A-LIGN

Fin Technologies, Inc.
dba Mantl's

Type 2 SOC 1

2023

MANTL

REPORT ON MANAGEMENT'S DESCRIPTION OF FIN TECHNOLOGIES, INC. DBA MANTL'S' SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

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

April 1, 2022 to March 31, 2023

Table of Contents

SECTION 1

ASSERTION OF FIN TECHNOLOGIES, INC. DBA MANTL'S' MANAGEMENT

MANTL

Assertion of Fin Technologies, Inc. dba Mantl's' Management

April 12, 2023

We have prepared the description of Fin Technologies, Inc. dba Mantl's' ('Mantl' or 'the Company') information technology general control system for the Financial Software-as-a-Service Platform Services System entitled "Description of Fin Technologies, Inc. dba Mantl's' Financial Software-as-a-Service Platform Services System" throughout the period April 1, 2022 to March 31, 2023, (description) for user entities of the system during some or all of the period April 1, 2022 to March 31, 2023, and their user auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

Mantl uses Alloy for KYC/AML identity verification services, First Data for credit card processing and payment services, Plaid for banking data API system services, SendGrid for transactional and marketing email platform services, and Google Cloud Platform ('GCP') for cloud hosting services (collectively, the 'subservice organizations'). The description includes only the control objectives and related controls of Mantl and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by Mantl in the description can be achieved only if complementary subservice organization controls assumed in the design of Mantl's controls are suitably designed and operating effectively, along with the related controls at Mantl. The description does not extend to controls of the subservice organizations.

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

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

a. The description fairly presents the information technology general control system made available to user entities of the system during some or all of the period April 1, 2022 to March 31, 2023 as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

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

        (1) the types of services provided.

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

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

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

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

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

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

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

iii. does not omit or distort information relevant to the scope of the information technology general control system, while acknowledging that the description is prepared to meet the common needs of broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the Financial Software-as-a-Service Platform Services information technology general control system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period April 1, 2022 to March 31, 2023, to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of Mantl's controls throughout the period April 1, 2022 to March 31, 2023. The criteria we used in making this assertion were that:

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

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

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

Ben Conant
Chief Technology Officer
Fin Technologies, Inc. dba Mantl's

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Fin Technologies, Inc. dba Mantl's

Scope

We have examined Fin Technologies, Inc. dba Mantl's ('Mantl' or 'the Company') description of its information technology general control system for the Financial Software-as-a-Service Platform Services entitled "Description of Fin Technologies, Inc. dba Mantl's' Financial Software-as-a-Service Platform Services System" throughout the period April 1, 2022 to March 31, 2023, (description) and the suitability of the design and operating effectiveness of Mantl's controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Assertion of Fin Technologies, Inc. dba Mantl's' Management" (assertion).

Mantl uses Alloy for KYC/AML identity verification services, First Data for credit card processing and payment services, Plaid for banking data API system services, SendGrid for transactional and marketing email platform services, and Google Cloud Platform ('GCP') for cloud hosting services (collectively, the 'subservice organizations'). The description includes only the control objectives and related controls of Mantl and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by Mantl can be achieved only if complementary subservice organization controls assumed in the design of Mantl are suitably designed and operating effectively, along with the related controls at Mantl. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of Mantl's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design and operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period April 1, 2022 to March 31, 2023. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved
- Evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization in their assertion

Independence and Ethical Responsibilities

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

Inherent Limitations

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

Description of Tests of Controls

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

Opinion

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

a. the description fairly presents the information technology general control system that was designed and implemented throughout the period April 1, 2022 to March 31, 2023.
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 April 1, 2022 to March 31, 2023 and subservice organizations and user entities applied the complementary user entity controls contemplated in the design of Mantl's controls throughout the period April 1, 2022 to March 31, 2023.

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period April 1, 2022 to March 31, 2023, if complementary subservice organization and user entity controls assume in the design of Mantl's controls operated effectively throughout the period April 1, 2022 to March 31, 2023.

