

SYSTEM AND ORGANIZATION CONTROLS (SOC) FOR SERVICE ORGANIZATIONS SOC 2® Type 1



AUDITWERX

A DIVISION OF
CARR, RIGGS & INGRAM CAPITAL, LLC

[AUDITWERX.COM](https://auditwerx.com)

REPORT ON

AXOS CLEARING LLC'S

DESCRIPTION OF ITS CLEARING AND CUSTODIAN
SERVICES AND ON THE SUITABILITY OF THE
DESIGN OF ITS CONTROLS RELEVANT TO
SECURITY AND AVAILABILITY

AS OF

June 30, 2022

TABLE OF CONTENTS

SECTION 1: INDEPENDENT SERVICE AUDITORS' REPORT	3
SECTION 2: AXOS CLEARING LLC'S ASSERTION	8
SECTION 3: AXOS CLEARING LLC'S DESCRIPTION OF ITS CLEARING AND CUSTODIAN SERVICES	10
COMPANY OVERVIEW	11
SERVICES OVERVIEW	11
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS	11
SCOPE OF THE DESCRIPTION	12
COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES	12
RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, CONTROL ACTIVITIES, INFORMATION AND COMMUNICATION, AND MONITORING	19
CONTROL ENVIRONMENT	19
RISK ASSESSMENT PROCESS	21
CONTROL ACTIVITIES	21
INFORMATION AND COMMUNICATION	22
MONITORING	22
COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS	23
COMPLEMENTARY USER ENTITY CONTROLS	23
SECTION 4: TRUST SERVICES SECURITY AND AVAILABILITY CRITERIA, RELATED CONTROLS AND RESULTS ..	24
INFORMATION PROVIDED BY AUDITWERX	25
COMMON CONTROL CRITERIA – SECURITY AND AVAILABILITY	26
CC1.0 CONTROL ENVIRONMENT	26
CC2.0 COMMUNICATION AND INFORMATION	28
CC3.0 RISK ASSESSMENT	30
CC4.0 MONITORING ACTIVITIES	32
CC5.0 CONTROL ACTIVITIES	33
CC6.0 CONTROL ACTIVITIES – LOGICAL & PHYSICAL ACCESS	35
CC7.0 CONTROL ACTIVITIES – SYSTEM OPERATIONS	38
CC8.0 CONTROL ACTIVITIES – CHANGE MANAGEMENT	40
CC9.0 RISK MITIGATION	42
ADDITIONAL CRITERIA FOR AVAILABILITY	43



SECTION 1: INDEPENDENT SERVICE AUDITORS' REPORT



INDEPENDENT SERVICE AUDITORS' REPORT

To: Axos Clearing LLC

Scope

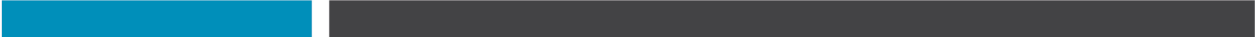
We have examined Axos Clearing LLC's ("Axos Clearing") accompanying description of its Clearing and Custodian Services found in Section 3 titled "Axos Clearing LLC's Description of its Clearing and Custodian Services" as of June 30, 2022 ("description") based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria") and the suitability of the design of controls stated in the description as of June 30, 2022, to provide reasonable assurance that Axos Clearing's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Axos Clearing uses subservice organizations to provide application and data cloud hosting and data center services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Axos Clearing, to achieve Axos Clearing's service commitments and system requirements based on the applicable trust services criteria. The description presents Axos Clearing's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Axos Clearing's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Axos Clearing, to achieve Axos Clearing's service commitments and system requirements based on the applicable trust services criteria. The description presents Axos Clearing's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Axos Clearing's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Axos Clearing LLC's Responsibilities

Axos Clearing is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Axos Clearing's service commitments and system requirements were achieved. In Section 2, Axos



Clearing has provided the accompanying assertion titled “Axos Clearing LLC’s Assertion” (“assertion”) about the description and the suitability of the design of controls stated therein. Axos Clearing is also 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; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization’s service commitments and system requirements.

Auditwerx’s Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. 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 of controls involves—

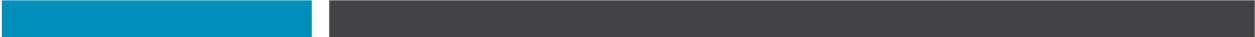
- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider



important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects—

- a. the description presents Axos Clearing's Clearing and Custodian Services that was designed and implemented as of June 30, 2022 in accordance with the description criteria.
- b. the controls stated in the description were suitably designed as of June 30, 2022 to provide reasonable assurance that Axos Clearing's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Axos Clearing's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Axos Clearing, user entities of Axos Clearing's Clearing and Custodian Services as of June 30, 2022, business partners of Axos Clearing subject to risks arising from interactions with the Clearing and Custodian Services, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than the specified parties.

Auditwerx, LLC

Auditwerx, LLC, a Division of Carr, Riggs & Ingram Capital, LLC

Tampa, Florida

November 4, 2022



SECTION 2: AXOS CLEARING LLC'S ASSERTION



We have prepared the accompanying description of Axos Clearing LLC's ("Axos Clearing") Clearing and Custodian Services titled "Axos Clearing LLC's Description of its Clearing and Custodian Services" as of June 30, 2022 ("description") based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria"). The description is intended to provide report users with information about the Clearing and Custodian Services that may be useful when assessing the risks arising from interactions with Axos Clearing's system, particularly information about system controls that Axos Clearing has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Axos Clearing uses subservice organizations to provide application and data cloud hosting and data center services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Axos Clearing, to achieve Axos Clearing's service commitments and system requirements based on the applicable trust services criteria. The description presents Axos Clearing's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Axos Clearing's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Axos Clearing, to achieve Axos Clearing's service commitments and system requirements based on the applicable trust services criteria. The description presents the service organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.


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

1. The description presents Axos Clearing's Clearing and Custodian Services that was designed and implemented as of June 30, 2022 in accordance with the description criteria.
2. The controls stated in the description were suitably designed as of June 30, 2022 to provide reasonable assurance that Axos Clearing's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Axos Clearing's controls as of that date.

By: /S/ Gary Wiedman

Gary Wiedman
President and Managing Principal

November 4, 2022



SECTION 3: AXOS CLEARING LLC'S DESCRIPTION OF ITS CLEARING AND CUSTODIAN SERVICES



AXOS CLEARING LLC'S DESCRIPTION OF ITS CLEARING AND CUSTODIAN SERVICES

COMPANY OVERVIEW

Axos Clearing LLC ("Axos Clearing" or the "Company") is a wholly owned subsidiary of Axos Securities, LLC ("Securities"), and is an indirect subsidiary of Axos Financial, Inc. (NYSE:AX). The Company is headquartered in Omaha, Nebraska.

