System and Organization Controls 1 (SOC 1) Type 2

Report on Integral Development Corporation's FX Trading Management System and suitability of the design and operating effectiveness of its controls

INTEGRATED TYPE 2 REPORT PREPARED IN ACCORDANCE WITH THE AICPA SSAE NO. 18 AND IAASB ISAE 3402 STANDARDS

For the Period September 1, 2021 to August 31, 2022

TABLE OF CONTENTS

SECTION ONE

Independent Service Auditor’s Report

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of Integral Development Corporation
Palo Alto, CA

Scope

We have examined Integral Development Corporation's ("Service Organization" or "Integral") description of its FX Trading Management System entitled " Integral Development Corporation's Description of Its FX Trading Management System" for providing cloud-based platform services throughout the period September 1, 2021 to August 31, 2022 (description) and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Assertion of Integral Development Corporation Management" (assertion). The controls and control objectives included in the description are those that management of Integral believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the FX Trading Management System that are not likely to be relevant to user entities' internal control over financial reporting.

The information included in Section 5, "Other Information Provided by Integral Development Corporation," is presented by management of Integral to provide additional information and is not a part of Integral's description of its FX Trading Management System made available to user entities during the period September 1, 2021 to August 31, 2022. Information about Integral's Disaster Recovery Plan has not been subjected to the procedures applied in the examination of the description of its FX Trading Management System and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of its FX Trading Management System and, accordingly, we express no opinion on it.

Integral uses a subservice organization for data center hosting services. The description includes only the control objectives and related controls of Integral and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by Integral can be achieved only if complementary subservice organization controls assumed in the design of Integral's controls are suitably designed and operating effectively, along with the related controls at Integral. Our examination did not extend to controls of the subservice organization and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Integral'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 2, Integral 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. Integral 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.

Our examination was conducted in accordance with attestation standards established by the AICPA and in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organization," issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform the 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 September 1, 2021 to August 31, 2022. 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 control objectives stated in the description, based on the criteria in management's assertion.
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.

- Evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements for providing cloud-based platform services. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

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

Opinion

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

a. the description fairly presents the FX Trading Management System that was designed and implemented throughout the period September 1, 2021 to August 31, 2022.

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 September 1, 2021 to August 31, 2022 and the subservice organization and user entities applied the complementary controls assumed in the design of Integral's controls throughout the period September 1, 2021 to August 31, 2022.

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period September 1, 2021 to August 31, 2022 if complementary subservice organization controls and user entity controls assumed in the design of Integral's controls operated effectively throughout the period September 1, 2021 to August 31, 2022.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Integral, user entities of Integral's FX Trading Management System during some or all of the period September 1, 2021 to August 31, 2022, and their auditors who audit and report on such user entities' financial statements or internal control

over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

CyberGuard Compliance, LLP
Las Vegas, NV
November 30, 2022

SECTION TWO

Assertion of Integral Development Corporation Management

ASSERTION OF INTEGRAL DEVELOPMENT CORPORATION MANAGEMENT

November 30, 2022

CyberGuard Compliance, LLP
Las Vegas, NV

Scope

We have prepared the description of Integral Development Corporation's ("Service Organization" or "Integral") FX Trading Management System entitled" Integral Development Corporation's Description of Its FX Trading Management System," for providing cloud-based platform services throughout the period September 1, 2021 to August 31, 2022 (description) for user entities of the system during some or all of the period September 1, 2021 to August 31, 2022, and their auditors who audit and report on such user entities' financial statements or internal control over financial statement reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves when assessing the risks of material misstatement of user entities' financial statements.

Integral uses a subservice organization for data center hosting services. The description includes only the control objectives and related controls of Integral and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organization.

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

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

1) The description fairly presents the FX Trading Management System made available to user entities of the system during some or all of the period September 1, 2021 to August 31, 2022 for providing cloud-based platform services as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

    a) Presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable:

i) The types of services provided, including, as appropriate, the classes of transactions processed.

ii) The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the 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, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the 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) The services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.

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 controls.

viii) Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

b) Includes relevant details of changes to the FX Trading Management 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 FX Trading Management 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 operating effectively throughout the period September 1, 2021 to August 31, 2022 to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of Integral's controls throughout the period September 1, 2021 to August 31, 2022. The criteria we used in making this assertion were that:

a) The risks that threaten the achievement of the control objectives stated in the description have been identified by management.

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.

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

Integral Development Corporation

SECTION THREE

Integral Development Corporation's Description of its FX Trading Management System

INTEGRAL DEVELOPMENT CORPORATION'S DESCRIPTION OF ITS FX TRADING MANAGEMENT SYSTEM

1 Overview of Integral Development Corporation's Operations

Company Background

Integral Development Corporation (Integral) founded in 1993, is a financial technology company that helps its customers -- banks, brokers, and asset managers outperform their competition in the foreign exchange market through innovative solutions for workflow management and advanced execution. This powerful cloud-based platform is the industry's only answer for FX institutions that want to design and deliver complete solutions tailored to their businesses. Integral's modern approach of addressing the entire FX lifecycle with an intelligent platform allows its customers to achieve the lowest transaction costs, greatest operational efficiency, and highest yield.

Description of Services Provided

Integral products include:

BankFX with all the features necessary to help banks win in FX — access to liquidity sources, unrivaled pricing engine, distribution channels, robust risk management algorithms, and analytics.

MarginFX, built on Integral's cloud-based technology, allows leading brokers to deliver state-of-the-art FX trading services to a global customer base at a fraction of the cost, with 100% reliability and maximized profits. MarginFX includes all major features required to operate a global, multi-level, competitive margin FX business out of the box including liquidity sources, customer price streams, front-end trading systems, and risk management models.

InvestorFX is the market leading FX execution platform for asset managers. Built with integral's cloud technology, InvestorFX is able to connect to all major OMS platforms and a variety of customer in-house platforms to deliverable scalable, end to end automation. InvestorFX provides optimal netting, best execution, TCA and workflow automation. Trade lists from Alladin, Charles River, Eze Software, LineData and Fidessa integrate directly with InvestorFX allowing for seamless transition from order management to execution management.