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 Mantl, user entities of Mantl's information technology general control system during some or all of the period April 1, 2022 to March 31, 2023, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
April 12, 2023

SECTION 3

DESCRIPTION OF FIN TECHNOLOGIES, INC. DBA MANTL'S' FINANCIAL SOFTWARE-AS-A-SERVICE PLATFORM SERVICES SYSTEM

OVERVIEW OF OPERATIONS

Company Background

Fin Technologies, Inc. dba Mantl is a customer-centric outer core ecosystem that gives banks and credit unions the flexibility to innovate using modern technology, while owning their brand throughout the entire customer lifecycle.

In their collective experience building everything from modern consumer FinTech companies to core banking systems, they saw a rift where new FinTech companies were able to leverage the latest technologies, while banks and credit unions - tethered to their outdated systems and vendors - struggled to remain competitive in the digital age.

That divide continues today. So, they pulled together a team with deep industry knowledge, and expertise in systems architecture, UI/UX, and data security & analysis to reunite the worlds of banking and technology.

Mantl was part of the Techstars' NYC Summer 2016 program and is Venture Capital-backed with corporate headquarters in New York City, New York.

Description of Services Provided

Financial SaaS Services

Mantl (mantl.com) provides a Software-as-a-Service platform that integrates services across financial institutions and provides customized application solutions for banks and credit unions.

Transactions Processing & Reporting

Mantl books the account and subservices on behalf of the customer and transfers customer information into the core banking application. Mantl obtains a valid response that is actionable from the KYC/AML decision engine to verify customer identity and reduce fraud risk. Mantl facilitates new account funding via ACH, or debit card/credit card processing to initiate new account funding transactions. In addition, Mantl successfully books the account and its related sub-products and sub-services in the core banking system.

Significant Events

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

Functional Areas of Operation

The Mantl staff provide support for the above service in each of the following functional areas:

- CEO - Development and mission accomplishment
- CTO - Planning, budgeting, and performance including information security
- Director of Engineering - Confidentiality, integrity, and availability of the IT systems and data
- Core Integration Architect - Core integration
- Software Engineers - Development and testing

Boundaries of the System

The scope of this report includes the Financial Software-as-a-Service Platform Services System performed in the San Francisco, California facility.

Subservice Organizations

This report does not include the KYC/AML identity verification services provided by Alloy at the New York, New York facility, the credit card processing and payment services provided by First Data at the Boston, Massachusetts facility, the banking data API system services provided by Plaid at the San Francisco, California facility, the transactional and marketing email platform services provided by SendGrid at the Denver, Colorado facility and the cloud hosting services provided by GCP at multiple US facilities.

Subservice Description of Services

Alloy - is the Identity Decisioning Platform that assists banks and fintech companies automate their decisions for onboarding, transaction monitoring and credit underwriting.

First Data - Provides secure and innovative payment technology and services solutions to merchants, including small-and mid-sized businesses, financial institutions, and government agencies around the world.

Plaid- Instant Account Verification (IAV) provider allowing end users to easily obtain their bank account and routing numbers by providing their bank account login information. Plaid outsources its cloud hosting services to Amazon Web Services (AWS).

SendGrid- Customer communication platform for transactional and marketing email. SendGrid outsources its data center hosting services to Steadfast data center.

GCP - Cloud services provider for Mantl servers, infrastructure, databases and other cloud building blocks.

Complementary Subservice Organization Controls

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

The following subservice organization controls should be implemented by Alloy to provide additional assurance that the control objectives described within this report are met:

Subservice Organization - Alloy	
Control Objective	**Control**
Information Security	Customers are granted access to the production applications based on fraud scores and authentication tests.

The following subservice organization controls should be implemented by First Data to provide additional assurance that the control objectives described within this report are met:

Subservice Organization - First Data	
Control Objective	**Control**
Information Security	Electronic files with approved funding transactions from customers are processed accurately and timely to initiate funding of new customer accounts via ACH or debit card/credit processing.

The following subservice organization controls should be implemented by Plaid to provide additional assurance that the control objectives described within this report are met:

Subservice Organization - Plaid	
Control Objective	**Control**
Account Setup	Plaid has a defined process for granting customers access to Plaid's API which is a Plaid product offering. Customers must be registered prior to obtaining access to Plaid's information system and services.
Data Communications	All emails sent from the Plaid's server are encrypted.
	Customer authentication and session data is encrypted while in transit.