SERVICES OVERVIEW

Axos Clearing is a full-service clearing firm and custodian serving introducing broker-dealers (BDs) and registered investment advisors (RIAs). Axos Clearing's services can be generally divided between (1) the clearing and settlement services it offers to BDs; and (2) the custody and related services it offers to RIAs through its Axos Advisor Services (AAS) division. The AAS division provides RIAs with the internally developed Liberty platform for RIAs to manage their customers' accounts, including placing trades. For BDs, Axos Clearing makes available a platform (BETAHost), offered by Refinitiv U.S. LLC, for order entry and to help BDs manage their customers' accounts.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Axos Clearing designs its processes and procedures related to the Clearing and Custodian Services ("System") to meet its objectives. Those objectives are based on the service commitments that Axos Clearing provides, the laws and regulations that govern the provision of the services, and the financial, operational and compliance requirements that Axos Clearing has established for the services.

Service commitments and system requirements are documented and communicated in the clearing and custodian service agreements, as well as in the description of the service offering provided online. Security and availability commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design of the System permits system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Availability of production databases by performing frequent backups.

Axos Clearing establishes operational requirements that support the achievement of security and availability commitments. Such requirements may be communicated in system policies and procedures, system design documentation. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. Policies also include how to carry out specific manual and automated processes required in the operation and development of the System.

SCOPE OF THE DESCRIPTION

This description addresses only Axos Clearing's System provided to user entities and excludes other services provided by Axos Clearing. The description is intended solely for the information and use of Axos Clearing, user entities of Axos Clearing's System as of June 30, 2022, business partners of Axos Clearing subject to risks arising from interactions with the System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators to help them understand the controls that are likely to be relevant to meeting the applicable trust services criteria.

Axos Clearing uses subservice organizations as follows:

- Sungard Availability Services ("Sungard") – data center services for disaster recovery for AAS.
- Amazon Web Services (AWS) – cloud hosting provider for network servers related to the clearing services.
- Refinitiv U.S. LLC ("Refinitiv") – application hosting and managed services, including backups, related to the clearing services.
 - Amazon Web Services (AWS) – cloud hosting provider, outsourced by Refinitiv, for the BETAHost application and supporting infrastructure.

The description includes only the related controls of Axos Clearing and excludes the related controls carved out to the subservice organizations.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

The System description is comprised of the following components:

- *Infrastructure* – The collection of physical or virtual resources that support an overall IT environment, including the physical environment and related structures, IT and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization used to provide the services.
- *Software* – The application programs and IT system software that support application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile, applications, desktop or laptop applications.
- *People* – The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- *Data* – The types of data used by the system, such as transaction streams, files, databases, tables and output used or processed by the system.

- *Procedures* – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

Infrastructure

Advisor Services

Axos Clearing uses Linux machines with IBM iSeries and Palo Alto firewall appliances to support the applications, databases, and infrastructures for AAS. The applications and supporting infrastructure for the AAS side of the business are hosted in the on-site server room located in Omaha, NE. Axos Clearing's IT and security personnel are responsible for the infrastructure components for AAS.

In addition to the firewall, Axos Clearing uses anti-virus and anti-spyware applications to protect systems from viruses.

Axos Clearing's security policies and procedures ensure that computer devices (including servers, desktops, printers, etc.) connected to the Axos Clearing network have proper virus protection software, current virus definition libraries, and the most recent operating system and security patches installed. The IT department verifies that all known and reasonable defenses are in place to reduce network vulnerabilities while keeping the network operating. In the event of a virus threat, the anti-virus system will attempt to delete or quarantine the infected file. If the virus cannot be deleted or quarantined, the infected machine will be disconnected from the network and cleaned manually.

Multiple controls are installed to monitor traffic that could contain malicious programs or code. The internal and external networks are scanned at least monthly for vulnerabilities to expose potential vulnerabilities to the production environments. In addition to the vulnerability scans, penetration tests are performed annually by a third-party vendor. Server operating systems utilize anti-virus and anti-spyware programs. Employee workstation computers have a minimum standard hardware and software configuration.

Clearing Services

The BETAHost application is a purchased application, which is hosted by Refinitiv at AWS. AWS provides the physical security and environmental protection controls, as well as, managed services for the clearing services.

The supporting network infrastructure is hosted on Linux machines within Axos Clearing's AWS environment. Security groups are configured to control external access.

In addition to the security groups, Axos Clearing uses AWS GuardDuty to protect against malicious attacks.

Physical Security and Environmental Controls

Advisor Services

The AAS production environment is housed on-site in Centennial, CO, and is secured by an access control system (ACS). Access to the on-site server room is restricted to authorized and appropriate personnel. Physical access requests are documented and administered by IT personnel. Environmental protection systems are installed and receive maintenance at least annually.

Access to the SunGard data center is restricted to authorized individuals. SunGard is responsible for the physical security and environmental protections over the disaster recovery site.

Clearing Services

The BETAHost production application is hosted by Refinitiv. The physical security and environmental protections are the responsibility of their subservice organization, AWS.

The network infrastructure related to the clearing services is hosted within Axos Clearing's AWS environment.

Management obtains and reviews SOC reports annually to monitor the physical security and environmental protection controls in place at Refinitiv and AWS.

Logical Access

Advisor Services

The network, Liberty and TCTrust applications, server, and database access are configured and managed by IT personnel of Axos. The access request process is tracked within a ticketing system. Access is granted by IT personnel after receiving authorization from the user's supervisor and/or manager.

New or modified access to the Systems is granted or changed after the completion of a request in the iCIMS or TPS (transfer, promotions, and separations) portals which are integrated with ServiceNow. When requests are made, a ServiceNow ticket is automatically created and the level of access required is detailed based off the information entered into the iCIMS or TPS portals by the user's supervisor or manager.

Logical access to the Liberty application for client users is managed by Axos Clearing. Client access requests are granted after approval from authorized individuals. Access is controlled via standard user authentication credentials (user ID and password).

Clearing Services

Refinitiv handles the physical hosting and virtual server and database infrastructure management related to the BETAHost production application for the clearing services. Axos Clearing handles the administration of users and establishment of password parameters involved in supporting the

BETAHost application, Axos Clearing AWS environment and internal network. Dedicated firewalls and security groups are used to restrict administrative access to the network and AWS environment. Appropriate firewall rules are in place and security groups configured to restrict access to the network and AWS environment and to limit the possibility of disruptions to customer operations from unauthorized users. Access to the BETAHost application is granted after receiving authorization from the user's supervisor and/or manager.

