data files on a specific date to evidence data is being downloaded at the appropriate frequency as configured by custodians. 2. Inspected custodial data feed for a custodian on a specific date to evidence it is downloaded at the appropriate frequency as configured by the custodian.	No exceptions noted.
3.2	Downloaded custodian data extracts are systematically aligned with Clearwater data in the Clearwater format. Any issues are investigated and resolved by the Clearwater team.	1. Inspected a downloaded custodian data extract for one account and compared to the respective reconciliation to evidence custodian data extracts were aligned appropriately.	No exceptions noted.
3.3	The system calculates principal, income and amortization predictions as well as market values daily.	1. Inspected supporting documentation for daily reconciliations for a sample of investments within client accounts to evidence that the system calculates principal, income and amortization predictions as well as market value daily. 2. Inspected supporting documentation for a sample of equity securities to evidence the system calculates income as well as market values daily. 3. Inspected supporting documentation for a sample of fixed income securities to evidence the system calculates principal, income and amortization predictions as well as market values daily.	No exceptions noted.
3.4	The system compares third party pricing, predicted principal and income, transactions, cash and positions, and market values to custodian data on a daily basis (Reconciliation).	1. Inspected supporting documentation of daily reconciliations for a sample of investments within client accounts to evidence that the system compares third party pricing, predicted principal and income, transactions, cash and positions, and	No exceptions noted.

©Clearwater Analytics, LLC 2016

		market values to custodian data on a daily basis (Reconciliation). 2. Inspected supporting documentation for a sample of equity securities to evidence the system compares predicted transactions, cash and positions, as well as market values to custodian data daily. 3. Inspected supporting documentation for a sample of fixed income securities to evidence the system compares predicted principal and income, transactions, cash and positions, as well as market values to custodian data daily.	
3.5	Reconciliation discrepancies outside of set tolerances are investigated and resolved daily by the Client Service team before accounts are marked as reconciled.	1. Inspected supporting documentation for daily reconciliations for a sample of investments within client accounts to evidence that reconciliation discrepancies outside of set tolerances are investigated and resolved daily by the Client Service team before accounts are marked as reconciled. 2. Inspected supporting documentation for a sample of equity securities to evidence that reconciliation discrepancies outside of set tolerances are investigated and resolved daily by the Client Service team before accounts are marked as reconciled. 3. Inspected supporting documentation for a sample of fixed income securities to evidence that reconciliation discrepancies outside of set tolerances are investigated and resolved daily by the Client Service team before accounts are marked as reconciled.	No exceptions noted.
3.6	A system-generated Task List identifies potential data issues through a number of consistency checks, reasonableness tests, and comparison with third-party data sources.	1. Inspected a sample of daily system-generated Task List reports to evidence that the report identifies potential data issues through a number of consistency checks, reasonableness tests, and comparison with third-party data sources.	No exceptions noted.

©Clearwater Analytics, LLC 2016

3.7	The automated system performs checks to ensure that the data being reported is accurate and internally consistent. System-identified issues are investigated and corrected or explained as applicable.	1. Inspected a sample of systems checks to evidence that items identified by systematic checks were corrected or explained, as applicable, prior to being pushed to the client reporting module. 2. Observed Client Service personnel run system checks and reconcile discrepancies for one item identified by systematic checks to evidence that the system performs checks to ensure data is accurate and consistent.	No exceptions noted.
3.8	For market-driven pricing, the Company uses industry-recognized and independent pricing sources to determine the daily valuation of the client's securities.	1. Inspected supporting documentation for a sample of equity securities to evidence that independent market pricing sources are being implemented in client accounts accurately. 2. Inspected supporting documentation for a sample of fixed income securities to evidence that independent market pricing sources are being implemented in client accounts accurately. 3. Observed Client Services personnel review the pricing sources requested by a client and setup in Clearwater's system to evidence the Company uses industry-recognized and independent pricing sources to determine the daily valuation of the client's securities.	No exceptions noted.
3.9	On a daily basis, third-party prices are systematically downloaded.	1. Inspected third-party data files on a specific date to evidence data is being downloaded at the appropriate frequency as configured by the third-party. 2. Inspected third-party data feed for a custodian on a specific date to evidence it is downloaded at the appropriate frequency as configured by the third-party.	No exceptions noted.
3.10	Pricing errors resulting from third parties downloads are monitored and resolved in a timely manner.	1. Inspected the downloading of third party prices for a sample of days to evidence that pricing errors resulting from third-party downloads are	No exceptions noted.

©Clearwater Analytics, LLC 2016

		monitored and resolved in a timely manner.	
3.11	On a daily basis, prices obtained from third party sources are systematically compared to prices assigned to selected client accounts.	Testing Period: From March 13, 2017 to December 31, 2017: 1. Inspected a sample of daily reports to evidence third-party pricing sources are compared to prices on client accounts on a daily basis.	No exceptions noted.
3.12	A daily pricing reasonableness test is executed on account pricing based on percent change from prior day. Prices outside a tolerable variance are investigated and resolved.	1. Inspected supporting documentation for a sample of equity securities to evidence that a daily pricing reasonableness test is executed on account pricing based on percent change from prior day. Prices outside a tolerable variance are investigated and resolved. 2. Inspected supporting documentation for a sample of fixed income securities to evidence that a daily pricing reasonableness test is executed on account pricing based on percent change from prior day. Prices outside a tolerable variance are investigated and resolved. 3. Observed Client Services personnel investigate and resolve a variance identified via the daily pricing reasonableness test for a specific security to evidence a daily pricing reasonableness test is executed on account pricing based on percent change from prior day and results outside tolerance are investigated and resolved.	No exceptions noted.
3.13	Notification of corporate actions are reconciled against recognized independent sources through the daily cash, positions, and transactions reconciliation process performed by Client Services and Data personnel.	1. Inspected corporate action resolution for a sample of corporate actions noting that corporate actions are identified and appropriately resolved using information from independent recognized sources.	No exceptions noted.
3.14	Automated checks are in place to compare and identify differences between the NAIC quarterly and annual filings and the Clearwater reports.	1. Inspected a sample of accounts requesting a schedule D reporting to evidence that automated checks are performed to compare and identify	No exceptions noted.