The following subservice organization controls should be implemented by SendGrid to provide additional assurance that the control objectives described within this report are met:

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

The following subservice organization controls should be implemented by GCP to provide additional assurance that the control objectives described within this report are met:

Subservice Organization - GCP	
Control Objective	**Control**
Information Security	Physical access to data centers is approved by an authorized individual.
	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
	Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.

Subservice Organization - GCP	
Control Objective	**Control**
	Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
	Physical access points to server locations are managed by electronic access control devices.
	Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Data Communications	Critical data is stored in encrypted format using software supporting AES-256.
Computer Operations - Availability	Google-owned data centers are protected by fire detection and suppression systems.
	Google-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
	Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Google-owned data centers.
	Google-owned data centers have generators to provide backup power in case of electrical failure.
	Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies.
	GCP performs periodic reviews of colocation service providers to validate adherence with GCP security and operational standards.
	GCS-Specific - Google Cloud Storage performs continuous integrity checks of the data at rest. Objects are continuously validated against their checksums to prevent object corruption.
	GCS-Specific - When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.
	GCS-Specific - Objects are stored redundantly across multiple fault-isolated facilities.
	GCS-Specific - The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.
	Google Cloud SQL-Specific - If enabled by the customer, Google Cloud SQL backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.
	Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.

Subservice Organization - GCP	
Control Objective	**Control**
	Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.
	Critical GCP system components are replicated across multiple Availability Zones and backups are maintained.
	Backups of critical GCP system components are monitored for successful replication across multiple Availability Zones.
Computer Operations - Backup	Critical data is stored in encrypted format using software supporting AES-256.

Mantl management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Mantl performs monitoring of the subservice organizations controls, including the following procedures:

- Reviewing service-related communications and attestation reports about services provided by the subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organizations

Significant Changes Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization last review.

CONTROL ENVIRONMENT

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 Mantl's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Mantl's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

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

- Formally, documented code of conduct communicates entity values and behavioral standards to personnel
- Comprehensive Information Security policies and procedures require employees to sign an acknowledgment form upon hiring and annually to confirm that they understand their responsibility for adhering to the policies and procedures contained within the manual
- Employees are required to sign a Confidentiality Agreement and non-disclosure statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties
- Pre-hire screening of potential employees includes thorough background investigations

Commitment to Competence

Mantl's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

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

- Management screens technical candidates thoroughly to ensure that they possess the requisite skills to fulfill their responsibilities at Mantl
- Annual Security Awareness Training is attended by personnel which focuses on maintaining the security, availability and confidentiality of the proprietary and customer-servicing systems and related data
- Management supports employee training required to maintain technical proficiency and professional licenses held by employees
- Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of the Mantl internal and information security controls

Management's Philosophy and Operating Style

Mantl'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.

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

- Business and industry risks discussed during the periodic management risk assessment meetings, discussed below, and that impact employees are communicated to the employee base via conferences or email by Management
- Annual Security Awareness Training is attended by personnel which focuses on maintaining the security, availability and confidentiality of the proprietary and customer-servicing systems and related data
- Mantl's management team has frequent, direct communication via "stand-up" and similar meetings with employees to ensure employees understand the most critical tasks and receive clear guidance from management on those tasks

Organizational Structure and Assignment of Authority and Responsibility

Mantl's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Mantl's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

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

- Organizational charts are in place to communicate key areas of authority and responsibility. These charts are communicated to employees and updated as needed

- Key controls that help ensure the security, availability and confidentiality of the products and services provided to customers are assigned to employee “owners” who are responsible for the timely execution of the controls

In addition to the annual Security Awareness Training, the employee-base would receive notification in the event that Mantl experienced a significant security breach or other incident in accordance with the Incident Response policy and procedures.