Software

The primary software systems utilized to manage and support the System includes:

Related Service	Software	Provider	Function
Clearing	BETAHost	Refinitiv	Clearing Services
Advisor	TCTrust	Internally developed	Advisor Services (Liberty backend)
Advisor	Liberty	Internally developed	Advisor Services (frontend for clients)

Related Service	Infrastructure	Operating System
Advisor	Dell servers	Windows
Advisor	IBM P-series servers	AIX
Advisor	RHEL 7/8	Linux
Advisor & Clearing	Desktops and laptops	Windows 10 and MacOS12

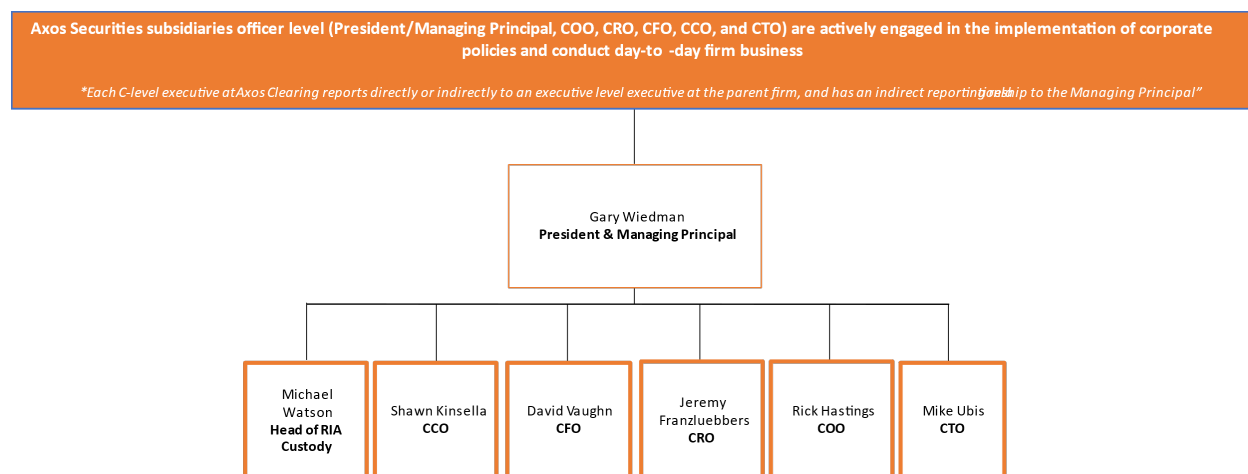
Related Service	Third-Party Software and Services	Function
Clearing	GuardDuty	Intrusion Prevention
Advisor	DellEMC - Avamar	Backups for AAS Services
Advisor	JIRACrowdStrike	Issue Tracking
Advisor	Nagios	Monitoring
Advisor	SolarWinds	Monitoring
Advisor	SAVI	TCTrust Source Code Management
Advisor	Git/GitLab	Liberty Source Code Management
Advisor	Qualys	Vulnerability Management
Advisor & Clearing	CrowdStrike	Cloud antivirus and threat intelligence monitoring
Advisor & Clearing	Defense Storm	Incident Management; Security Logging
Advisor & Clearing	Cyberhaven	Data Loss Prevention
Advisor & Clearing	Axway Security Transport	SFTP
Advisor & Clearing	Palo Alto	Firewall for AAS Services
Advisor & Clearing	OpenVPN	Virtual private network
Advisor & Clearing	ServiceNow	Support Tracking

People

Axos Clearing employs dedicated team members to handle major product functions, including operations, and support. The IT Team monitors the environment, as well as manages data backups and recovery for AAS. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep Axos Clearing and its data secure.

Axos Clearing is led by the President and Managing Principal who assigned authority and responsibility by Axos Financial President and CEO. Key management personnel are selected based on their skills and experience to ensure they can carry out necessary assignments. Such assignments commonly relate to achieving corporate objectives, oversight of operating functions, and any compliance with applicable regulatory requirements. Open dialogue and individual initiative are encouraged as fundamental parts of Axos Clearing's goal to deliver client service.

The following organizational chart depicts the Axos Clearing corporate structure.



President and Managing Principal - The President of Clearing is the head of management, provides leadership, and leads efforts related to defining strategies, roadmaps, and the Company's direction to increase operational efficiencies, manage costs, and scale strategies. The President develops relevant strategic plans and proposals and is responsible for managing the operational model and evolving the technology offerings to support new business lines and initiatives.

Head of RIA Custody - The Head of RIA Custody leads the RIA custody business development, sales, marketing, and implementation strategies to include the business go-to-market value proposition, technology offerings, and operation's needs. This role provides leadership, direction, and partnership to establish operational efficiencies, manage costs, and scale the business.

Chief Compliance Officer (CCO) – The CCO is responsible for managing and directing compliance-related functions and Privacy to ensure that the Company meets regulatory requirements related to the products and services offered by Clearing. In addition, the CCO oversees product lifecycles from inception and advises the Company's product teams on compliance matters throughout design, development, and testing.

Chief Financial Officer (CFO) - The CFO directs finance-related initiatives, and activities for the Company's financial accounting and reporting. The CFO heads treasury, accounting, budget, and tax, and is responsible for the financial audit activities for the organization.

Chief Risk Officer (CRO) – The CRO is the head of the Risk organization and is responsible for mitigating risks associated with products and services offered by the Company. The CRO oversees the Market, Credit, and Operational Risk Management, which includes the Risk and Controls Assessment processes to ensure that the control environment is appropriate and within the Firm's risk appetite.

Chief Operating Officer (COO) – The COO oversees aspects of the Axos Securities business operations, including the development, approval, implementation, and support of Clearing products and services. The COO leads and directs the execution of business plans, the evaluation of progress, and the development of short- and long-term goals. The COO is responsible for operational processes that support the development and establishment of strategy and management for all Clearing-related products and services.

Chief Technology Officer (CTO) - The CTO directs all Information Technology (IT) functions, services, and governance for the Company. The role provides technical leadership in aspects of the Clearing technology business.


Data

Information takes many forms. It may be stored on computers, transmitted across networks, printed or written on paper, and spoken in conversations. Employees of Axos Clearing are obligated to respect and, in all cases, to protect confidential and private data. Customer information, employment-related records, and other intellectual property-related records are, subject to limited exceptions, and are generally confidential as a matter of law. Many other categories of records, including Company and other personnel records, and records relating to Axos Clearing's business and finances are, as a matter of Axos Clearing policy, treated as confidential.