©Clearwater Analytics, LLC 2016

		differences between NAIC reports and the STAT reports.	
3.15	All items identified by the systematic comparison between Company calculated figures and custody data are addressed prior to the availability of period-end report files.	1. Inspected a sample of system comparisons to evidence all items identified by the systematic comparison were resolved prior to data being pushed to the client reporting module. 2. Observed Client Services personnel run system checks one period and reconcile items identified by systematic comparison between Company calculated figures and custody data.	No exceptions noted.

©Clearwater Analytics, LLC 2016

Control Objective 4: Controls provide reasonable assurance that the compliance platform tracks, reports, and archives client investment guideline information accurately and completely.

Control Number	Controls	Testing performed by Eide Bailly LLP	Results of Tests
4.1	Only authorized Clearwater employees can edit client investment guideline parameters.	1. Inspected the listing of users with access to edit client investment guideline parameters to evidence users are authorized.	No exceptions noted.
4.2	New compliance rules are tested and reviewed to verify they are functioning properly.	1. Observed a Client Service team member implement a new compliance rule in the system to evidence new compliance rules are not released into production before they are functioning properly. 2. Observed a Client Service team member attempt to implement a rule with incorrect logic to evidence new compliance rules are not allowed to be released into production until they function properly.	No exceptions noted.
4.3	The system records compliance violations daily, which are retained for archival review.	1. Inspected logged compliance issues retained for archival review to evidence the system records compliance violations daily.	No exceptions noted.

©Clearwater Analytics, LLC 2016

4.4	Compliance history modification rights are limited to authorized staff.	1. Inspected a sample of staff with compliance history modification rights and inquired of management to evidence the rights are limited to authorized staff.	**Exception Noted**: For 1 out of 5 authorized staff tested, access to make compliance modifications was improper due to permission not being removed when no longer appropriate. **Management Response:** Per additional testing performed by Clearwater, access to modify compliance history had not been removed for the noted employee after the employee changed roles. Management confirmed the employee made no changes to compliance history while he had inappropriate access. Management reviewed all access for transferred employees during July-December 2017 and noted 4 additional employees whose access had not been removed appropriately as part of a transfer. Management reviewed access history of the 4 exceptions and confirmed no changes were made while they had inappropriate access. Management also implemented a secondary review to confirm transferred employee access is updated appropriately.

©Clearwater Analytics, LLC 2016

4.5	Client Services team members review out-of-compliance issues to verify compliance violations have occurred.	1. Observed Client Services team members review the out-of-compliance violations log to evidence compliance violations have occurred. 2. Re-performed review of out-of-compliance issues for an account to evidence compliance violations had occurred, and resolutions procedure were addressed.	No exceptions noted.
4.6	Compliance limit changes made by company employees are only done as specified by the client.	1. Inspected client change requests for a sample of compliance limit changes to evidence Compliance limit changes made by company employees are only done as specified by the client.	No exceptions noted.

©Clearwater Analytics, LLC 2016

Statutory Reporting

Control Objective 5: Controls provide reasonable assurance that Clearwater STAT reports and filing statements meet relevant NAIC procedures and formats.

Control Number	Controls	Testing performed by Eide Bailly LLP	Results of Tests
5.1	The automated system performs checks to ensure that the data being reported is accurate and internally consistent. System-identified issues are investigated and corrected or explained as applicable.	1. Inspected a sample of systems checks to evidence that items identified by systematic checks were corrected or explained, as applicable, prior to being pushed to the client reporting module. 2. Observed Client Service personnel run system checks and reconcile discrepancies identified by systematic checks to evidence that the system performs checks to ensure data is accurate and consistent.	No exceptions noted.
5.2	Clearwater obtains directly from the NAIC new "blanks" and instructions annually as well as any updates, which highlight any changes to relevant reports or instructions.	1. Inspected system templates to evidence implementation of changes to relevant reports or instructions.	No exceptions noted.
5.3	Changes to NAIC quarterly and annual text files as a result of quarterly NAIC updates are tested prior to being released to production.	1. Inspected most recent changes made to Schedule D text file as a result of quarterly NAIC updates. 2. Observed as Schedule D text file was downloaded from the system to analysis software and any errors identified were reviewed and reconciled.	No exceptions noted.
5.4	If the client elects to use NAIC pricing, a systematic process is used to populate the market price based on the NAIC data.	1. Observed security pricing, using NAIC data, for a security from a client that uses NAIC pricing to evidence that client requested pricing is properly populated in periodic reporting.	No Exceptions noted.
5.5	Automated checks are in place to compare and identify differences between the NAIC quarterly and annual filings and the Clearwater reports.	1. Inspected NAIC report consistency check results for a sample of clients requesting Schedule D or STAT reports to evidence that the system performs consistency checks before periodic reports are available.	No exceptions noted.

©Clearwater Analytics, LLC 2016

5.6	When loading historical information, Clearwater reconciles loaded historical reports with previously filed reports. Discrepancies identified are evaluated and corrected.	1. Inspected reconciliations of loaded historical reports to previously filed reports and corrections of any noted discrepancies for a sample of new clients to evidence the reconciliation was performed.	No exceptions noted.

©Clearwater Analytics, LLC 2016

Information Technology

Control Objective 6: Controls provide reasonable assurance that application development standards are appropriate to ensure proper developmental oversight and that permissions to modify sources code and migrate changes into production are properly restricted.

Control Number	Controls	Testing performed by Eide Bailly LLP	Results of Tests
6.1	To create and maintain code, developers utilize a code repository, which tracks all changes to source code files, including what change was made, when the change was made, and who made the change.	1. Inspected the log of changes in the log tracking tool to evidence that it tracks changes to source code files, including what change was made, when the change was made, and who made the change.	No exceptions noted.
6.2	The ability to make code modifications in the code repository is strictly limited to appropriate members of the Development team.	1. Inspected a sample of users with access to modify code in the code repository to evidence these users are limited to members of the Development team. 2. Inspected the results of management's most recent review of users with access to modify code in the code repository to evidence that the review was performed.	No exceptions noted.
6.3	Before being introduced into production code testing occurs. Testing includes both functional testing of new features, as well as regression testing to ensure existing functionality remains intact.	1. Inspected a sample of application changes to evidence changes were tested prior to being introduced into production.	No exceptions noted.
6.4	Once code has been prepared for deployment (compiled, tested, and versioned), the versioned file cannot be modified.	1. Inspect the repository of compiled versions and observed that users are not able to modify the compiled code.	No exceptions noted.