Human Resources Policies and Practices

Mantl's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensure the service organization is operating at maximum efficiency. Mantl's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

- New employees are required to sign acknowledgement forms for the Confidentiality Agreement and Code of Conduct following new hire orientation within the first week of employment
- Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of the Mantl internal and information security controls
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

RISK ASSESSMENT

Mantl holds an annual risk assessment that quantifies the impact and probability of each risk, the controls in place that mitigate each risk, and management's plan of action with regards to all residual risks over the next twelve months. Mantl identifies and manages risks that would jeopardize the achievement of strategic objectives and risks to the Information Technology (IT) infrastructure supporting its products, as well as specific fraud risks that could threaten the security, confidentiality, and availability of customer data. Mantl identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

Management holds monthly Risk and Security Team meetings which include key members of the executive team as well as other key individuals to address the IT risks identified and tracked via the automated ticket workflow management system.

This process has identified risks resulting from the nature of the services provided by Mantl, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance risk - legal and regulatory changes

Mantl has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm’s internal controls. The approach is intended to align the entity’s strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Mantl attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

CONTROL OBJECTIVE AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

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

Selection and Development of Control Activities Specified by the Service Organization

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

Mantl'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. Although the control objectives and related control activities are included in Section 4, they are, nevertheless, an integral part of Mantl's description of the Financial SaaS Services System.

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

MONITORING

Mantl monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

As noted throughout the system description, Mantl has deployed a number of system and data monitoring tools that control owners are responsible for monitoring and responding in a timely fashion. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications. Issues noted that require changes to be made to information systems supporting customers or the Mantl infrastructure are tracked via the ticketing system and adhere to the change management procedures and controls through resolution.

Management's close involvement in Mantl's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision to address any control's weakness is made based on whether the incident was isolated or requires a change in the Company's procedures or personnel. The goal of this process is to ensure the security, availability and confidentiality of the systems and data and to maximize the performance of Mantl's personnel. The monthly Risk and Security Team meetings are a key component of Mantl's monitoring of the monitoring tools, the risk and threat landscape, and the execution of controls by Mantl personnel.

Vendor Management

Mantl has defined the following activities to oversee controls performed by vendors that could impact on the Financial SaaS Services System:

- Reviewing attestation reports over services provided by vendors
- Monitoring external communications, such as customer complaints relevant to the services by the vendors

Reporting Deficiencies

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

INFORMATION AND COMMUNICATION SYSTEMS

Information Systems

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

Infrastructure

Primary infrastructure used to provide Mantl's Financial Software-as-a-Service Platform Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Web Servers	Docker containers running on google Kubernetes engine with nginx ingress	Hosts files to support the web application and transaction server
Databases	Google Cloud SQL postgres, Google firestore, BigQuery	Stores encrypted database data to support the web application and transaction server
Firewalls	Cloud armor and Cloudflare	Filters traffic into and out of the private network supporting the application services
Switches	GCP Managed	Connects devices on the corporate network by sending messages to the specific device(s) that need to receive it
Routers	GCP Managed	Connects multiple networks and forward packets within the network or other networks

Software

Primary software used to provide Mantl's Financial SaaS Services System includes the following:

Primary Software	
Software	**Purpose**
Google Cloud Storage	Perform scheduled backups of client data according to the requirements defined by the customer and provide status alerts to operations personnel
Cloudflare	Web application firewall and DNS
Google Cloud Storage	Storage
Orca Security Platform	Monitoring applications are used to provide monitoring, alert, and notification services for the hosted client environments
GCP Identity Access Management (IAM) and strongDM	Provides user administration including access control policies for authentication of users, commands, and audit logging
GIT	Version control software
Jira	Provides ticketing functionality to document and track issues and requests for the client environment
Slack	Monitoring for alerts such as file integrity, security, availability
Cloud Strike	Antivirus
JAMF	Apple mobile device management
LogDNA	Application log management and analysis tool
Buildkite	CI/CD pipeline tool
Okta	IAM and SSO
Terraform	Infrastructure as code
Vault	Storing token, passwords, certificates, encryption keys
Auth0	Authentication and authorization service to access applications
BetterCloud	Onboarding and offboarding
1Password	Password Manager
Greenhouse	Applicant tracking system and recruiting software
GSuite	Email and google apps
Orca Security	Infrastructure security monitoring
Dropbox	File Storage

Communication Systems

Communication is an integral component of Mantl's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Mantl, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Mantl personnel via email messages.