OCX, Open Currency Exchange, is the most modern FX OTC exchange. It brings together the most diverse pool of FX market participants into a single integrated network of liquidity. OCX was designed from the ground up to include all FX market participants. No other platform reaches as many, as varied, and as comprehensive a set of FX products and participants as OCX. By lowering access fees and eliminating the exclusivity requirements of legacy platforms, OCX opens the FX market to everyone.

Integral's award-winning services also include the family of FX Inside Professional™ products for the professional segment including FX Inside White Label™ and www.TrueFX.com.

The Integral FX Benchmark™ offers free second-by-second mid-rates of major currency pairs. It is based on joint research collaboration between Integral and Stanford University, and on feedback from major buy-side participants in the FX market.

TrueFX® brings real, dealable prices from the market-making banks to everyone for free. Registered users have access to streaming real-time and historical tick-by-tick data.

Integral maintains development, support, and sales offices in Palo Alto, New York, London, Tokyo, Singapore, and Bangalore. For more information, visit www.integral.com.

Integral technology is protected under U.S. Patent Nos. 7,882,011; 8,417,622; 8,862,507; 9,412,134; 9,836,789; 10,387,952; 10,467,696; 10,621,665; 10,915,951; 10,956,977, as well as patent pending applications and related intellectual property.

Principal Service Commitments and System Requirements

Integral establishes system and operational requirements to support the achievement of its principal service commitments, applicable laws, and regulations. These requirements are communicated in Integral's policies and procedures, system design documentation, and/or customer contracts.

Information Security policies define how systems and data are protected. These policies are updated as appropriate based on evolving technologies, changes to the security threat landscape, and changes to industry standards, provided any updates do not materially reduce the service commitments or overall service provided to customers as described in the customer contracts.

2 Overview of the System and Applications

Scope and System Boundaries

The scope of the review is limited to the Integral's FFX Trading Management System. The specific control objectives and related control activities included in the scope of this engagement can be found in Section 4 ("Description of Control Objectives, Controls, Tests, and Results of Tests").

System Overview

General Organizational Summary

Integral's Management Team ensures several controls are in place to provide reasonable assurance that the organizational structure provides for management oversight of staff and contractors, segregation of duties, and administrative practices. Internal staff functions are

documented via an organizational chart and job descriptions are documented. All staff members are issued an Employee Handbook and must agree to abide by the expectations outlined. Each staff member is required to go through a background check to obtain employment. Contractors for Integral are required to sign a contractor agreement that includes a non-disclosure agreement. Each contract entered into with user entities outlines the scope of services to be provided.

Business Support

From a customer service perspective, controls are followed that give reasonable assurance that customer inquiries or requests are addressed and resolved in a timely manner. Integral management has established formal policies and procedures to guide the customer support process. The customer support function is available to customers Sunday noon PST through Friday 2:00 pm PST via e-mail or telephone support. All customer technical support requests are entered into and tracked via support tracking software. Each step taken in a given support incident or request is tracked through the duration of the request. All steps are documented throughout the lifetime of a given request to ensure resolution.

Customer Configuration

Management has established formal policies and procedures for new customer setup. New customer set-up controls provide reasonable assurance that new customer accounts are set up and changes made to existing customer accounts are authorized and processed completely, accurately, and in a timely manner. Once customers are configured, all application-based security is controlled by the customer. Any change to a customer's configuration must be either performed by the customer itself or requested by an authorized customer contact. All requests to Integral for configuration change are tracked via support ticket tracking software.

Client Application Access

Access to client- specific trading website instances is acquired via a web browser and requires username and password credentials or two-factor authentication for access. Once configured by Integral's business support service, the client has full administrative control over user credentials for their trading admin site. Username and password assignment are controlled by the client.

Web Application Security

The trading web applications have several security measures in place to protect client access to their trading site as well as protect data transmission over the Internet.

- Account Security
  - User accounts are locked upon three unsuccessful attempts at login. Accounts must be manually unlocked either by a client site administrator or Integral's Support to re-enable the given account.

    - Password complexity requirements are in place to ensure passwords are difficult to guess.

- Data Security
    - Client data is only visible to the given clients. Data is logically segregated by tagging all data with a customer's organization ID.
- Network Security
    - Network traffic between client web browsers and trading sites is protected by use of a signed SSL certificate. This encrypts all traffic, end-to-end, and over the Internet.

System Infrastructure Security

Integral has policies and procedures in place to protect and secure the company's development, pre-production and production infrastructure. Each subcategory is described in detail under the "Control Environment" section of this document. Areas covered include:

- Logical Security
    - Assurance that applications and network resources are protected via strong authentication process, encryption and secured by enterprise class firewalls.
- Physical Security
    - Assurance that all facilities are protected by strong access controls.
- Environmental Security
- Systems are in place to automatically monitor all resources for presence of smoke, fire, heat, water or power interruptions.
- Computer Operations
    - Systems are in place to monitor and track server systems, services, database and application performance.
- Availability and Recovery
    - Automated systems are in place to ensure all data is backed up and recoverable.

Software Development Lifecycle & Change Control

Software Development Lifecycle & Change Control provides reasonable assurance that system changes are authorized, tested, and approved prior to implementation. Integral management has established a formal policy for application development and change management that requires changes to be authorized, tested, approved, and documented. Quality assurance (QA) testing is performed before application changes are migrated into production systems. This defined segregation of duties ensures changes to application source and or database schema are not deployed without proper QA and approval. All development activity is logged, documented, tracked in a project management system, and tracked throughout its lifecycle.

The IT Director monitors the quality of internal control performance as a normal part of his activities. The IT Director is heavily involved in day-to-day activities and regularly reviews

various aspects of internal and customer-facing operations to (i) determine if objectives are achieved, (ii) identify any new risks that develop, and (iii) implement appropriate measures to address those risks. Integral adopts a proactive approach to the monitoring of application security to ensure that any issues or risks are addressed before becoming significant problems.

Data Centers

The primary data center facilities are located at secure tier 4 Equinix facilities in Secaucus, New Jersey; Slough, United Kingdom; Tokyo, Japan and Crescent, Singapore where Integral has long-term leases in place. Only selected operations personnel from Integral have physical access to the data center cage seven days a week and 24 hours a day. Selected Integral operations personnel have password-restricted and rights-controlled remote access to servers and devices network applications.