Electronic communications are treated with the same level of confidentiality and security as physical documents. Networks are protected by enterprise class firewalls and appropriate enterprise-class virus protection is in place. Password protection with assigned user rights is required for access to the System. Access to the System is restricted to authorized internal and external users to prohibit unauthorized access to confidential data.

Procedures

Axos Clearing employs a set of procedures in order to obtain the stated objectives for network and data security for both the Company and its clients. The definition and execution of these procedures are performed by trained, qualified, and experienced members of the Axos Clearing team.



Management has developed and communicated the policies and procedures to employees. Reviews and changes to these policies and procedures are performed annually and are approved by senior management. These procedures cover the following key areas:

- Acceptable Use and Business Conduct
- Business Continuity
- Change Control
- Information Security
- Incident Response
- Risk Management

Software Development Life Cycle (SDLC)

For internally-developed software solutions, Axos Clearing uses an agile-based SDLC process, which includes research and planning, analysis and design, initial development, and quality assurance (QA) testing before final release.

Axos Clearing has implemented various technologies to automate its SDLC. GitLab, Git, and SAVI help automate certain aspects of the development process.

Axos Clearing's software solutions follow the bellow procedures:

- Backlog creation
- Sprint planning
- Development
- Quality assurance
- Acceptance
- Release to production

Change Management

Axos Clearing has change control procedures in place to control information resources that require an outage for planned upgrades, maintenance, or fine-tuning. Additionally, unplanned outages may occur that may result in upgrades, maintenance, or fine-tuning. The purpose of the change control procedures is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require forethought, monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information Resources. The Axos Clearing change control procedures apply to individuals who install, operate, or maintain Information Resources.

Patch Management

For the AAS production environment, the Security Operations Team reviews the availability of patches and independently determines if they are necessary to deploy within the production environment. Approved patches are tracked and scheduled for installation in ServiceNow.



Backup and Recovery

Refinitiv is responsible for maintaining backups of the BETAHost databases and transactional records for the clearing services.

Axos Clearing maintains daily database backups for AAS. Backups are encrypted and stored on-site in the dedicated backup servers. The subservice organization, Sungard, is utilized for disaster recovery.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, CONTROL ACTIVITIES, INFORMATION AND COMMUNICATION, AND MONITORING

CONTROL ENVIRONMENT

The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal controls across an organization. The organizational structure, separation of job responsibilities by departments and business function, documentation of policies and procedures, and internal audits are the methods used to define, implement, and assure effective operational controls. Senior management establishes the tone at the top regarding the importance of internal controls and expected standards of conduct.

Management Philosophy


Management is responsible for directing and controlling operations, establishing, communicating, and monitoring control policies and procedures, as well as setting the tone for the organization. Importance is placed on accuracy and integrity, maintaining written and updated procedures, security, and establishing and maintaining sound internal controls over all functional aspects of operations.

Management's philosophy and operating style affect the way the Company is managed, including the kinds of business risks accepted. Axos Clearing places a great deal of importance on working to ensure that the integrity of processing is a primary focus and that controls are maximized to mitigate risk in daily operations. Management and specific teams are structured to ensure the highest level of integrity and efficiency in customer support and transaction processing.

Formal job descriptions and departmental meetings and staff interactions ensure communication of organizational values, ethics, and behavior standards. Personnel operate under Axos Clearing's policies and procedures, including confidentiality agreements and security policies. Annual training is conducted to communicate regulations and the importance of security. Management is committed to being aware of regulatory and economic changes that impact lines of business and monitoring the customer base for trends, changes, and anomalies.

Hiring and Termination Practices

Axos Clearing has standardized business conduct and ethics policies and procedures across locations. The result is a uniform set of practices that provide equitable hiring and advancement opportunities across the organization.



Axos Clearing requires potential candidates to submit an employment application that includes education, professional experience, and certifications. Background investigations are performed for new employees and include criminal fingerprint background checks and drug screening.

New employees are provided with the Employee Handbook, Master Policy on Ethics and Professional Integrity, and the Confidentiality Agreement. The Employee Handbook includes policies on professional standards, confidentiality, conflicts of interest, and trade secrets. New employees are required to sign an acknowledgement of receipt and understanding of the Master Policy on Ethics and Professional Integrity, the Employee Handbook, and the Confidentiality Agreement. Additionally, the Master Policy on Ethics and Professional Integrity is reaffirmed annually. Employees are also given access to the Company's security related policies covering the topics outlined in the Procedures section of this document and are required to sign an acknowledgement form indicating they have received and understand the Acceptable Use Policy.

Performance reviews are expected to be conducted semi-annually by the employee's manager to discuss expectations, goals, and improvement plans.

Training and Supervision

New employees are trained on the specific duties and responsibilities of their respective positions. During training, employees become familiar with Axos Clearing's policies and procedures including those related to their specific position and to Axos Clearing in general. When changes to policy are made, employees are supplied with copies of the amended policy. Axos Clearing policies pertain to confidentiality, information security, personal behavior, rules of conduct, and regulatory guidelines. Policies state that employees are prohibited from divulging confidential information regarding client affairs or taking action not in the interests of the client or Axos Clearing.

Training of personnel for specific job-related duties is accomplished through supervised on-the-job training. Positions require completion of specific training before working independently on behalf of clients. In-house promotion with additional responsibilities within a service group or with another group is dependent on the understanding of the responsibilities of the current position and the proper performance of the duties of that position.

Security Awareness

Axos Clearing conducts security training programs for employees in the areas of security and availability. Employees are required to attend security awareness training upon hire and annually thereafter. Each member of the Company is made aware of the security implications that revolve around their functions and actions. Approaching security as an organization has a more profound effect than relying solely on a single group.

RISK ASSESSMENT PROCESS

Risk assessment involves a dynamic iterative process for identifying and analyzing risks to achieving an organization's objectives, forming a basis for determining how risks should be managed. Management considers possible changes in the external environment and within its own organization that may impede its ability to achieve its objectives.

Business Risks

Axos Clearing management members, both individually and collectively, have an ongoing responsibility to monitor risk. Management is responsible for identifying and analyzing the risks relative to the achievement of its objectives through the use of information derived from various sources, such as:

- Management input,
- Previous monitoring activity and/or audit results,
- Industry experience and knowledge,
- Feedback obtained from clients,
- Business/external environment, and
- Planned system and process changes.