COMPLEMENTARY USER ENTITY CONTROLS

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

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

Control Objective 1 - Information Security

1. User entities are responsible for documenting information security policies and procedures.
2. User entities are responsible for granting appropriate access to new hires on their systems.
3. User entities are responsible for revoking access for terminations on their systems.
4. User entities are responsible for utilizing role-based security on their systems.
5. User entities are responsible for restricting administrative access on their systems.
6. User entities are responsible for utilizing strong password parameters on their systems.
7. User entities are responsible for utilizing account lockout and timeout on their systems.
8. User entities are responsible for logging and alerting unauthorized activity and threats on their systems.
9. User entities are responsible for reviewing access on a periodic basis on their systems.
10. User entities are responsible for restricting access to sensitive data on their systems.

Control Objective 2 - Data Communications

11. User entities are responsible for documenting information security policies and procedures.
12. User entities are responsible for utilizing firewalls to filter unauthorized inbound network traffic from the internet and deny all types of traffic not explicitly authorized by the firewall system rules.
13. User entities are responsible for limiting access to their firewalls.
14. User entities are responsible for securing data transmissions using strong encryption.
15. User entities are responsible for utilizing multi-factor authentication for remote access to their systems.

16. User entities are responsible for revoking access for their terminated employees.
17. User entities are responsible for performing vulnerability scans and penetration tests on their systems on a periodic basis.
18. User entities are responsible for monitoring for security threats on their systems.
19. User entities are responsible for utilizing antivirus on their workstations and updating virus definitions regularly.

Control Objective 3 - Change Control

20. User entities are responsible for documenting change control policies and procedures.
21. User entities are responsible for authorizing, testing, and approving changes by management prior to implementation.
22. User entities are responsible for tracking system changes in a change management tracking system.
23. User entities are responsible for utilizing version control systems.
24. User entities are responsible for separating development, test, and production environments.
25. User entities are responsible for limiting access to development, test, and production and utilizing file integrity monitoring when segregations of duties incompatibilities exist.
26. User entities are responsible for communicating bugs and requesting enhancements.
27. User entities are responsible for user acceptance testing and approval.
28. User entities are responsible for clearly communicating requirements.

Control Objective 4 - Availability

29. User entities are responsible for documenting incident response procedures.
30. User entities are responsible for tracking incidents in a ticket tracking application.
31. User entities are responsible for monitoring ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.
32. User entities are responsible for performing backups on a regular basis.
33. User entities are responsible for monitoring backup failures.
34. User entities are responsible for documenting business continuity and disaster recovery plans.
35. User entities are responsible for performing vulnerability scans and penetration tests on a periodic basis.
36. User entities are responsible for installing antivirus on workstations and updating definitions regularly.

Control Objective 5 - Backups

37. User entities are responsible for documenting backup and restore procedures.
38. User entities are responsible for automatically backing up systems on a regular schedule.
39. User entities are responsible for monitoring backups for failures.
40. User entities are responsible for documenting business continuity and disaster recovery plans.
41. User entities are responsible for testing business continuity and disaster recovery plans on a periodic basis.
42. User entities are responsible for storing backups and/or data in an encrypted format.

Control Objective 6 - Account Setup

43. User entities are responsible for taking ownership of the account once the account has been created.
44. User entities are responsible for notifying Mantl of any issues in a timely manner.

SECTION 4

DESCRIPTION OF FIN TECHNOLOGIES, INC. DBA MANTL'S' CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

GUIDANCE REGARDING DESCRIPTION OF FIN TECHNOLOGIES, INC. DBA MANTL'S' CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

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

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

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

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

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

CONTROL AREA 1 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition, or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.1	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
1.2	Logical access to systems is granted to an employee as a component of the hiring process.	Inspected the hiring procedures, system user access listings, and the user access request ticket for a sample of new hires to determine that logical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.
1.3	Logical access to systems is revoked as a component of the termination process.	Inspected the termination procedures, system user access listings, and the completed user offboarding checklist for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
1.4	Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Security Manager regarding privileged access to sensitive resources to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Inspected the listings of users with administrative access to the network, operating system, database, application, and Identity- Aware Proxy (IAP) to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
1.5	Network administrative access is restricted to user accounts accessible by authorized personnel.	Inquired of the Security Manager regarding network administrative access to determine that network administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.