Integral provides software services through a combination of internally developed high-speed, low latency application, web, and database platforms. The trading network operates on a Linux-based platform. For security and redundancy purposes, multiple servers are used for various service delivery functions and applications.

Management of Integral receives and reviews the SOC report of Equinix on an annual basis, including the complementary subservice organization controls (CSOC) included within Equinix report. In addition, through its daily operational activities, management of Integral monitors the services performed by Equinix to ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also holds periodic calls with the subservice organization to monitor compliance with the service level agreement, stay abreast of changes at the subservice organization, and relay any issues or concerns to the subservice organization management.

Logical Security Policy

Logical security controls to Integral data and server applications in the production environments in Secaucus, New Jersey; Slough, United Kingdom; Tokyo, Japan and Crescent, Singapore; the pre-production environment in Palo Alto, California; and the development environment in Palo Alto provide reasonable assurance that access to company network resources is restricted to properly authorized individuals and programs. Security policies are incorporated in the Employee Handbook provided to each staff member. User access is formally requested by Management, then is approved and granted by the Information Technology department. Contractors are granted specific access to resources based on their role. Access levels are restricted to authorized accounts and are in line with each staff member's job function. Each internal account is configured to enforce complex password requirements. Security is proactively assessed periodically through security and vulnerability scans. Access to production systems is requested by Management, then is approved and granted by the Information Technology department. Additionally, controls provide reasonable assurance that security events are logged, reviewed and researched regularly.

Physical Security

Physical Security policies and procedures exist to guide personnel in the performance of their duties. A card access control system exists for the Integral development facility to control physical access into and throughout all areas of the building. No one can access Integral's floor without an Integral access badge. All critical/sensitive computer servers have been moved off site to an offsite local Data Center. Access to this Data Center is strictly monitored and controlled. Only noncritical servers such as the phone server remain in the Integral office. Visitors to the Company facility must be escorted by an authorized Company representative. Facility access is logged and reviewed on a routine basis. Physical access to the Integral production environment is governed by Equinix and outlined in the "Subservice Organization'' section of this document.

Environmental Security

Environmental security controls for the Integral development environment provide reasonable assurance that hardware is protected from damage by fire, flood, and other environmental hazards. The pre-production development environment is equipped with monitoring devices that watch and detect temperature. Such devices notify appropriate company personnel in the event pre-determined thresholds are exceeded. Any anomalies result in IT staff notification via email. Integral production systems in Secaucus, New Jersey; Slough, United Kingdom; Tokyo, Japan and Crescent, Singapore are protected in a highly secure tier 3 data center. Controls for the Equinix are listed below in the Subservice Organization line item.

Computer Operations

Computer Operations controls provide reasonable assurance that systems are in place to proactively track network, system, and application problems, and ensure effective and timely resolution. All networks are protected by enterprise class firewall systems. An Intrusion Detection system is in place to proactively track network traffic in and out of the network. Network security logs are reviewed routinely by Integral management for anomalies. Any unusual events are investigated promptly. unusual events are investigated promptly. In the event of a security incident, a policy is in place to react to, manage and log incidents.

Availability and Recovery

Availability and recovery controls provide reasonable assurance that backup and recovery procedures are in place to ensure the continuity of operations and preserve the integrity of programs and data. Multiple automated backup systems are in place to backup all data, applications and complete systems hourly or daily. Backup data is stored in separate locations. The backup systems are configured to notify Integral staff upon completion of jobs. Backup logs are emailed to Integral staff nightly. Backup logs are reviewed for any failures daily. Backups are routinely tested for recoverability. Additionally, Integral applications, end points and services are monitored by real time monitoring software. Staff is notified in the event of any service disruption of network connection, hardware failures or application faults.

Anti-virus/Anti-spam/Web Filtering
Industry-leading anti-virus software exists at the workstation level to block spam, restrict access to inappropriate websites, and protect Integral's applications and data from viruses and infection by other malicious code. Incoming email messages are scanned for spam and viruses by an e-mail gateway filter device provided by Barracuda. The anti-virus software is configured to receive virus definition updates daily.

Vulnerability Management
Vulnerability assessments of the FFX Trading Management System are performed on a quarterly basis to identify potential security vulnerabilities. If a potential or actual security breach is detected, security personnel work to identify the cause and remediate immediately. Additionally, penetration tests are performed annually to find and address any security weaknesses. Security personnel review the reports and document remediation plans to resolve any potential vulnerabilities, as applicable. Management reviews results of the report and evaluates updates to the Risk Assessment based on findings.

Integral addresses vulnerabilities potentially affecting the security and availability of systems and data through the following:

- The implementation of antivirus software on all systems commonly affected by malicious software.
- The application of vendor-supplied security patches as needed. Critical security patches are installed within one month of release.
- Vulnerability scans run on a quarterly basis or more frequently as needed due to significant changes in the network.
- Penetration tests are performed on an annual basis, or more frequently as needed due to significant changes to the infrastructure or applications.

Issues identified in vulnerability scans and penetration test results are remediated and repeat scans and testing are performed to ensure that weaknesses have been corrected.

Management Controls

The overall organization supports the framework for an effective control environment. The organization is comprised of the following functional areas:

Executive Management provides strategic direction and leadership for Integral and all of its domestic and international subsidiaries and affiliates. Executive Management oversees and is ultimately responsible for all aspects of service delivery (including business development, marketing, and quality assurance), and all corporate services functions including but not limited to finance, information technology, human resources, legal, real estate and facilities, and corporate development.

Sales is responsible for building and maintaining client relationships in order to sell the suite of products and services to the marketplace. They work with the customer to develop customized solutions to solve their challenges and they support the customer when they have any questions about our products. Technical account managers help customers during the on-boarding process, working with them to initially configuring their systems for trading. They also provide ongoing training for customers for features and new releases.

Trading Operations/Information Technology ("IT") Management has overall responsibility and accountability for the enterprise- computing environment, including data centers, computer hardware, operating systems, network systems and the trading applications. Trading Operations personnel work closely with engineering and business support to develop and implement guidelines and procedures to ensure that the enterprise-computing environment is functioning both efficiently and effectively with regard to the Company's business objectives and requirements. IT personnel also support the sales business processes, including the administration of systems supporting key business processes as well as maintaining application patch levels in accordance with vendor recommendations.