Risk Mitigation

In addition to assessing risk, management is responsible for mitigating risks. Risk mitigation strategies include prevention, mitigation, and detection through the implementation of internal controls and transference through commercial general and umbrella insurance policies. Management takes various steps, including items described in other sections herein, to mitigate risk. For instance, management is responsible for making decisions to ensure that the internal network and the sensitive data stored there is securely protected from unauthorized access; many of the steps taken to mitigate these risks are described in the other sections of this document.


CONTROL ACTIVITIES

Control activities are the actions established by policies and procedures to help ensure that management directives to mitigate risks to the achievement of objectives are executed. Control activities are performed at all levels of the organization and at various stages within business processes, and over the technology environment.

Trust Services Categories, Criteria, and Related Controls

The security and availability categories, and applicable trust services criteria were used to evaluate the suitability of design of controls stated in the description. Criteria and controls designed, implemented, and operated to meet them ensure that the system:

- Security – is protected against unauthorized access (both physical and logical).
- Availability – is available for operation and use.



The Company's trust services criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them here in Section 3 and repeating them in Section 4. Although the trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Axos Clearing's description of controls.

For specific criterion, which was deemed not relevant to the system, see Section 4 for related explanation.

INFORMATION AND COMMUNICATION

Information is necessary for the Company to carry out internal control responsibilities in support of achievement of its objectives. Communication occurs both internally and externally and provides the Company with the information needed to carry out day-to-day controls. Communication enables personnel to understand internal control responsibilities and their importance to the achievement of the objective.

Axos Clearing uses a variety of methods for communication to ensure that significant events and issues are conveyed in a timely manner and that staff understand their role and responsibility. These methods include new hire training, ongoing training, policy and procedure updates, use of email to communicate time-sensitive information, and the documentation and storage of historical data in internal repositories for business and support activities. Additional communication methods include periodic department meetings between each manager and their staff to discuss new Company policies, procedures, and other business issues, electronic mail messages, and the posting of information via corporate intranet on topics such as reporting of information security incidents and procedures for change management. Communication is encouraged at all levels to promote the operating efficiency of Axos Clearing.

MONITORING

Ongoing evaluations, separate evaluations or some combination of the two are used to ascertain whether each of other components of internal control is present and functioning. Findings are evaluated and deficiencies are communicated in a timely manner, with serious matters reported to senior management, as deemed appropriate.

Monitoring of the Subservice Organization

Management of Axos Clearing receives and reviews the SOC reports of Refinitiv, AWS, and Sungard on an annual basis. In addition, through its daily operational activities, management of Axos Clearing monitors the services performed by Refinitiv, AWS, and Sungard to ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

Controls related to the System cover only a portion of overall internal control for each user entity of Axos Clearing. It is not feasible for the trust services criteria related to the System to be achieved solely by Axos Clearing. Therefore, each user entity's internal controls should be evaluated in conjunction with Axos Clearing's controls and the related tests and results described in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Complementary Subservice Organization Controls (CSOC)	Related Criteria
Sungard is responsible for maintaining physical security and environmental protection controls over its data center which hosts the AAS disaster recovery system.	CC6.4 A1.2
AWS (network environment) is responsible for maintaining physical security, including the disposal of physical assets, and environmental protection controls over its data center which hosts network servers related to the clearing services.	CC6.4, CC6.5
Refinitiv is responsible for maintaining the servers and databases used to host the BETAHost application and client data, as well as backups of client data.	CC6.1, CC6.6, CC6.7 CC6.8, CC7.1, CC8.1 A1.2
AWS (Refinitiv subservice organization) is responsible for maintaining physical security, including the disposal of physical assets, and environmental protection controls over its data center which hosts the BETAHost application and supporting infrastructure for the clearing services.	CC6.4, CC6.5 A1.2

COMPLEMENTARY USER ENTITY CONTROLS

Controls related to the System cover only a portion of overall internal controls for each user entity. It is not feasible for the trust services criteria related to the System to be achieved solely by Axos Clearing. Therefore, the ability of each user entity's internal controls should be evaluated in conjunction with Axos Clearing's controls and the related tests and results described in Section 4 of this report, taking into account the related complementary user entity controls identified below. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal controls to determine whether the identified complementary user entity controls have been implemented and are operating effectively.

User entities should consider whether the following controls have been placed in operation to provide reasonable assurance that:

- Access to the BETAHost and Liberty applications is requested by appropriately authorized personnel and requests are submitted timely for user access changes. (CC6.1,CC6.2,CC6.3)



SECTION 4: TRUST SERVICES SECURITY AND AVAILABILITY CRITERIA, RELATED CONTROLS AND RESULTS



TRUST SERVICES SECURITY AND AVAILABILITY CRITERIA, RELATED CONTROLS, AND RESULTS

INFORMATION PROVIDED BY AUDITWERX

Axos Clearing's internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by Axos Clearing. In planning the nature, timing, and extent of our testing of the controls to achieve the service commitments and system requirements based on the applicable trust services criteria, we considered aspects of Axos Clearing's control environment, risk assessment process, monitoring activities, and information and communications.

In addition, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

COMMON CONTROL CRITERIA – SECURITY AND AVAILABILITY

CC1.0 CONTROL ENVIRONMENT

Ref. #	Client Controls	Results
CC1.1 - The entity demonstrates a commitment to integrity and ethical values.		
CC1.1.1	<p>Established policies and procedures, which outline operating practices and business conduct for Axos Clearing personnel, are reviewed annually.</p> <p>The policies and procedures include the following:</p> <ul style="list-style-type: none"> • Code of Business Conduct and Ethics • Code of Ethics (for top management) • Employee Handbook • Master Policy on Ethics and Professional Integrity 	No deviations noted.
CC1.1.2	Employees are required to read and accept the Master Policy on Ethics and Professional Integrity upon hire and annually thereafter.	No deviations noted.
CC1.1.3	Employees are required to read and accept the Employee Handbook and sign a Confidentiality Agreement upon hire.	No deviations noted.
CC1.1.4	Management monitors personnel compliance with the Company's integrity and ethical standards through monitoring of customer and workforce member complaints and the use of an anonymous third-party administered ethics hotline. The Code of Ethics, Employee Handbook, and Master Policy on Ethics and Professional Integrity include a sanctions policy for personnel who violate the policy.	No deviations noted.
CC1.2 - The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
CC1.2.1	Axos Clearing does not have a Board of Directors. In lieu of a Board of Directors, executive management exercises oversight of the development and performance of internal control.	No deviations noted.