CONTROL AREA 1 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition, or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the network administrator listing and access rights to determine that network administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
1.6	Network are configured to enforce the following password requirements: • Minimum password length • Password History	Inspected the network password settings to determine that the network was configured to enforce the following password requirements: • Minimum password length • Password History	No exceptions noted.
	Operating System (Google Container Optimized)		
1.7	Operating system administrative access is restricted to user accounts accessible by authorized personnel.	Inquired of the Security Manager regarding operating system administrative access to determine that operating system administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Inspected the operating system administrator listing and access rights to determine that operating system administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
1.8	Operating systems are configured to enforce password requirements that include: • Minimum password length • Password History	Inspected the operating system password settings to determine that operating systems were configured to enforce password requirements that include: • Minimum password length • Password History	No exceptions noted.
1.9	Operating system account lockout settings are in place that include session timeout.	Inspected the operating system account lockout settings to determine that operating system account lockout settings were in place that included session timeout.	No exceptions noted.

CONTROL AREA 1 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition, or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Database (PostgreSQL)		
1.10	Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database user access listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
1.11	Database administrative access is restricted to user accounts accessible by authorized personnel.	Inquired of the Security Manager regarding database administrative access to determine that database administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Inspected the database administrator listing and access rights to determine that database administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
	Application (MANTL Platform)		
1.12	Application administrative access is restricted to user accounts accessible by authorized personnel.	Inquired of the Security Manager regarding application administrative access to determine that application administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Inspected the application administrator user listing to determine that application administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
1.13	The application is configured to enforce password requirements that include: • Password length • Complexity	Inspected the application password settings to determine that application was configured to enforce password requirements that include: • Password length • Complexity	No exceptions noted.

CONTROL AREA 1 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition, or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.14	Application account lockout settings are in place that include: • Account lockout threshold • Manual account reset by an administrator	Inspected the application account lockout settings to determine that application account lockout settings were in place that included: • Account lockout threshold • Manual account reset by an administrator	No exceptions noted.
	Remote Access (Identity Aware Proxy)		
1.15	The ability to administer Identity-Aware Proxy (IAP) access is restricted to user accounts accessible by authorized personnel.	Inquired of the Security Manager regarding IAP administrator access to determine that the ability to administer IAP access was restricted to user accounts accessible by authorized personnel. Inspected the IAP administrator listing and access rights to determine that the ability to administer IAP access was restricted to user accounts accessible by authorized personnel.	No exceptions noted. No exceptions noted.
1.16	IAP users are authenticated via multi-factor authentication by Okta prior to being granted remote access to the system.	Inspected the Okta policy settings to determine that IAP users were authenticated via multi-factor authentication by Okta prior to being granted remote access to the system.	No exceptions noted.

CONTROL AREA 2 **DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that data transmissions between the service organization and its clients are complete, accurate, and secure and that data received is posted to the relevant systems in accordance with the Company's guidelines.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.1	Policies and procedures are in place to guide users in the governance of the firewall, router, telecommunications, and network practices.	Inspected the information security policies and procedures to determine that policies and procedures were in place to guide users in the governance of the firewall, router, telecommunications, and network practices.	No exceptions noted.
2.2	A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram and firewall rulesets to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
2.3	The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and firewall rulesets to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
2.4	The ability to administer the firewall system is restricted to user accounts accessible by authorized personnel.	Inquired of the Security Manager regarding firewall administrator access to determine that the ability to administer the firewall system was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Inspected the firewall administrator user listing to determine that the ability to administer the firewall system was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
2.5	Data transmissions are secured using secure sockets layer (SSL), hyper-text protocol (HTTPS), Identity-Aware Proxy (IAP), and Advanced Encryption Standards (AES) encryption are utilized over public network data transmissions.	Inspected the data transmission encryption configurations to determine data transmissions were secured using SSL, HTTPS, IAP, and AES encryption were utilized over public network data transmissions.	No exceptions noted.
2.6	IAP users are authenticated via multi-factor authentication by Okta prior to being granted remote access to the system.	Inspected the Okta policy settings to determine that IAP users were authenticated via multi-factor authentication by Okta prior to being granted remote access to the system.	No exceptions noted.