Business Support ("BS") manages an ongoing relationship with customers and works with all customer's key personnel from the trading desk to the back office to ensure smooth operations and a high level of service delivery. BS is staffed by experienced, FX-knowledgeable business specialists, skilled in all Integral products. As a trusted partner, BS acts as a neutral facilitator if discrepancies arise. All customers have phone and e-mail support. If BS is contacted via e-mail by a customer, customers receive an automatically generated ticket number to Integral's online-ticketing and tracking system. Integral's robust first line support includes 24-hour support service from Sunday night when the markets open in Australia to close-of-market in New York on Friday evening. Integral business support staff will work with customers to arrange for training, to coordinate a customer's service implementation, and to plan for projects such as STP or protocol integrations to a customer's back office.

Engineering is responsible for the design and development of Integral's software products and applications, ensuring that we build products that are required by customers and that these products work the way they are supposed to.

Human Resources is responsible for managing all functions related to recruiting and hiring, benefits, employee relations, performance management, training, resource management, and career assistance. The Human Resources team partners proactively with Executive Management and business units to ensure that all initiatives are appropriately aligned with Integral mission, vision, and values. Additionally, Human Resources ensure that meaningful, accurate metrics are kept and that Integral maintains compliance with all federal and state rules and regulations.

Marketing is responsible for the strategic deployment of the Integral brand and for building awareness through multiple media channels including the Internet, public relations,

advertising, industry associations, and direct mail. Marketing also supports the business development group through action-oriented targeted marketing initiatives that qualify prospects and drive revenue generation.

Finance Management is primarily responsible for the accuracy of financial reporting and non-client related tax compliance. Finance personnel are responsible for corporate treasury matters, client invoicing and payment applications, payroll, and procurement processing. Finance provides support and assistance as needed to client services.

Integral is committed to equal opportunity of employment and all employment decisions are based on merit, qualifications, and abilities. Employment-related decisions are not influenced or affected by an employee's race, color, nationality, religion, sex, marital status, family status, sexual orientation, disability or age. Integral endorses a work environment free from discrimination, harassment, and sexual harassment.

3 Control Objectives and Related Controls

Integral's control objectives and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the control objectives and related control activities are included in Section 4, they are, nevertheless, an integral part of Integral's system description. The description of the service auditor's tests and the results of those tests are also presented in Section 4, adjacent to the service organization's description of controls. The description of the tests and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Control Environment

Key facets of the Company's control environment relating to processing and staffing for all processes performed by the Company are summarized below. These areas include:

- Integrity and Ethical Values
- Commitment to Competence
- Board of Directors Participation
- Management's Philosophy and Operating Style
- Human Resources Policies and Practices
- Organizational Structure and Assignment of Authority and Responsibility

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Integral control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the products of Integral's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice.

Specific control activities that the service organization has implemented in this area are described below:

- The Employee Handbook contains organizational policy statements and codes of conduct to which employees are required to adhere.
- Employees sign an acknowledgement form to document that they have reviewed the Employee Handbook and understand their obligation to adhere to the policy statements and codes of conduct.
- Employees sign an agreement that documents the employees' understanding of Integral's policy and procedure for handling sensitive or confidential information.
- Background checks are obtained for employees as a component of the employee hiring process.

Commitment to Competence

Integral's management defines competence as the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Integral has focused on hiring experienced employees for the various positions required for the business. Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated the required skills and knowledge levels into written position requirements.
- Personnel are provided with orientation, hands-on training and supervision to the extent deemed necessary for each position.

Board of Directors Participation

Integral's control consciousness is influenced significantly by its board of directors and audit committee. A board of directors oversees management activities.

Management's Philosophy and Operating Style

Integral's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks and management's attitudes toward information processing, accounting functions, and personnel. Management weekly meetings are held to discuss operational issues.

Human Resources Policies and Practices

Integral's Human Resources policies and procedures relate to employee hiring, orientation, training, evaluating, promoting, compensating and remedial actions. Specific control activities that the service organization has implemented in this area are described below:

- Human Resources personnel utilize new hire document lists to ensure that specific elements of the hiring process are consistently executed, and a copy of the lists are maintained in the employee file.
- Management performs evaluations for each employee on an annual basis.
- Management has established employee termination procedures that guide personnel in the termination process.

Organizational Structure and Assignment of Authority and Responsibility

Integral's organizational structure provides the framework within which its activities for achieving entity- wide objectives are planned, executed, controlled, and monitored. Integral's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility, and appropriate lines of reporting. Integral has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities. Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and updated as needed.

Risk Assessment

Integral recognizes the importance of risk management in properly managing Integral and customer transactions and providing high-quality, cost-effective services to its customers. The IT Director oversees the assessment of risk with respect to the IT processing environment and related application systems and services provided to users of the company's application systems.

Information and Communication

Information Systems

The primary IT facilities are located in Palo Alto, California. Additional IT facilities are located in each of Integral's client service locations where Integral has a long-term lease in place. Integral users have password-restricted access to network applications seven days a week and 24 hours a day, except for brief maintenance periods. Remote employees have password-restricted and rights-controlled intranet access to network applications.

The IT network operates on a Microsoft Windows-based platform, with SQL server client databases in use where possible. For security and redundancy purposes, multiple servers are used for various service delivery functions and applications. An Ethernet configuration is used for local network connectivity.

Communication Systems

Integral utilizes both formal and informal methods for corporate-wide communication. Upper management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls.

This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to an appropriate higher level within the Company.

Additionally, formal communication tools such as organizational charts, employee handbooks, and job descriptions are in place. Management's communication activities are made electronically, verbally, and through the actions of management.

4 Monitoring

Management monitors the quality of internal control performance as a normal part of their activities. They are heavily involved in day-to-day activities and regularly review various aspects of internal and customer-facing operations to determine if objectives are achieved, identify any new risks that develop, and implement appropriate measures to address those risks. Integral adopts a proactive approach to the monitoring of application and network security to ensure that any issues or risks are identified and addressed as soon as possible.