©Clearwater Analytics, LLC 2016

6.5	Access to production and domain servers is limited to appropriate system administrators with strong passwords, limiting access from unauthorized users. not clear the policy for Password setting configuration	1. Inspected user access lists and inquired of management for production and domain servers to evidence that access was limited to appropriate and authorized personnel and that administrator rights were sufficiently restricted. 2. Inspected configurations on production servers and domain controllers to ensure password settings for length and complexity are appropriate to reduce the risk of unauthorized access.	No exceptions noted.
6.6	Access for terminated employees is removed within 24 hours.	1. Inspected system documentation evidencing access for a sample of terminated employees was removed within 24 hours. 2. Inspected the ticketing system for terminated users to evidence that employees had physical access removed within 24 hours.	No exceptions noted.
6.7	Each new Clearwater employee is granted access to systems needed to perform his/her job function only after approval from the appropriate department manager has been received.	1. Inspected system documentation evidencing approval from the appropriate department manager is required to grant each new employee access to systems needed to perform his/her job function. 2. Inspected a sample of new users to evidence that access granted to new users had been approved by the appropriate department manager.	No exceptions noted.
6.8	The company maintains tools that track bugs to ensure that identified bugs are properly recorded and addressed by the Development team.	1. Inspected a sample of critical issues from the tracking tool logs to evidence that bugs are properly recorded and addressed by the Development team.	No exceptions noted.

©Clearwater Analytics, LLC 2016

6.9	No developers have the ability to deploy applications to the production environment.	1. Inspected permissions in version management software and on production servers to ensure that the ability to migrate code into test and production environments is limited to authorized individuals and not to software developers.	No exceptions noted.

©Clearwater Analytics, LLC 2016

Control Objective 7: Controls provide reasonable assurance that logical access to the reporting platform and data is restricted and only granted to properly authorized individuals; and information technology security measures exist and are adhered to.

Control Number	Controls	Testing performed by Eide Bailly LLP	Results of Tests
7.1	Access to edit client investment reporting information is restricted to authorized users.	1. Inspected a sample of users who have the ability to edit client investment reporting information and inquired of management to evidence that the users are appropriately authorized. 2. Inspected management's review of access privileges conducted during the review period.	No exceptions noted.
7.2	The ability to directly modify data within the application database is limited to authorized staff.	1. Inspected a sample of employees to evidence that authorization of access to directly modify data within the application database is limited to authorized employees. 2. Inspected management's review of access privileges conducted during the review period.	No exceptions noted.
7.3	The ability to make code modifications in the code repository is strictly limited to appropriate members of the Development team.	1. Inspected a sample of users with access to modify code in the code repository to evidence these users are limited to members of the Development team. 2. Inspected the results of management's most recent review of users with access to modify code in the code repository to evidence that the review was performed.	No exceptions noted.
7.4	Client users and Company employee access to the reporting system is limited through the use of a web-based log-in protocol.	1. Re-performed attempt to access the application through alternate means besides the login page.	No exceptions noted.
7.5	Both read and write access to accounts granted to external	1. Obtained a population of external users with write access	No exceptions noted.

©Clearwater Analytics, LLC 2016

	users must be approved by the client.	to test users have been approved by the client. 2. Selected a sample of external users with write access from the population and obtained evidence these users have been approved by the client.	
7.6	Password policies are determined at the private label level. The default is that passwords must meet a set of minimum criteria including a minimum length of characters, of which at least two must be special characters, to be accepted by the system.	1. Re-performed attempt to change the password outside of the established parameters, noting any failures. 2. Inspected the password configurations within the system for the control objective.	No exceptions noted.
7.7	User passwords are encrypted and cannot be discovered by the system administrator. A new password must be generated if forgotten.	1. Inspected user table in the application database to determine whether the passwords fields were encrypted.	No exceptions noted.
7.8	Single sign-on architecture is appropriately designed to ensure secure connections.	1. Observed an authorized company employee log onto a test account on the company's website and navigate to a web application housed on Clearwater's systems to evidence that single sign-on architecture was appropriately designed to ensure secure connections.	No exceptions noted.
7.9	Authentication is performed on every request accessible on the reporting system. Data will not be returned to any request not properly authenticated.	1. Re-performed attempt to enter URL for a protected page on the site in an unauthenticated browser, noting access was appropriately denied.	No exceptions noted.
7.10	All transmissions between the client and the Company server are encrypted.	1. Inspected a selection of web pages in the system to determine whether proper SSL cryptography applied to the pages.	No exceptions noted.
7.11	Significant security events within the application are logged and trigger rules which notify System Administrators, and significant security events in network device logs and in network traffic trigger rules	1. Inspected a log of security events that occurred during the review period. 2. Inspected log tracking tools that are monitored by the System Administrators and Information Security Team.	No exceptions noted.

©Clearwater Analytics, LLC 2016

	which notify the Information Security Team.		
7.12	Access to production and domain servers is limited to appropriate system administrators with strong passwords, limiting access from unauthorized users.	1. Inspected user access lists and reviewed with management for production and domain servers. Observed that access was limited to appropriate and authorized personnel and that administrator rights were sufficiently restricted. 2. Inspected configurations on production servers and domain controllers to ensure password settings for length and complexity are appropriate to reduce the risk of unauthorized access.	No exceptions noted.
7.13	The client data upload for designations and pricing is done through the secured NAIC website.	1. Inspected a client data file uploaded to NAIC to evidence that the website is secured.	No exceptions noted.
7.14	Only users authorized by the client can download reports from the Clearwater secure web site.	1. Inspected user access to evidence that the client had authorized the user to download reports from the Clearwater secure website. 2. Re-performed a client administrative setup to evidence that only users authorized by the client can authorize sub users.	No exceptions noted.
7.15	Access for terminated employees is removed within 24 hours.	1. Inspected system documentation evidencing access for a sample of terminated employees was removed within 24 hours. 2. Inspected the physical access logs for users to evidence that terminated users did not access the building between their termination date and the date their access was removed.	No exceptions noted.
7.16	Each new Clearwater employee is granted access to systems needed to perform his/her job function only after approval from the appropriate department manager has been received.	1. Inspected evidence of department manager approval for access to systems and compared to access date for a sample of employees.	No exceptions noted.