Ref. #	Client Controls	Results
CC1.3 - Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
CC1.3.1	An organizational structure is in place to establish and communicate key areas of authority, responsibility, and appropriate lines of reporting. The organizational structure is updated real-time via the HR management system.	No deviations noted.
CC1.3.2	Roles and responsibilities of key managers are defined in the policies and procedures including duties such as proper oversight, management, and monitoring of vendor, security and availability activities.	No deviations noted.
CC1.4 - The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
CC1.4.1	Candidates' abilities to meet job requirements are evaluated as part of the hiring process.	No deviations noted.
CC1.4.2	Active employees' abilities to meet job requirements are evaluated as part of the semi-annual performance review process.	No deviations noted.
CC1.4.3	Management establishes continued training and monitors completion of security training programs upon hire and at least annually.	No deviations noted.
CC1.4.4	Prior to employment, personnel are verified against regulatory screening databases, including criminal background checks and drug screenings.	No deviations noted.
CC1.5 - The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
CC1.5.1	Active employees' abilities to meet job requirements are evaluated as part of the semi-annual performance review process.	No deviations noted.

CC2.0 COMMUNICATION AND INFORMATION

Ref. #	Client Controls	Results
CC2.1 - The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
CC2.1.1	<p>Established policies and procedures, which outline operating practices and business conduct for Axos Clearing personnel, are reviewed annually.</p> <p>The policies and procedures include the following:</p> <ul style="list-style-type: none"> • Acceptable Use Procedure • Business Continuity Policy • Change Control Management • Enterprise Data Governance • Incident Response • Information Security Policy • Privacy Policy • Risk Assessment Policy • Risk Management Policy • Security Standard • Software Acquisition • Software Development • Vendor Management 	No deviations noted.
CC2.1.2	On a quarterly basis, management meets to assess the Company's strategic plan and budget, which identifies the information required and expected to support the internal control and achievement of service commitments and system requirements.	No deviations noted.
CC2.2 - The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
CC2.2.1	Policy and procedure documents for significant processes that address system requirements for incident response and designing, developing, implementing, operating, maintaining, and monitoring controls are provided to personnel via the SharePoint Site to carry out their responsibilities.	No deviations noted.
CC2.2.2	Employees are required to read and accept the Acceptable Use Policy upon hire.	No deviations noted.

<i>Ref. #</i>	<i>Client Controls</i>	<i>Results</i>
CC2.2.3	On a quarterly basis, management meets to assess the Company's strategic plan and budget, which identifies the information required and expected to support the internal control and achievement of service commitments and system requirements.	No deviations noted.
CC2.2.4	System changes are communicated to system users through ongoing communications mechanisms such as email communication.	No deviations noted.
CC2.2.5	Management establishes continued training and monitors completion of security training programs upon hire and at least annually.	No deviations noted.
<i>CC2.3 - The entity communicates with external parties regarding matters affecting the functioning of internal control.</i>		
CC2.3.1	The clearing and custodian service agreements include the system descriptions that delineates the boundaries of the system and system processes that include infrastructure, software, people, processes and procedures, and the data that is captured and is made available to external users of the system.	No deviations noted.
CC2.3.2	The Company posts contact email and phone numbers on its website for customers and other external users to communicate relevant information.	No deviations noted.
CC2.3.3	System changes are communicated to system users via the Company website.	No deviations noted.

CC3.0 RISK ASSESSMENT

Ref. #	Client Controls	Results
CC3.1 - The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
CC3.1.1	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No deviations noted.
CC3.1.2	Management performs an annual risk assessment, based on the Company objectives. The objectives incorporate the relevant service commitments and system requirements.	No deviations noted.
CC3.1.3	Management meets quarterly to discuss key performance indicators to assess performance towards operational initiatives.	No deviations noted.
CC3.2 - The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
CC3.2.1	<p>Management performs an annual risk assessment and meets quarterly to discuss, review, and track remediation of identified risks. The risk assessment includes the following:</p> <ul style="list-style-type: none"> • Business objectives for entity, subsidiary, division, operating unit, and functional levels. • The effect of environmental, regulatory, and technological changes on system security. • The effect of changes in management on the system of internal control. • Appropriate levels of management are involved. • Threats to operations, including security threats, associated with technology asset records. • Threats to operations, including threats from vendors, business partners, and other parties. • The significance of the risks. • A risk mitigation strategy. 	No deviations noted.
CC3.2.2	A vendor risk management program is established to assess and manage risks as associated with vendors and business partners. A vendor risk assessment is performed annually for vendors that impact the security of the system.	No deviations noted.

Ref. #	Client Controls	Results
CC3.3 - The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
CC3.3.1	<p>Management conducts an annual risk assessment that includes an assessment of fraud risks to identify the various ways that fraud and misconduct can occur, including how management might engage in inappropriate actions, considers opportunities, assesses attitudes and rationalizations, and considers risks related to IT and access to information.</p>	No deviations noted.
CC3.4 - The entity identifies and assesses changes that could significantly impact the system of internal control.		
CC3.4.1	<p>Management performs an annual risk assessment and meets quarterly to discuss, review, and track remediation of identified risks. The risk assessment evaluates:</p> <ul style="list-style-type: none"> • changes in the regulatory, economic, physical, and business environment, including industry, competitors, and consumers • the potential impact of new business lines, dramatically altered business lines, or divested business operations, rapid growth, changing reliance on foreign geographies, and new technologies • management and their respective attitudes and philosophies on the system of internal control • changes in technology • vendor and business partner relationships 	No deviations noted.

CC4.0 MONITORING ACTIVITIES

Ref. #	Client Controls	Results
CC4.1 - The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
CC4.1.1	Internal and external network vulnerability scans are performed monthly and their frequency is adjusted as required to meet ongoing and changing commitments and requirements.	No deviations noted.
CC4.1.2	Penetration tests are performed annually and their frequency is adjusted as required to meet ongoing and changing commitments and requirements.	No deviations noted.
CC4.1.3	Management obtains and reviews SOC reports for subservice organizations on an annual basis.	No deviations noted.
CC4.2 - The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.		
CC4.2.1	If applicable, remediation is developed and changes are implemented to remediate critical and high vulnerabilities, at a minimum, identified during the penetration tests or vulnerability scans.	No deviations noted.
CC4.2.2	As part of the annual risk assessment, management identifies controls that have been designed and operated to address risks. When the need for new controls is identified, management develops the requirements for the new controls and uses the change management process to implement them.	No deviations noted.