Subservice Organization

Integral utilizes Equinix Inc. (Equinix) for data center hosting services. The following Complementary Subservice Organization Controls (CSOCs) are expected to be operating effectively at Equinix IBX, alone or in combination with controls at Integral, to provide assurance that the required control objectives in this report are met.

Subservice Organization – Equinix Inc.	
Control Objective	**Complementary Subservice Organization Control**
Physical Security	Equinix is responsible for restricting physical access to data center facilities, backup media, and other system components including network devices and servers.
Environmental	Equinix is responsible for ensuring environmental protection controls are in place to meet availability commitments and requirements.
Management of Integral receives and reviews the SOC report of Equinix on an annual basis, including the complementary user entity controls (CUEC) included within the Equinix report. In addition, through its daily operational activities, management of Integral monitors the services performed by Equinix to ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively.	

5 Description of Complementary User Entity Controls

This section describes certain controls that user entities should consider for the achievement of control objectives identified in this report. The Integral system was designed with the assumption that internal controls would be placed in operation by user entities. The application of such internal controls by user entities is necessary to achieve certain control

objectives identified in this report. There may be additional control objectives and related controls that would be appropriate for the processing of user entity transactions which are not identified in this report.

Integral requires that user entities implement internal controls that are stipulated in the contractual agreement such user entities execute with Integral, including but not limited to those controls that are necessary in order to comply with applicable law.

In addition to any contractual requirements, Integral requires that user entities implement internal controls in order to be properly on-boarded onto the Integral system.

SECTION FOUR

Description of Control Objectives, Controls, Tests, and Results of Tests

DESCRIPTION OF CONTROL OBJECTIVES, CONTROLS, TESTS, AND RESULTS OF TESTS

1 Overview

On the pages that follow, the description of control objectives and the controls to achieve those objectives have been specified by and are the responsibility of Integral. The testing performed by CyberGuard Compliance, LLP and the results of tests are the responsibility of the service auditor.

Our tests of Integral's entity level controls included, to the extent we considered necessary: (a) a review of the organizational structure of Integral, including information technology policies and procedures, the segregation of functional and technical responsibilities, and personnel policies, (b) discussions with management, operations, administrative and other personnel who are responsible for developing, ensuring adherence to and applying information technology controls, (c) observations of personnel in the performance of their assigned duties, and (d) tests of controls specified by Integral. We applied tests to specific controls to obtain evidence about their operating effectiveness in meeting Integral's related control objectives, for the period September 1, 2021 to August 31, 2022.

It is each interested party's responsibility to evaluate this information in relation to internal controls in place at user organizations to obtain an understanding of the internal controls and control risk. User organizations and their respective auditors must evaluate the controls provided by Integral in conjunction with controls executed by user organizations, including, but not necessarily limited to, those listed in "Description of Complementary User Entity Controls" in Section 3 of this report. If effective user organization internal controls are not in place, Integral's controls may not compensate for such weaknesses.

Exceptions, if any, noted by CyberGuard Compliance, LLP, regarding the adequacy of the controls identified to achieve the stated objective or the level of compliance with the controls are presented next to each control under the caption "Test Results." Exceptions identified are not necessarily weaknesses in the total system of internal controls of Integral, as this determination can only be made after consideration of controls in place at user organizations.

2 Control Objectives, Control Activities, Testing Procedures, and Results of Tests

This report, when combined with an understanding of the controls at user entities, is intended to assist auditors in planning the audit of user entities' financial statements or user entities' internal control over financial reporting and in assessing control risk for assertions in user entities' financial statements that may be affected by controls at Integral.

Our examination was limited to the control objectives and related controls specified by Integral in Sections 3 and 4 of the report and did not extend to controls in effect at user entities.

It is the responsibility of each user entity and its independent auditor to evaluate this information in conjunction with the evaluation of internal control over financial reporting at the user entity in order to assess total internal control. If internal control is not effective at user entities, Integral's controls may not compensate for such weaknesses.

Integral's internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by Integral. In planning the nature, timing, and extent of our testing of the controls to achieve the control objectives specified by Integral, we considered aspects of Integral's control environment, risk assessment process, monitoring activities, and information and communications.

The following table clarifies certain terms used in this section to describe the nature of the tests performed:

Type of Test	General Description of Test
Inquiry or Corroborative Inquiry	Inquired of appropriate personnel to ascertain compliance with controls.
Observation	Observed application of specific controls.
Inspection	Obtained and inspected documents and reports indicating performance of the controls.
Re-performance	Re-performed application of the controls.

In addition, as required by paragraph .35 of ATC Section 205, *Assertion Based Engagements* (AICPA, *Professional Standards*), and paragraph .30 of ATC Section 320, when using information produced (or provided) by the service organization, 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.

3 Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For tests of controls requiring the use of IPE (e.g., controls requiring system-generated populations for sample-based testing), CGC performed a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used:

1) Inspect the source of the IPE,
2) Inspect the query, script, or parameters used to generate the IPE,
3) Tie data between the IPE and the source, and/or
4) Inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity.

In addition to the above, procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), CGC inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

ORGANIZATION AND ADMINISTRATION: Controls provide reasonable assurance that the organizational structure provides for management oversight, segregation of duties and administrative practices.			
1.0	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
1.1	An organizational chart is documented for each department and is available to management personnel.	**Inspection:** Obtained and reviewed the organizational chart and a screenshot of the organizational chart location on the Company's intranet. Verified an organizational chart was documented for each department and was available to management personnel.	No exceptions noted.
1.2	Job descriptions describe the required duties for each position.	**Inspection:** Obtained and reviewed the job descriptions for the sampled active employees during the audit period. Verified job descriptions described the required duties for each position.	No exceptions noted.
1.3	New employees receive an employee handbook upon being hired and must sign an Acknowledgment of the Receipt of Employee Handbook.	**Inspection:** Obtained and reviewed the handbook acknowledgment form for the sampled employees hired during the audit period. Verified new employees received an employee handbook upon being hired and must sign an Acknowledgment of the Receipt of Employee Handbook.	No exceptions noted.
1.4	All employees and subcontractors must sign a "Confidentiality and Inventions Agreement" upon being hired/engaged.	**Inspection:** Obtained and reviewed the signed Confidentiality and Inventions Agreement for the sampled employees hired during the audit period. Verified all employees and subcontractors signed a "Confidentiality and Inventions Agreement" upon being hired/engaged.	No exceptions noted.