©Clearwater Analytics, LLC 2016

7.17	DBA privileges are sufficiently limited to appropriate system administrators.	1. Inspected a list of users with DBA privileges and verified with management that DBA privileges were limited to appropriate system administrators. 2. Inspected management's review of access privileges conducted during the review period.	No exceptions noted.

©Clearwater Analytics, LLC 2016

Control Objective 8: Controls provide reasonable assurance that physical security standards are appropriate to safeguard critical systems.

Control Number	Controls	Testing performed by Eide Bailly LLP	Results of Tests
8.1	Clearwater management performs monitoring to ensure that company personnel with physical access to the co-location facilities is limited to authorized members of the Clearwater IT staff.	1. Inspected evidence of periodic reviews performed by management of co-location physical access lists to validate only authorized company employees may access the facilities. Inspected evidence of management's review of the most recent SOC report from their colocation providers, to evidence that management validated controls are in place to ensure that only authorized employees may access the facilities.	No exceptions noted.
8.2	Clearwater management performs monitoring to ensure that physical access to the servers is limited by the use of biometric scanners or electronic keypads.	1.Inspected evidence of periodic reviews performed by management of the co-location facilities to validate that physical access controls include use of biometric fingerprint scanners or electronic keypads. Inspected evidence of management's review of the most recent SOC reports from their colocation providers, to evidence that management validated physical access controls are in place to include the use of biometric scanners or electronic keypads.	No exceptions noted.
8.3	Clearwater management performs monitoring to ensure that Clearwater hardware is secured in locked cabinets and segregated from other customer equipment in the data centers.	1. Inspected evidence of periodic monitoring performed by management to validate that Clearwater hardware was segregated from other equipment in locked cabinets at the co-location facilities.	No exceptions noted.

©Clearwater Analytics, LLC 2016

8.4	Clearwater management performs monitoring to ensure that the co-location facilities are monitored 24/7 by surveillance cameras and / or experienced facility network/security staff.	1. 1. Inspected evidence of periodic monitoring performed by management to validate the presence of facility surveillance cameras at the co-location facilities. Inspected evidence of management's review of the most recent SOC reports from their colocation providers, to evidence that management validated controls are in place to ensure the presence of facility surveillance cameras at the colocation facilities.	No exceptions noted.

Physical location 3rd party

Control Objective 9: Controls provide reasonable assurance that environmental standards are appropriate to safeguard critical systems.

Control Number	Controls	Testing performed by Eide Bailly LLP	Results of Tests
9.1	Clearwater management performs monitoring to ensure that climate control to the data centers is provided by redundant heating ventilation and cooling (HVAC) units, which are monitored by facility staff.	1. Inspected evidence of periodic monitoring performed by management to validate the use of HVAC units in the co-location facilities. 2. Inspected evidence that management has obtained and reviewed the most recent HVAC tests to determine that heating and cooling units are being monitored and appropriately controlled. 3. Inspected evidence of management's review of the most recent SOC reports from their colocation providers, to evidence that management validated controls are in place to ensure that climate control to data centers is provided by redundant heating ventilation and cooling (HVAC) units, which are monitored by facility staff.	No exceptions noted.

©Clearwater Analytics, LLC 2016

9.2	Clearwater management performs monitoring to ensure that fire detection equipment is located within the data centers to alert facility staff to potential fire conditions. Gas fire suppression systems are used in the event of a fire. The fire detection equipment and the gas fire suppression system are tested, at a minimum, on an annual basis.	1. Inspected evidence of periodic monitoring performed by management to validate the presence of fire detection equipment including gas fire suppression systems at the co-location facilities. 2. Inspected evidence of management's review of the most recent SOC reports from their colocation providers, to evidence that management validated the presence of fire detection equipment including gas fire suppression systems at the co-location facilities.	No exceptions noted.
9.3	Clearwater management performs monitoring to ensure that uninterruptible power supply (UPS) systems are utilized to ensure consistent power to the data centers and an orderly shutdown of systems if necessary.	1. Inspected evidence of periodic monitoring performed by management to validate the existence, location, and utilization of UPS systems at the co-location facilities. 2. Inspected evidence of management's review of the most recent SOC reports from their colocation providers, to evidence that management validated the existence, location, and utilization of UPS systems at the colocation facilities.	No exceptions noted.
9.4	Clearwater management performs monitoring to ensure that regular tests are conducted to provide assurance the UPS systems and generators are working properly.	1. Inspected evidence that management has obtained and reviewed the most recent UPS systems and generators. Inspected evidence of management's review of the most recent SOC reports from their colocation providers, to evidence that management validated that regular tests are conducted to provide assurance the UPS systems and generators are working properly.	No exceptions noted.

©Clearwater Analytics, LLC 2016

9.5	Clearwater management performs monitoring to ensure that the co-location facilities also utilize diesel generators to provide power during extended outages.	1. Inspected evidence of periodic monitoring performed by management to validate the existence, location, and utilization of diesel power generators. 2. Inspected evidence of management's review of the most recent SOC reports from their colocation providers, to evidence that management validated that the co-location facilities also utilize diesel generators to provide power during extended outages.	No exceptions noted.

©Clearwater Analytics, LLC 2016

Control Objective 10: Controls provide reasonable assurance that application data is regularly and completely backed-up and stored off-site.

Control Number	Controls	Testing performed by Eide Bailly LLP	Results of Tests
10.1	Automated jobs are performed to ensure backups are regularly and consistently executed.	1. Inspected automated job configurations to evidence that the application database is scheduled to be backed up on a daily basis from the co-location facility to the Clearwater site. 2. Inspected automated job configurations to evidence that transaction logs are scheduled to be backed up on an hourly basis from the co-location facility to the Clearwater site.	No exceptions noted.
10.2	Backups are regularly tested to ensure data is fully restorable.	1. Inspected automated job configurations to evidence that the application database is scheduled to be restored on a three-minute basis. 2. Observed the logs demonstrating successful restoration of recently backed-up application data.	No exceptions noted.
10.3	Backups are stored in an offsite location.	1. Observed the backup and storage process. 2. Inspected automated notifications and alerts provided to database administrators for the purpose of monitoring the progress of backups moved to an offsite location.	No exceptions noted.

©Clearwater Analytics, LLC 2016

Control Objective 11: Controls provide reasonable assurance that the network design, maintenance, and monitoring activities are appropriate to safeguard critical systems.