CONTROL AREA 2 **DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that data transmissions between the service organization and its clients are complete, accurate, and secure and that data received is posted to the relevant systems in accordance with the Company's guidelines.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.7	A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test results to determine that a third-party performed a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
2.8	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, IDS configurations and firewall rule sets for the production environment to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
2.9	Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console and antivirus configurations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
2.10	The antivirus software provider pushes updates to the installed antivirus software as new updates are available.	Inspected the centralized antivirus configurations to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates were available.	No exceptions noted.
2.11	The antivirus software is configured to scan workstations in real time.	Inspected the centralized antivirus configurations to determine that the antivirus software was configured to scan workstations in real time.	No exceptions noted.

CONTROL AREA 3 **CHANGE CONTROL**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that new development of and changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transaction processing.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.1	Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the infrastructure change management and code change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
3.2	System change requests are documented and tracked in a ticketing system.	Inspected the pull requests and supporting change ticket for a sample of application and infrastructure changes to determine that system change requests were documented and tracked in a supporting ticketing system.	No exceptions noted.
3.3	Commercial version control software is utilized to centrally maintain source code versions and promote application source code through the development process.	Inspected the change control software to determine that commercial version control software was utilized to centrally maintain source code versions and promoted application source code through the development process.	No exceptions noted.
3.4	System changes are tested prior to implementation. Types of testing performed depend on the nature of the change.	Inspected the pull requests and supporting change ticket for a sample of application and infrastructure changes to determine that system changes were tested prior to implementation and types of testing performed depended on the nature of the change.	No exceptions noted.
3.5	Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed.	Inspected the code repository branches to determine that prior code was held in the source code repository for rollback capability in the event that a system change did not function as designed.	No exceptions noted.
3.6	Development and test environments are physically and logically separated from the production environment.	Inspected the separate development, QA, and production environments to determine that development and test environments were physically and logically separated from the production environment.	No exceptions noted.

CONTROL AREA 3 **CHANGE CONTROL**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that new development of and changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transaction processing.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.7	Access to implement changes in the production environment is restricted to authorized IT personnel.	Inquired of the Security Manager regarding users with access to deploy changes into the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.
		Inspected the list of users with access to deploy changes into the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.

CONTROL AREA 4 **COMPUTER OPERATIONS - AVAILABILITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that system processing is authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete accurate and timely manner.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.1	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
4.2	A ticket tracking application is utilized to track and respond to incidents, resolve events, and open change tickets were necessary.	Inquired of the Security Manager regarding security incidents to determine that a supporting ticket tracking application was utilized to track and respond to incidents, resolve events, and open change supporting tickets were necessary.	No exceptions noted.
		Inspected the incident response policies and procedures to determine that a supporting ticket tracking application was required to be utilized to track and respond to incidents, resolve events, and open change supporting tickets were necessary.	No exceptions noted.
		Inspected the supporting incident supporting ticket for a sample of incidents to determine that a ticket tracking application was utilized to track and respond to incidents, resolve events, and open change supporting tickets were necessary.	Testing of the control activity disclosed that there were no security incidents during the review period.
4.3	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, IDS configurations and firewall rule sets for the production environment to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.

CONTROL AREA 4 **COMPUTER OPERATIONS - AVAILABILITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that system processing is authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete accurate and timely manner.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.4	Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup and recovery policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
4.5	An automated backup system is utilized to perform scheduled backups.	Inspected the backup system configurations to determine that an automated backup system was utilized to perform scheduled backups.	No exceptions noted.
4.6	The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, monitoring notification settings, and an example monitoring alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
4.7	Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
4.8	Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
4.9	A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test results to determine that a third-party performed a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
4.10	Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console and antivirus configurations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.