ORGANIZATION AND ADMINISTRATION: Controls provide reasonable assurance that the organizational structure provides for management oversight, segregation of duties and administrative practices.			
1.0	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
1.5	Background checks are performed on new employees as a condition of employment to ensure they are able to work in a trading environment.	**Inspection:** Obtained and reviewed the background check reports for the sampled employees hired during the audit period. Verified background checks were performed on new employees as a condition of employment to ensure they are able to work in a trading environment.	No exceptions noted.
1.6	The Company maintains various types of corporate insurance policies in place during the year.	**Inspection:** Obtained and reviewed the property and the liability insurance policy. Verified the Company maintained various types of corporate insurance policies in place during the year.	No exceptions noted.
1.7	The Company has a Vendor Management Policy, which provides guidance with respect to the identification and the management of critical vendors.	**Inspection:** Obtained and reviewed the Vendor Management Policy. Verified a policy was in place which provided guidance with respect to the identification and the management of critical vendors.	No exceptions noted.
1.8	On an annual basis, management reviews the complementary user entity control considerations contained within the Service Organization Control (SOC) audit reports (or equivalent) for applicable subservice providers and verifies the controls are satisfactorily implemented and in place within their environment.	**Inspection:** Obtained and reviewed the subservice organization Service Organization Control (SOC) reports and management's review. Verified on an annual basis, management reviewed the complementary user entity control considerations contained within the SOC audit reports (or equivalent) for applicable subservice providers and verified the controls were satisfactorily implemented and in place within their environment.	No exceptions noted.

ORGANIZATION AND ADMINISTRATION: Controls provide reasonable assurance that the organizational structure provides for management oversight, segregation of duties and administrative practices.			
1.0	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
1.9	Management requires all subservice organizations without a SOC report to be evaluated for security and overall data risk on an annual basis.	**Observation, Inquiry, and Inspection:** Inquired of client management, observed the generation of a list of subservice organizations without a SOC report during the audit period, inspected the list, and determined there were none. Therefore, no samples were available to test. However, obtained and reviewed the Vendor Management Policy, and verified management would require all subservice organizations without a SOC report to be evaluated for security and overall data risk on an annual basis.	Control is designed effectively; however, no samples were available to test the operating effectiveness of the control.

CUSTOMER SERVICE: Controls provide reasonable assurance that customer inquiries or requests are addressed and resolved in a timely manner.			
2.0	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
2.1	Management has established formal procedures to guide the customer service process. The procedures are reviewed at least annually.	**Inspection:** Obtained and reviewed the Customer Issues Procedures. Verified procedures were in place to guide the customer service process and the procedures were reviewed in the past 12 months.	No exceptions noted.
2.2	Customer support is available 24-hours from Sunday through Friday via telephone or e-mail.	**Inspection:** Obtained and reviewed screenshots of customer support availability within the Company's website. Verified customer support was available 24-hours from Sunday through Friday via telephone or e-mail.	No exceptions noted.
2.3	Customer service issues and support requests are managed via a formalized process or project tracking system.	**Inspection:** Obtained and reviewed the issue ticket for sampled customer service issues during the audit period. Verified customer service issues and support requests were managed via a formalized process or project tracking system.	No exceptions noted.
2.4	An open project tracking report is reviewed by management on a weekly basis to ensure customer service inquiries or requests are addressed and resolved timely.	**Inspection:** Obtained and reviewed the project tracking reports for sampled weeks during the audit period. Verified an open project tracking report was reviewed by management on a weekly basis to ensure customer service inquiries or requests were addressed and resolved timely.	No exceptions noted.

LOGICAL SECURITY: Controls provide reasonable assurance that logical access to Company network resources is restricted to properly authorized individuals and programs.			
3.0	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
3.1	Security policies have been reviewed and approved by management. The policies and procedures are reviewed at least annually.	**Inspection:** Obtained and reviewed the Integral Security Policy and Security Handbook. Verified security policies were in place and reviewed in the past 12 months.	No exceptions noted.
3.2	The Company makes its IT security policies available to all employees.	**Inspection:** Obtained and reviewed the Integral Security Policy and a screenshot of the policy on the Company's intranet. Verified the Company makes its IT security policies available to all employees.	No exceptions noted.
3.3	New or modified access must be authorized and approved by Human Resources prior to granting access or changing existing access to systems.	**Inspection:** Obtained and reviewed the access requests for the sampled employees hired during the audit period. Verified new access was authorized and approved by Human Resources prior to granting access. Additionally, verified there were no access modifications during the audit period.	No exceptions noted.
3.4	Terminated employees' network access is removed in a timely manner upon separation from the Company.	**Inspection:** Obtained and reviewed the termination tickets and checklists for the sampled employees terminated during the audit period. Verified terminated employees' network access was removed in a timely manner upon separation from the Company.	No exceptions noted.
3.5	System administrator access within the internal network domain and the network domain at the hosted environment is restricted to authorized user accounts and in line with their job function.	**Inspection:** Obtained and reviewed a screenshot of domain administrators and reconciled with the list of active employees during the audit period. Verified system administrator access within the internal network domain and the network domain at the hosted environment was restricted to authorized user accounts and in line with their job function.	No exceptions noted.

LOGICAL SECURITY: Controls provide reasonable assurance that logical access to Company network resources is restricted to properly authorized individuals and programs.			
3.0	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
3.6	The default administrative operating system password has been changed, and all unnecessary default accounts have been disabled.	**Inspection:** Obtained and reviewed screenshots of the administrator account properties. Verified the default administrative operating system password had been changed, and all unnecessary default accounts had been disabled.	No exceptions noted.
3.7	A user access review of all network accounts is performed annually to ensure appropriate logical access is maintained.	**Inspection:** Obtained and reviewed the user access review performed during the audit period. Verified a user access review of all network accounts was performed annually to ensure appropriate logical access was maintained.	No exceptions noted.
3.8	Users are required to authenticate via a user account ID and password before being granted access to the internal network domain.	**Inspection:** Obtained and reviewed the domain user listing and reconciled with the active employee list. Verified users were required to authenticate via a user account ID and password before being granted access to the internal network domain.	No exceptions noted.
3.9	The internal network domain is configured to enforce the following password requirements: • Maximum Password Age • Minimum Password Length • Invalid Password Lockout • Passwords are stored in encrypted format • Complexity	**Inspection:** Obtained and reviewed screenshots of the network password and lockout policies. Verified the internal network domain was configured to enforce the following password requirements: • Maximum Password Age • Minimum Password Length • Invalid Password Lockout • Passwords are stored in encrypted format • Complexity	No exceptions noted.