Control Number	Controls	Testing performed by Eide Bailly LLP	Results of Tests
11.1	By default, all services and ports on the firewall are disabled. Management enables only those ports necessary for client connectivity and back-office communications.	1. Observed firewall configuration to determine whether only ports necessary for client connectivity and back-office are enabled.	No exceptions noted.
11.2	The network architecture utilizes firewalls, a VPN, a DMZ and dual web, database and application servers to ensure redundancy, high availability and sufficient security.	1. Observed the use of firewalls, a VPN, a DMZ and high availability configurations.	No exceptions noted.
11.3	Access to production and domain servers is limited to appropriate system administrators with strong passwords, limiting access from unauthorized users.	1. Inspected user access lists and inquired of management for production and domain servers to evidence that access is limited to appropriate and authorized personnel and administrator rights were sufficiently restricted. 2. Inspected configurations on production servers and domain controllers to ensure password settings for length and complexity are appropriate to reduce the risk of unauthorized access.	No exceptions noted.
11.4	The ability to view and modify firewall configurations is limited to appropriate IT administrators.	1. Inspected firewall user access settings with Network Administrator to evidence that the ability to view and modify firewall configurations is limited to appropriate IT administrators.	No exceptions noted.
11.5	Patches are applied on a regular basis to all web, application, and domain servers. Clearwater utilizes tools to ensure all required patches are installed.	1. Inspected the settings of patch monitoring tools to ensure servers are regularly scanned to evidence that all required patches are installed. 2. Inspected results of the most recent scans to evidence that patches have been applied.	No exceptions noted.

©Clearwater Analytics, LLC 2016

11.6	Independent third-party application and network vulnerability audits are performed daily. Significant issues resulting from the audit are addressed.	1. Inspected evidence of daily application and network vulnerability audits and the resolution of significant issues.	No exceptions noted.
11.7	Independent third-party penetration testing is performed annually. Any significant issues identified by these tests are addressed.	1. Inspected the report from the most recent independent third-party penetration testing to evidence that testing was performed. 2. Observed open tickets associated with each recommendation from the most recent penetration test report to evidence that the organization is tracking and addressing identified significant vulnerabilities.	No exceptions noted.
11.8	Access for terminated employees is removed within 24 hours.	1. Inspected system documentation evidencing access for a sample of terminated employees was removed within 24 hours. 2. Inspected the physical access logs for users to evidence that terminated users did not access the building between their termination date and the date their access was removed.	No exceptions noted.
11.9	The organization utilizes network management tools including host-based monitoring and intrusion detection to monitor network activity for predefined security events. System Administrators are alerted to predefined network security events.	1. Inspected reports, alerts, and dashboards provided by network monitoring tools.	No exceptions noted.

©Clearwater Analytics, LLC 2016

clearwater

Appendix A

Documents sent to onboarding clients containing a comprehensive list of assumptions that can be applied to the accounting platform

©Clearwater Analytics, LLC 2016

Basic Client Information

clearwater

This form is used to gather essential information for the onboarding process with Clearwater. Below are accounting assumptions available for selection on the Clearwater system as well as areas to list your contacts and key information.

Basic Information

Company Name _____

Street Address _____

Address Line 2 _____

City _____

State AL _____ Zip Code _____

Company Ticker *(or preferred abbreviation)* _____

Please provide an invoicing contact. You may provide multiple contacts if necessary.

Name _____

Title _____

Email _____

Phone _____

Street Address _____

Address Line 2 _____

City _____

State AL _____ Zip Code _____

Specific Invoicing Requests *(cost centers, delivery method, etc.)*:

_____

_____

Name _____

Title _____

Email _____

Phone _____

Street Address _____

Address Line 2 _____

City _____

State AL _____ Zip Code _____

Specific Invoicing Requests *(cost centers, delivery method, etc.)*:

_____

_____

Name _____

Title _____

Email _____

Phone _____

Street Address _____

Address Line 2 _____

City _____

State AL _____ Zip Code _____

Specific Invoicing Requests *(cost centers, delivery method, etc.)*:

_____

_____

Please list your primary contacts for the following:

Implementation _____

_____

Implementation escalation _____

_____

Accounting and general ledger _____

_____

Compliance _____

_____

Risk and performance _____

_____

Systems Information

What is your current ERP system (for example: SAP, Oracle, PeopleSoft, etc.)? _____

What system do you use for your treasury work station (for example: Wallstreet Office, Kyriba, Orbit, etc.)?

_____

Please provide an approximate overall asset value for your entire portfolio that is expected to be reported on by Clearwater over the next 12 months.

_____

NOTE: All items with an asterisk* represent Clearwater default settings. Please select one option for each setting. If no selection is made, Clearwater will apply the default.

Please contact your account manager with questions about these guidelines.

©Clearwater Analytics, LLC 2016

Lot Inventory Method

Please select the inventory method for selection of lots for disposal:

- ○ First-in-first-out *(FIFO)**
- ○ Last-in-first-out *(LIFO)*
- ○ Average cost
- ○ High-cost *(book value)*
- ○ Low-cost *(book value)*

To address situations where different costs or trade dates across bases exist, please indicate the accounting basis the inventory method should be based on. If left blank, the default basis will be GAAP. _____

Asset-Specific Inventory Method Overrides

Clearwater has found that for certain asset classes, the broker may have a different lot inventory method than clients standard reporting. Having Clearwater align to the broker's inventory method on derivatives is critical to daily margin reconciliation.

Specifically, we have found that a number of brokers want to close out lots that are opened and relieved on the same day.

Top day for futures (do you want to close any lots opened on the same day first)?

○ Yes ○ No

If you have elected a different inventory method above, use FIFO for futures?

○ Yes ○ No

Period-End Settings

What is your expected book-of-record conversion month (for example, if October was selected, you would book October entries in November)?

_____

What is your fiscal calendar? _____

Do you have a different calendar for performance reporting?

○ Yes ○ No

If yes, what is your performance reporting calendar?

_____

What business day after the period-end close do you want reports locked down?

_____

Do you file 13F? ○ Yes ○ No

Currency Settings

Do you have multi-currency investments?

○ Yes ○ No

What is the functional (base) currency for the majority of your portfolio? We will request account-specific functional currencies on the account list.