CC5.0 CONTROL ACTIVITIES

Ref. #	Client Controls	Results
CC5.1 - The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
CC5.1.1	Policies and procedures related to risk management are developed and implemented.	No deviations noted.
CC5.1.2	As part of the annual risk assessment, management identifies controls that have been designed and operated to address risks. When the need for new controls is identified, management develops the requirements for the new controls and uses the change management process to implement them.	No deviations noted.
CC5.1.3	Role based access is configured within the System to enforce segregation of duties.	No deviations noted.
CC5.2 - The entity also selects and develops general control activities over technology to support the achievement of objectives.		
CC5.2.1	<p>Established policies and procedures, which outline operating practices and business conduct for Axos Clearing personnel, are reviewed annually.</p> <p>The policies and procedures include the following:</p> <ul style="list-style-type: none"> • Acceptable Use Procedure • Business Continuity Policy • Change Control Management • Enterprise Data Governance • Incident Response • Information Security Policy • Privacy Policy • Risk Assessment Policy • Risk Management Policy • Security Standard • Software Acquisition • Software Development • Vendor Management 	No deviations noted.

Ref. #	Client Controls	Results
CC5.3 - The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
CC5.3.1	Roles and responsibilities of key managers are defined in the policies and procedures including duties such as proper oversight, management, and monitoring of vendor, security and availability activities.	No deviations noted.
CC5.3.2	Active employees' abilities to meet job requirements are evaluated as part of the semi-annual performance review process.	No deviations noted.
CC5.3.3	<p>Established policies and procedures, which outline operating practices and business conduct for Axos Clearing personnel, are reviewed annually.</p> <p>The policies and procedures include the following:</p> <ul style="list-style-type: none"> • Acceptable Use Procedure • Business Continuity Policy • Change Control Management • Enterprise Data Governance • Incident Response • Information Security Policy • Privacy Policy • Risk Assessment Policy • Risk Management Policy • Security Standard • Software Acquisition • Software Development • Vendor Management 	No deviations noted.

CC6.0 CONTROL ACTIVITIES – LOGICAL & PHYSICAL ACCESS

Ref. #	Client Controls	Results
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
CC6.1.1	Roles and users are reviewed and updated by management on a monthly basis. Access change requests resulting from the review are submitted to the security group via a change request record.	No deviations noted.
CC6.1.2	Administrator access to the System is restricted to authorized personnel.	No deviations noted.
CC6.1.3	The Company maintains segregated databases for each client to logically separate the client environments.	No deviations noted.
CC6.1.4	Logging is enabled to track access to the network.	No deviations noted.
CC6.1.5	Password complexity standards are established to enforce control over System passwords.	No deviations noted.
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
CC6.2.1	New access to the System is granted after the completion of an access request form that is authorized by appropriate individuals.	No deviations noted.
CC6.2.2	Management notifies security administrators of terminations resulting in the individual's logon ID being disabled or the password reset.	No deviations noted.
CC6.2.3	Roles and users are reviewed and updated by management on a monthly basis. Access change requests resulting from the review are submitted to the security group via a change request record.	No deviations noted.
CC6.2.4	Client access requests are granted after approval from authorized individuals.	No deviations noted.

Ref. #	Client Controls	Results
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
CC6.3.1	Roles and users reviewed and updated by management on a monthly basis. Access change requests resulting from the review are submitted to the security group via a change request record.	No deviations noted.
CC6.3.2	Management notifies security administrators of terminations resulting in the individual's logon ID being disabled or the password reset.	No deviations noted.
CC6.3.3	Client access requests are granted after approval from authorized individuals.	No deviations noted.
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
CC6.4.1	Access to the Company facilities, on-site server room, and third-party data center is limited to authorized personnel. Administrator access to the on-site access control system is restricted to authorized individuals.	No deviations noted.
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.		
CC6.5.1	Data retention and disposal procedures are in place to guide the secure disposal of sensitive data.	No deviations noted.
CC6.5.2	Digital media is degaussed and sanitized to remove any data and software prior to disposal.	No deviations noted.
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
CC6.6.1	A firewall is in place to control network traffic and prevent unauthorized traffic from passing between the internal and external networks. Administrator access to the firewall is restricted to authorized individuals.	No deviations noted.
CC6.6.2	VPN connections are utilized over public networks for encrypting sensitive information. Administrator access to the VPN console is restricted to authorized individuals.	No deviations noted.

<i>Ref. #</i>	<i>Client Controls</i>	<i>Results</i>
CC6.6.3	Intrusion detection systems (IDS) are used to provide continuous monitoring of the Company's network and early identification of potential security breaches. Administrator access to the IDS is restricted to authorized individuals.	No deviations noted.
CC6.6.4	The web application enables security protocols and transport layer security (TLS) encryption to secure transmission of data through the website.	No deviations noted.
<i>CC6.7 - The entity restricts the authorized internal and external users and processes, transmission, movement, and removal of information to and protects it during transmission, movement, or removal to meet the entity's objectives.</i>		
CC6.7.1	Data loss prevention software is used to scan for sensitive information in outgoing transmissions over public communication paths. Administrator access to the DLP solution is restricted to authorized individuals.	No deviations noted.
CC6.7.2	A Secure File Transfer Protocol (SFTP) server is used to protect transmission of data and other communications beyond the connectivity access points.	No deviations noted.
CC6.7.3	Backup media are encrypted during creation.	No deviations noted.
CC6.7.4	VPN connections are utilized over public networks for encrypting sensitive information. Administrator access to the VPN console is restricted to authorized individuals.	No deviations noted.
CC6.7.5	The web application enables security protocols and TLS encryption to secure transmission of data through the website.	No deviations noted.
<i>CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.</i>		
CC6.8.1	Anti-virus software is installed and configured on production servers and workstations to automatically scan and update virus definitions on a daily basis. Administrator access to the anti-virus software is restricted to authorized individuals.	No deviations noted.
CC6.8.2	IDS are used to provide continuous monitoring of the Company's network and early identification of potential security breaches. Administrator access to the IDS is restricted to authorized individuals.	No deviations noted.