LOGICAL SECURITY: Controls provide reasonable assurance that logical access to Company network resources is restricted to properly authorized individuals and programs.			
3.0	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
3.10	Data transmissions between the Company, its clients and any bank are secure using encryption technology.	**Inspection:** Obtained and reviewed the SSL certificates. Verified data transmissions between the Company, its clients and any bank were secure using encryption technology.	No exceptions noted.
3.11	Vulnerability scans are performed on a quarterly basis to identify risks to the Company's information assets.	**Inspection:** Obtained and reviewed the vulnerability scan reports for sampled quarters during the audit period. Verified vulnerability scans were performed on a quarterly basis to identify risks to the Company's information assets.	No exceptions noted.
3.12	A penetration test is performed annually to identify risks to the Company's information assets.	**Inspection:** Obtained and reviewed the penetration test report. Verified a penetration test was performed annually to identify risks to the Company's information assets.	No exceptions noted.
3.13	Remote employee access to the Company's network is permitted using a VPN connection which requires unique username and password authentication.	**Inspection:** Obtained and reviewed the VPN configuration. Verified remote employee access to the Company's network was permitted using a VPN connection which requires unique username and password authentication.	No exceptions noted.

PHYSICAL SECURITY: Controls provide reasonable assurance that physical access to facilities and computer equipment located in the corporate data center, to storage media, and to client data are protected in a secure environment and restricted to properly authorized individuals.			
4.0	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
4.1	Physical security policies exist to guide personnel in the performance of their duties. The policy is reviewed at least annually.	**Inspection:** Obtained and reviewed the Employee Handbook and evidence of review. Verified physical security policies exists to guide personnel in the performance of their duties and the policy was reviewed in the past 12 months.	No exceptions noted.
4.2	The Company facility has a building access system that monitors access to doors.	**Inspection:** Obtained and reviewed the badge access reports. Verified the Company facility has a building access system that monitored access to doors.	No exceptions noted.
4.3	A termination checklist is used by Human Resources to ensure that terminated employees' access badges or keys are returned and deactivated as a component of the termination process.	**Inspection:** Obtained and reviewed the termination checklist for the sampled employees terminated during the audit period. Verified a termination checklist was used by Human Resources to ensure that terminated employees' access badges or keys were returned and deactivated as a component of the termination process.	No exceptions noted.
4.4	Access to the off-site data center(s) is restricted to authorized personnel.	**Inspection:** Obtained and reviewed the datacenter access review report. Verified access to the off-site data center(s) was restricted to authorized personnel. _____ This control is also the responsibility of Equinix.	No exceptions noted.

PHYSICAL SECURITY: Controls provide reasonable assurance that physical access to facilities and computer equipment located in the corporate data center, to storage media, and to client data are protected in a secure environment and restricted to properly authorized individuals.			
4.0	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
4.5	Visitors to the Company facility must be escorted throughout the facility.	**Inspection:** Obtained and reviewed the Security Access Policy. Verified visitors to the Company facility must be escorted throughout the facility.	No exceptions noted.
Equinix is responsible for restricting physical access to data center facilities, backup media, and other system components including network devices and servers.			

Computer Operations: Controls provide reasonable assurance that a system is in place to track network, system, and application problems, and ensure effective and timely resolution.			
5.0	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
5.1	Systems are in place to log network security events and the Information Systems/IT group is notified in the event security thresholds are exceeded.	**Inspection:** Obtained and reviewed screenshots of the system log notification system. Verified systems were in place to log network security events and the Information Systems/IT group was notified in the event security thresholds were exceeded.	No exceptions noted.
5.2	When an incident is detected or reported, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined procedures.	**Inspection:** Obtained and reviewed the incident tickets for the sampled incidents during the audit period. Verified when an incident was detected or reported, a defined incident management process was initiated by authorized personnel. Additionally, corrective actions were implemented in accordance with defined procedures.	No exceptions noted.
5.3	Anti-virus software is installed on workstations and servers and is configured to scan on a continuous basis.	**Inspection:** Obtained and reviewed the antivirus installation report. Verified anti-virus software was installed on workstations and servers and was configured to scan on a continuous basis.	No exceptions noted.
5.4	Anti-virus software provider pushes updates to the installed anti-virus software multiple times each day as new updates/signatures become available.	**Inspection:** Obtained and reviewed the anti-virus configurations. Verified the anti-virus software provider pushed updates automatically as new updates/signatures become available.	No exceptions noted.

SDLC & CHANGE CONTROL: SDLC Controls provide reasonable assurance that system changes are authorized, tested and approved prior to implementation and usage.			
6.0	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.1	Management has established a formal process change management. The process requires changes to be authorized, tested, approved, and documented. The process is reviewed at least annually by management.	**Inspection:** Obtained and reviewed the Change Management Process and management's review. Verified management had established a formal change management process which was reviewed annually and required changes to be authorized, tested, approved, and documented.	No exceptions noted.
6.2	A formal change request ticketing system is used to track all change requests. All changes must be properly reviewed and approved before being implemented to production.	**Inspection:** Obtained and reviewed the change tickets for sampled system changes during the audit period. Verified a formal change request ticketing system was used to track all change requests. All changes were properly reviewed and approved before being implemented to production.	No exceptions noted.
6.3	Quality assurance (QA) testing is performed before any change is released as final into the production system.	**Inspection:** Obtained and reviewed the quality assurance test reports for sampled bi-weekly releases during the audit period. Verified quality assurance (QA) testing was performed before any change was released as final into the production system.	No exceptions noted.
6.4	All Company designed application programs have a separate test and production environment.	**Inspection:** Obtained and reviewed screenshots of the separate testing and production environments. Verified all Company designed application programs had a separate test and production environment.	No exceptions noted.