_____

What balance sheet rate source should Clearwater use?

- ○ New York EOD *(provided by Reuters)**
- ○ London EOD *(provided by Reuters)*
- ○ Client-provided
- ○ Other

What activity rate source should Clearwater use?

- ○ New York EOD *(provided by Reuters)**
- ○ London EOD *(provided by Reuters)*
- ○ Client-provided
- ○ Other

Market Valuation Daily Source

Clearwater uses a client-defined pricing hierarchy for daily market valuation of your portfolio. Clearwater's pricing process will walk through the below defined hierarchy and set the daily market price based on the source to first provide a price. **> Download more information here.**

Pricing Overrides*: client-provided prices for securities that cannot be priced by the custodian or S&P and can be updated periodically

Clearwater Calculated Prices: Clearwater calculates or assigns a market price for the following:

- CP and CDs' market price is calculated by accreting the purchase price to face value at maturity
- Money market funds are priced at 1
- Repurchase agreements and auction rate securities are priced at par

S&P Capital IQ: pricing received directly from S&P, a leading provider of multi-asset class and real-time pricing on a daily basis

Account Source: the custodian or safekeeping institution's price received in the daily feed sent to Clearwater

Clearwater strongly recommends the first two positions in the pricing hierarchy are set as follows for all clients:

1. Pricing Overrides 2. Clearwater Calculated Prices

©Clearwater Analytics, LLC 2016

The options below allow clients to specify the remaining hierarchy that Clearwater will select the first available price from.

Please chose your preferred pricing hierarchy between S&P Capital IQ and Account Source:

- ○ (3) S&P Capital IQ, (4) Account Source*
- ○ (3) Account source, (4) S&P Capital IQ

In addition to the above hierarchy, Clearwater can use iMoneyNet for floating NAV and/or asset manager pricing. Please elect if you would like to include one or both of these in your hierarchy:

- ☐ Use iMoneyNet for floating NAV MMF first *(will be above Clearwater calculated)**
- ☐ Use asset manager pricing

If using asset manager pricing, please indicate what source from the above options it should precede

Average Credit Rating Considerations

Credit ratings pertain to the calculation of average credit rating for the portfolio. Average credit rating can be calculated two ways on the Clearwater system (simple and complex).

The complex method for calculating average credit rating involves taking the weighted average rating applied to each security with an exponential credit rating schedule (AAA=1, AA+=10, AA=20, AA=40, ...).

The simple method for calculating average credit rating involves taking the weighted average of ratings applied to each security with a linear credit rating schedule (AAA=1, AA+=2, AA=3, AA-=4, ...).

Please select the average credit rating calculation method you would like applied to your portfolio.

○ Complex* ○ Simple

Minimum number of ratings required for portfolio average rating (securities that do not meet the minimum number of ratings will receive the lowest weight; selecting "none" will exclude securities with NA/NR ratings from the average credit rating for the portfolio):

○ None* ○ One
○ Two ○ Three

Clearwater provides ratings from S&P, Moody's, Fitch, and DBRS. Please select the rating(s) you would like to be used for your average credit rating calculation.

- ○ Lower of S&P and Moody's*
- ○ Second Lowest NAIC Method: S&P, Moody's, Fitch, and DBRS* *(Clearwater default setting **recommended for STAT**)*
- ○ Lower of S&P, Moody's, and Fitch
- ○ Lower of S&P, Moody's, DBRS, Fitch
- ○ Higher of S&P, Moody's, DBRS, Fitch
- ○ Higher of S&P, Moody's, and Fitch
- ○ Higher of S&P and Moody's
- ○ Higher of DBRS and S&P
- ○ S&P only ○ Moody's only
- ○ Fitch only ○ DBRS only
- ○ Second Lowest: S&P, Moody's, and Fitch*
- ○ Barclay Index Methodology: uses all sources. If there are three ratings, take the middle rating; if there are two ratings, take the lower rating; and if there is one rating, use it. If there are no ratings, it is considered not rated.
- ○ Canadian Insurance Regulation: uses DBRS, Moody's, and S&P only. If there are three ratings, take the middle rating; if there are two ratings, take the lower rating; and if there is one rating, use it. If there are no ratings, it is considered not rated.

Some data providers may require additional licensing agreements. Clearwater will notify clients if this occurs. **> Download more information about the average credit rating calculation here.**

Option Cost Assignment

When an option is exercised, how do you want Clearwater to assign the cost?

- ○ No assignment*
- ○ Gain to the option

Insurance-Specific Questions

(may not apply to all clients)

What annual reporting software do you use for uploading your NAIC filings? _____

What is your current/previous Schedule D provider?

_____

©Clearwater Analytics, LLC 2016

What quarter would you like to first use Clearwater statements for your NAIC/Schedule D filing?

○ Q1 ○ Q2 ○ Q3 ○ Q4

Are your state deposit investments shadow-posted through your primary custodian?

○ Yes ○ No

Should Clearwater request pricing and designations from the NAIC Security Valuation Office (SVO) as an authorized third-party administrator on your behalf? For Clearwater to provide this, Clients will be required to maintain a direct contract with the SVO.

☑ **Yes:** for pricing and designations, Clearwater will use NAIC-provided prices (when available) for quarter- and year-end pricing (applies to all GAAP, STAT and NAIC reports). Designations will be requested monthly. Clearwater will be responsible for filing missing designation requests with the NAIC.

☑ **Yes:** for designations only. Designations will be requested monthly. Clients will be responsible for filing missing designation requests with the NAIC.

☑ **No:** Clearwater will use your daily pricing source for quarter- and year-end pricing (applies to all GAAP, STAT, and NAIC reports) and not request designations from the SVO.

Should Clearwater request price points for modeled securities (structured securities, 43R, RMBS/CMBS, etc.) from the SVO as an authorized third-party administrator on your behalf? For Clearwater to provide this, clients will be required to maintain a direct contract with the SVO.

○ Yes ○ No

For life insurance companies, what are your AVR and IMR tax rates as of the prior-year-end?

AVR _____

IMR _____

©Clearwater Analytics, LLC 2016

Basis-Specific Account Settings

clearwater

The elections provided in this document are used to drive the accounting values from each reporting basis. Clearwater requires a Basis-Specific Account Settings form for each reporting basis.