CONTROL AREA 4 **COMPUTER OPERATIONS - AVAILABILITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that system processing is authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete accurate and timely manner.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.11	The antivirus software provider pushes updates to the installed antivirus software as new updates are available.	Inspected the centralized antivirus configurations to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates were available.	No exceptions noted.
4.12	The antivirus software is configured to scan workstations in real time.	Inspected the centralized antivirus configurations to determine that the antivirus software was configured to scan workstations in real time.	No exceptions noted.

CONTROL AREA 5 **COMPUTER OPERATIONS - BACKUP**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that timely system backups of critical files to an off-site location are performed and available for restoration in the event of unexpected processing interruptions, with respect to user entities' internal control over financial reporting.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.1	Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup and recovery policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
5.2	An automated backup system is utilized to perform scheduled backups.	Inspected the backup system configurations to determine that an automated backup system was utilized to perform scheduled backups.	No exceptions noted.
5.3	Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
5.4	Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
5.5	IAP, HTTPS over TLS are used for defined points of connectivity.	Inspected the encryption configurations and digital certificates to determine that IAP, HTTPS over TLS were used for defined points of connectivity.	No exceptions noted.
5.6	Backups are replicated to a different availability zone.	Inspected the backup replication configurations to determine that backups were replicated to a different availability zone.	No exceptions noted.
5.7	Backup restoration tests are performed on an annual basis, as part of the disaster recovery test.	Inspected the completed disaster recovery test results inclusive of backup restoration testing, to determine that data backup restoration tests were performed on an annual basis, as part of the disaster recovery test.	No exceptions noted.

CONTROL AREA 6 **ACCOUNT SETUP**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that Mantl books the account and subservices on behalf of the customer and passes all necessary customer information into the core banking application.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.1	Mantl gets a valid response that is actionable from the KYC/AML decision engine to verify customer identity and reduce fraud risk.	Inspected an evaluation status of a valid response from the KYC/AML decision engine to determine that Mantl got a valid response that was actionable from the KYC/AML decision engine to verify customer identity and reduce fraud risk.	No exceptions noted.
6.2	Mantl facilitates new account funding via ACH, or debit card/credit card processing to initiate a new account funding transaction.	Inspected that the funding transaction alert to determine that Mantl facilitated new account funding via ACH, or debit card/credit card processing to initiate a new account funding transaction.	No exceptions noted.
6.3	Mantl successfully books the account and its related sub-products and sub-services in the core banking system.	Inspected the alert from the core banking system to determine that Mantl successfully booked the account and its related sub-products and sub-services in the core banking system.	No exceptions noted.
6.4	Edit checks are in place to prevent incomplete or incorrect data from being entered into the system.	Inspected the edit check configurations to determine that edits checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
6.5	Data flow diagrams are maintained by management to identify the relevant internal and external information sources of the system.	Inspected the data flow diagrams to determine that data flow diagrams were maintained by management to identify the relevant internal and external information sources of the system.	No exceptions noted.
6.6	Data that entered into the system, processed by the system, and output from the system is protected from unauthorized access.	Inquired of the Security Manager regarding application administrator access to determine data that entered into the system, processed by the system, and output from the system was protected from unauthorized access.	No exceptions noted.
		Inspected the application administrator user listing and access rights to determine that data that entered into the system, processed by the system, and output from the system was protected from unauthorized access.	No exceptions noted.

CONTROL AREA 6 **ACCOUNT SETUP**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that Mantl books the account and subservices on behalf of the customer and passes all necessary customer information into the core banking application.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the application password settings to determine that data that entered into the system, processed by the system, and output from the system was protected from unauthorized access.	No exceptions noted.
		Inspected the application account lockout threshold to determine that data that entered into the system, processed by the system, and output from the system was protected from unauthorized access.	No exceptions noted.
		Inspected the intrusion detection system (IDS) and encryption configurations to determine that data that was entered into the system, processed by the system, and output from the system was protected from unauthorized access.	No exceptions noted.