CC7.0 CONTROL ACTIVITIES – SYSTEM OPERATIONS

Ref. #	Client Controls	Results
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		
CC7.1.1	IT operations monitors critical systems for performance, security threats, changing resource utilization needs, and unusual system activity. Errors are logged and alerts are generated to notify IT staff when conditions exceed defined threshold settings. Administrator access to monitoring systems is restricted to authorized individuals.	No deviations noted.
CC7.1.2	Internal and external network vulnerability scans are performed monthly and their frequency is adjusted as required to meet ongoing and changing commitments and requirements.	No deviations noted.
CC7.1.3	Penetration tests are performed annually and their frequency is adjusted as required to meet ongoing and changing commitments and requirements.	No deviations noted.
CC7.1.4	If applicable, remediation is developed and changes are implemented to remediate critical and high vulnerabilities, at a minimum, identified during the penetration tests or vulnerability scans.	No deviations noted.
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
CC7.2.1	Security incidents are reported to the security team and tracked through to resolution in a ticketing system.	No deviations noted.
CC7.2.2	IDS are used to provide continuous monitoring of the Company's network and early identification of potential security breaches. Administrator access to the IDS is restricted to authorized individuals.	No deviations noted.
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		
CC7.3.1	An Incident Response Plan is established to define the resolution and escalation of reported events.	No deviations noted.
CC7.3.2	Security personnel log and track incidents in a ticketing system for evaluating and escalating reported events.	No deviations noted.

Ref. #	Client Controls	Results
CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
CC7.4.1	Management has established defined roles and responsibilities to oversee the implementation of information security policies including incident response.	No deviations noted.
CC7.4.2	An incident response plan is established to define the resolution and escalating of reported events to include that procedures are in place to contain security incidents, mitigate effects of ongoing security incidents, restore operations to an interim state and communicate security incidents to affected parties.	No deviations noted.
CC7.4.3	Data restoration procedures are defined within the incident response plan.	No deviations noted.
CC7.4.4	After an incident has been confirmed, specific personnel are engaged in the containment process to reduce the magnitude of the incident.	No deviations noted.
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.		
CC7.5.1	Incident response procedures are in place to restore affected environments to functional operation by rebuilding systems, updating software, installing patches, and changing configurations, as needed.	No deviations noted.
CC7.5.2	As part of the annual risk assessment, management identifies controls that have been designed and operated to address risks. When the need for new controls is identified, management develops the requirements for the new controls and uses the change management process to implement them.	No deviations noted.
CC7.5.3	Business continuity and disaster recovery plans, including restoration of backups and emergency notification systems, are tested annually. Test results are reviewed and the contingency plan is adjusted as necessary.	No deviations noted.

CC8.0 CONTROL ACTIVITIES – CHANGE MANAGEMENT

Ref. #	Client Controls	Results
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		
CC8.1.1	The software development process establishes a methodology for managing system changes throughout the lifecycle that governs the development, acquisition, implementation, and maintenance of information systems.	No deviations noted.
CC8.1.2	A ticketing system is established to track system changes from initiation through deployment, logging activities throughout the process.	No deviations noted.
CC8.1.3	Changes to the Liberty and TCTrust applications are tested in a segregated environment prior to system implementation.	No deviations noted.
CC8.1.4	Changes to the Liberty and TCTrust applications are reviewed and approved by management prior to implementation.	No deviations noted.
CC8.1.5	Source code management software is utilized for version control of development projects for the Liberty application and is configured to require a secondary approval prior to migration of changes to production to enforce segregation of duties. Administrator access is restricted to authorized individuals.	No deviations noted.
CC8.1.6	Source code management software is utilized to control access to the source code for the TCTrust application changes and is configured to generate alert emails when changes are deployed to ensure that unauthorized changes are not made. Administrator access is restricted to authorized individuals.	No deviations noted.
CC8.1.7	Management approves the implementation of changes to infrastructure prior to implementation.	No deviations noted.
CC8.1.8	A documented patch management process is established.	No deviations noted.
CC8.1.9	IT personnel periodically review the availability of patches for production systems and critical patch updates are installed by IT personnel.	No deviations noted.

<i>Ref. #</i>	<i>Client Controls</i>	<i>Results</i>
CC8.1.10	As part of the annual risk assessment, management identifies controls that have been designed and operated to address risks. When the need for new controls is identified, management develops the requirements for the new controls and uses the change management process to implement them.	No deviations noted.

CC9.0 RISK MITIGATION

Ref. #	Client Controls	Results
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
CC9.1.1	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No deviations noted.
CC9.1.2	<p>Management performs an annual risk assessment and meet quarterly to discuss review and track remediation of identified risks. The risk assessment includes the following:</p> <ul style="list-style-type: none"> • Business objectives for entity, subsidiary, division, operating unit, and functional levels. • The effect of environmental, regulatory, and technological changes on system security. • The effect of changes in management on the system of internal control. • Appropriate levels of management are involved. • Threats to operations, including security threats, associated with technology asset records. • Threats to operations, including threats from vendors, business partners, and other parties. • The significance of the risks. • A risk mitigation strategy. 	No deviations noted.
CC9.1.3	The risk management program includes the use of cybersecurity insurance to minimize the financial impact of any loss events.	No deviations noted.
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.		
CC9.2.1	Formal information sharing agreements are in place with related parties and vendors. These agreements include the scope of services and security commitments applicable to that entity.	No deviations noted.
CC9.2.2	A vendor risk management program is established to assess and manage risks associated with vendors and business partners. A vendor risk assessment is performed annually for vendors that impact the security of the system.	No deviations noted.
CC9.2.3	Management has defined roles and responsibilities to oversee the management of risks associated with vendors and business partners.	No deviations noted.
CC9.2.4	Management obtains and reviews SOC reports for subservice organizations on an annual basis.	No deviations noted.

ADDITIONAL CRITERIA FOR AVAILABILITY

Ref. #	Client Controls	Results
<i>A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.</i>		
A1.1.1	IT operations monitors critical systems for performance, security threats, changing resource utilization needs, and unusual system activity. Errors are logged and alerts are generated to notify IT staff when conditions exceed defined threshold settings. Administrator access to monitoring systems is restricted to authorized individuals.	No deviations noted.
A1.1.2	High availability clusters and replication are implemented for redundancy of the production environment.	No deviations noted.
<i>A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.</i>		
A1.2.1	Environmental protection systems are installed and receive maintenance on an annual basis. Environmental protections include the following: <ul style="list-style-type: none"> • Cooling systems • Backup generator • Smoke detectors • Sprinklers • Fire suppression 	No deviations noted.
A1.2.2	A backup process is in place to automatically perform daily database backups. Backups are monitored for failure and notification alerts are sent to designated individuals for resolution. Administrator access to the backup software is restricted to authorized individuals.	No deviations noted.
A1.2.3	High availability clusters and replication are implemented for redundancy of the production environment.	No deviations noted.
<i>A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.</i>		
A1.3.1	Business continuity plans, including restoration of backups and emergency notification systems, are tested annually. Test results are reviewed and the contingency plan is adjusted as necessary.	No deviations noted.