Please indicate what accounting basis these elections are for:

☐ GAAP ☐ STAT ☐ Tax ☐ IFRS
☐ Other _____

Portfolio Classification

Consolidation Entity for Transfers

Please define what accounts (based on common grouping) Clearwater should use to determine if security transfers are intra or inter entity. This means they will automatically process at book value (intra) or market value (inter). Clearwater will gather the specific details on the account list.

GAAP would generally reference GL reporting entity, STAT would generally reference GL reporting entity or NAIC entity, and Tax would generally reference tax legal entity.

Mark-to-Market Category

Clearwater can support M2M/MTM categories with guidance for FAS115/IAS 39/IFRS 9. If multiple categories exist, please indicate the primary category. We will request account-specific categories on the account list. Note: this selection does not apply to STAT basis. Note: this selection does not apply to STAT basis.

Trading/Fair Value Through Profit or Loss (FVPL) portfolio accounting designation applies to investing where securities are purchased for short-term appreciation. Each period, unrealized gains and losses are recognized through holding gain/loss and flow through the income statement.

Held to Maturity (HTM)/Amortized Cost portfolio accounting designation applies to investing with the intent and ability to hold securities to maturity. Unrealized gains and losses are not recognized as long as the company expects to receive full face value of the security.

Available for Sale (AFS) Fair Value Through Other Comprehensive Income (FVOCI) portfolio accounting designation applies to any company not falling into Trading or Held to Maturity investing. AFS is categorized by low turnover but a willingness to sell if the situation demands it. Changes in unrealized gains and losses are recorded to Other Comprehensive Income (OCI) each period for AFS portfolios.

Please select the FAS 115/IAS 39 category that best matches your portfolio's investment style:

☐ Available for Sale *(FVOCI)** ☐ Trading *(FVPL)*
☐ Held to Maturity *(Amortized Cost)*

Changing guidance, GAAP (2019), and IFRS (2018) will require equities to be considered as Trading (FVPL). Do you consider your equities as Trading?

☐ Yes* *(suggested default for IFRS)*
☐ No* *(suggested default for GAAP)*

Are there any other exceptions? If yes, please explain:

☐ Yes _____
☐ No

Balance Sheet Classification Assumptions

Securities will be classified on the balance sheet as cash and cash equivalent, short-term, and long-term. Clients can combine short- and long-term assets into a marketable securities grouping bucket within the general ledger if required. Additional classifications by basis can be made by selecting the appropriate options below:

The number of days used to categorize cash and cash equivalents, short-term, and long-term will be based on using:

☐ Trade date* ☐ Settle date

NOTE: All items with an asterisk* represent Clearwater default settings. Please select one option for each setting. If no selection is made, Clearwater will apply the default.

Maturity date used to classify investments on the balance sheet will be based on the (this does not affect STAT classifications):

- ☐ Final maturity date*
- ☐ Effective maturity date (original fully repaid date)

Cash and cash equivalents are defined as securities with an original maturity less than or equal to:

☐ 90 days* ☐ 91 days ☐ Other _____

Security Type Classification Settings

Variable Rate Demand Notes *(VRDNs)* should be classified as:

- ☐ Calculate using time from purchase to maturity*
- ☐ Cash equivalent ☐ Short-term ☐ Long-term

Auction Rate Securities *(ARNs)* should be classified as

- ☐ Calculate using time from purchase to maturity*
- ☐ Cash equivalent ☐ Short-term ☐ Long-term

Money market funds can be classified as cash equivalent or short-term investments. Please select the classification you would like applied for money market funds for any basis other than STAT, which will follow NAIC guidance.

☐ Cash equivalent* ☐ Short-term

GAAP guidance allows for long-term securities to reclassify to short-term when they are one year from their maturity date. Please select if you would like to reclassify long term assets one year from maturity. STAT classifications will follow STAT guidance. Selecting "maintain original classification" will allow you to keep you GAAP and STAT classifications aligned.

- ☐ Move to short-term*
- ☐ Maintain original classification*
  (suggested default for STAT only)

Amortization

Static Assumptions (cannot be changed)

When using constant-yield, prepaying securities are amortized/accreted to the fully repaid date.

Callable securities (excluding loan-backed securities) purchased above par (100) and above the premium call price are amortized to the next call date at the premium call price. If market conditions change and the security is not called, the security will continue to amortize to par.

For STAT basis reporting, premiums will amortize according to the yield-to-worst guidance per *SSAP 26*.

Callable securities purchased above par (100) but below the premium call price are amortized to the final maturity date at par. Callable securities purchased below par are accreted to the legal final maturity date.

The following security types will follow straight line amortization: agency discount notes, commercial paper, time deposits, certificates of deposit, and variable rate. Selecting "No Amortization" is the only setting that will override static assumptions.

Please select the amortization method Clearwater is to apply to the accounts:

☐ Constant Yield* ☐ Straight Line
☐ No Amortization

When using straight-line amortization, loan-backed securities purchased at a premium are amortized to the following static maturity date:

☐ Full Repaid Date ☐ Final Maturity Date*

When using straight-line amortization, loan-backed securities purchased at a discount are amortized to the following static maturity date:

☐ Full Repaid Date ☐ Final Maturity Date*

When using Constant Yield Amortization, adjustments to the amortization schedule for prepaying and loan-backed securities can be:

Retrospective: recalculating the amortization curve as of the purchase date based on new cash flows and adjusting to the newly calculated curve

Prospective: recalculating the amortization curve from adjustment date forward based on new cash flows and adjusts to the new rate of amortization moving forward

None: maintaining the original amortization curve for the life of the security

Guidance for US GAAP (FAS91) prefers retrospective or none.

STAT guidance on 43R adjustments allows for only retrospective or prospective on a monthly or quarterly basis.

Tax does not take an adjustment and defaults to "None" regardless of other basis elections.

Please select the amortization adjustment method and frequency you would like applied:

- ☐ Retrospective Quarterly* ☐ Prospective Quarterly
- ☐ Retrospective Monthly ☐ Prospective Monthly
- ☐ Retrospective Annually ☐ Prospective Annually
- ☐ None

When the book price for units disposed due to a paydown is not 100 or the units pre-paid are less than the factor change due to a principal loss, the difference should be taken through:

☐ Realized Gain/Loss ☐ Amortization/Accretion*

Some reporting guidance requires that amortization schedules ignore call and put dates. Please indicate if the elected basis should ignore call and put dates and calculate to final maturity on callable securities:

☐ Yes* *(required default for financial institutions)*
☐ No

Do you take an annual mark-to-market adjustment (revaluation of the book value to market value)?