SDLC & CHANGE CONTROL: SDLC Controls provide reasonable assurance that system changes are authorized, tested and approved prior to implementation and usage.			
6.0	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.5	A list of required changes to the software, with target completion dates, is maintained and reviewed by management, bi-weekly to ensure required changes are completed in a timely manner.	**Inspection:** Obtained and reviewed the release planning tickets for the sampled bi-weekly releases during the audit period. Verified a list of required changes to the software, with target completion dates, was maintained and reviewed by management, bi-weekly to ensure required changes were completed in a timely manner.	No exceptions noted.
6.6	A segregation of duties exists in that developers are not allowed to deploy their own development changes to the production environment.	**Inspection:** Obtained and reviewed the software access groups configuration settings. Verified a segregation of duties exists in that developers were not allowed to deploy their own development changes to the production environment.	No exceptions noted.

BACKUP AND RECOVERY: Controls provide reasonable assurance that backup and recovery procedures are in place to ensure the continuity of operations and preserve the integrity of programs and data.			
7.0	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.1	Documented system backup and retention policies and procedures are in place to guide personnel through the backup and retention process.	**Inspection:** Obtained and reviewed the Backup and Retention Policy. Verified documented system backup and retention policies and procedures were in place to guide personnel through the backup and retention process.	No exceptions noted.
7.2	Backups are performed for all client operating systems, database and application software and confidential client data managed by the Company.	**Inspection:** Obtained and reviewed the backup configuration. Verified backups were performed for all client operating systems, database and application software and confidential client data managed by the Company.	No exceptions noted.
7.3	The automated backup system is configured to notify computer operations personnel the results of each backup job.	**Inspection:** Obtained and reviewed the backup system configuration and notification email group. Verified the automated backup system was configured to notify computer operations personnel the results of each backup job.	No exceptions noted.
7.4	Restore tests from backup media are performed on at least on an annual basis.	**Inspection:** Obtained and reviewed a screenshot of the backup restore test. Verified restore tests from backup media were performed on at least on an annual basis.	No exceptions noted.

CLIENT SETUP PROCEDURES: Controls provide reasonable assurance that new clients are set up with complete and accurate information in a timely manner. Controls provide reasonable assurance that changes requested by clients are processed completely, accurately and timely.			
8.0	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
8.1	New client on-boarding procedures exist to ensure each new client is on-boarded in a complete, accurate and timely manner. Such processes are reviewed at least annually.	**Inspection:** Obtained and reviewed the client on-boarding procedures. Verified new client on-boarding procedures existed to ensure each new client was on-boarded in a complete, accurate and timely manner. Such processes were reviewed at least annually.	No exceptions noted.
8.2	A new client on-boarding information checklist is used to ensure each client is set up with complete and accurate information. The checklist is monitored by IT department personnel to ensure timely onboarding.	**Inspection:** Obtained and reviewed the onboarding checklist for sampled new customers during the audit period. Verified a new client on-boarding information checklist was used to ensure each client was set up with complete and accurate information. Additionally, verified the checklist was monitored by IT department personnel to ensure timely onboarding.	No exceptions noted.
8.3	Access to the client application is restricted to authorized personnel.	**Inspection:** Obtained and reviewed the client access provisioning tickets for the sampled clients during the audit period. Verified access to the client application was restricted to authorized personnel.	No exceptions noted.
8.4	Training is provided and performed on a timely basis for each new client, so they understand how to use the software. This training includes webinars for new software releases, if applicable.	**Inspection:** Obtained and reviewed the onboarding checklist for sampled new customers during the audit period. Verified training was provided and performed on a timely basis for each new client, so they understood how to use the software. The training included webinars for new software releases.	No exceptions noted.

SYSTEM SURVEILLANCE: Controls provide reasonable assurance that Integral monitors that the applications are working properly.			
9.0	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
9.1	Monitoring systems are deployed to alert the Company of any erratic system activities.	**Inspection:** Obtained and reviewed screenshots of the system monitoring and alert system. Verified monitoring systems were deployed to alert the Company of any erratic system activities.	No exceptions noted.
9.2	The Company has a process to ensure the performance of application systems is continuously monitored and exceptions are reported in a timely and comprehensive manner.	**Inspection:** Obtained and reviewed screenshots of the application and network monitoring system. Verified the Company had a process to ensure the performance of application systems was continuously monitored and exceptions were reported in a timely and comprehensive manner.	No exceptions noted.

POSITION REVIEW: Controls provide reasonable assurance that Integral monitors for positions in the system in the event that such position has made the system unstable or nonresponsive.			
10.0	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
10.1	Management has established a formal policy covering all position review procedures. The policy is reviewed at least annually.	**Inspection:** Obtained and reviewed the Customer Issue Procedure and the Enterprise Risk Management Procedure. Verified management established a formal policy covering all position review procedures. The policy was reviewed at least annually.	No exceptions noted.
10.2	The Company monitors for risk positions during trading hours using real-time monitoring and alerts.	**Inspection:** Obtained and reviewed a screenshot of the FXCloud Monitor alert dashboard and example alert notification. Verified the Company monitored for risk positions during trading hours using real-time monitoring and alerts.	No exceptions noted.
10.3	The Company notifies customers or providers of a risk position immediately when a risk position is detected.	**Inspection:** Obtained and reviewed a screenshot of the risk position notification configuration. Verified the Company notified customers or providers of a risk position immediately when a risk position was detected.	No exceptions noted.

SECTION FIVE

Other Information Provided by Integral Development Corporation

OTHER INFORMATION PROVIDED BY INTEGRAL DEVELOPMENT CORPORATION

The information included in this section of the report is presented by Integral Development Corporation to provide additional information to user entities and is not part of Integral's description of controls placed in operation. The information in this section has not been subjected to the procedures applied in the examination of the description of controls related to the control objectives and, accordingly, CyberGuard Compliance, LLP expresses no opinion on it.

1 Disaster Recovery Plan

Integral undergoes an annual test of their disaster recovery plan. Integral's disaster recovery plan allows it to establish and implement procedures to recover the Organization's technology platform from catastrophic events which deny access to the normal facility. The disaster recovery plan refers to an IT focused plan designed to restore operability of the production system at an alternate site after an emergency.