☐ No* ☐ Yes—first day of the year
☐ Yes—last day of the year

Prepayment assumptions for fixed rate agency mortgage-backed securities are determined using constant prepayment rates obtained from a broker-dealer survey. Prepayment assumptions for other loan-backed and structured securities are obtained from an outside vendor using a model/scenario based on the current interest rate and economic environment. Additional information regarding Clearwater's prepayment speed selection for MBS securities can be found here.

FX Unrealized Accrued Holding Gain/Loss

Should unrealized gains/losses on accrued due to changes in FX rates be attributed to OCI or net income (treat accrued as a monetary asset)?

☐ OCI ☐ Net Income

Tax-Specific Amortization Options
(will only apply to Tax basis)

Tax Deferral Percent

What percentage of unrealized gains/losses do you want deferred to your differed tax asset account for your GAAP ledger?

Should accretion on non-OID securities purchased at a discount be taken through income?

☐ Yes ☐ No*

By default, if a market discount is de minimis, Clearwater will not accrete the discount (i.e. defer the accretion) and therefore recognize any gain or loss at disposal as a capital gain or loss. Should the market discount be accreted, even in instances that the market discount at purchase is de minimis?

☐ Yes ☐ No*

Clearwater can turn off premium amortization on all securities in the tax basis only so that when a security is disposed, the difference between the purchase cost and disposal price will be a capital gain or loss. Please indicate if Clearwater should disable premium amortization in the tax basis:

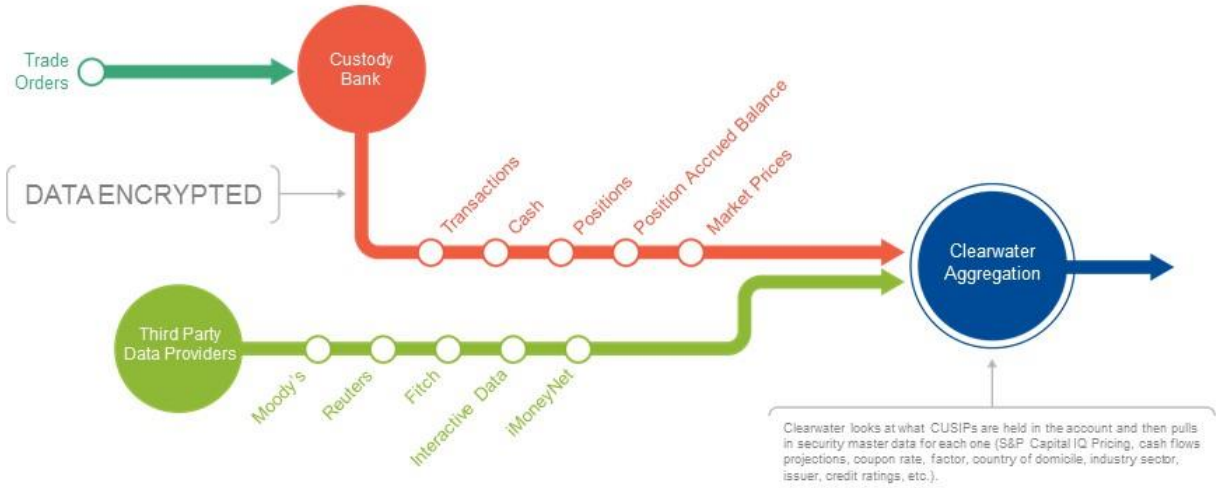
☐ Yes ☐ No*

clearwater

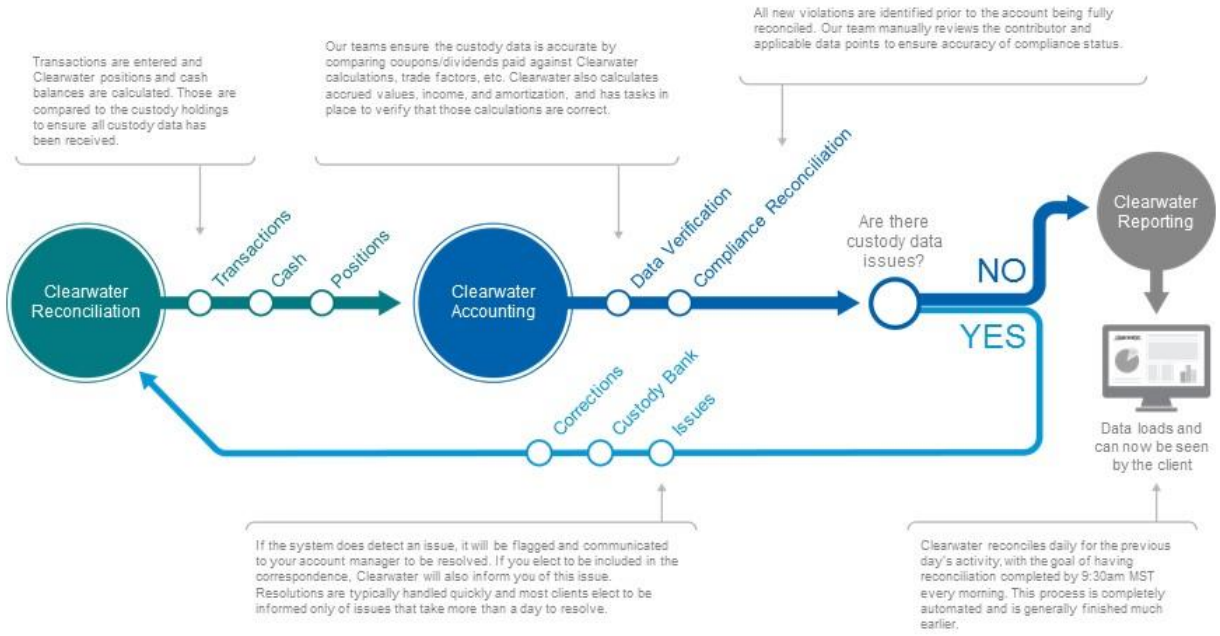
Appendix B

Illustration of Clearwater's reconciliation process.

Daily Reconciliation



clearwater



clearwater