BankTEL Systems, LLC (an AvidXchange Company)

Type II System and Organization Controls Report (SOC 1)

Independent Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of the Controls for the Period of January 1, 2020, through September 30, 2020.

Using SSAE No. 18 Section AT-C320, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting.

KirkpatrickPrice
4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

SECTION I:
INDEPENDENT SERVICE AUDITOR'S REPORT

on BankTEL Systems, LLC's Description of Its Financial Software Service System and the Suitability of the Design and Operating Effectiveness of the Controls

Boyce Adams Jr.
SVP of Financial Services
BankTEL Systems, LLC (an AvidXchange Company)
319 Park Creek Drive
Columbus, MS 39705-8370

Scope

We have examined BankTEL Systems, LLC's description of its financial software service system, documented in Section III, for developing user entities' financial accounting and cash management software throughout the period of January 1, 2020, to September 30, 2020. The examination evaluated the suitability of the design and operating effectiveness of the included controls to achieve the related control objectives stated in the description, based on the criteria identified in Section II. The controls and control objectives included in the description are those that management of BankTEL Systems, LLC believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the financial software service system that are not likely to be relevant to user entities' internal control over financial reporting.

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

BankTEL Systems, LLC uses Rackspace and Jack Henry & Associates to store customer data, and CyberlinkASP is used for BankTEL's internal network. The description includes only the control objectives and related controls of BankTEL Systems, LLC and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by BankTEL Systems, LLC can be achieved only if complementary subservice organization controls assumed in the design of BankTEL Systems, LLC's controls are suitably designed and operating effectively, along with the related controls at BankTEL Systems, LLC. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

In Section II, "BankTEL Systems, LLC's Assertion," BankTEL Systems, LLC has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. BankTEL Systems, LLC is responsible for preparing the description and its assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, specifying the control objects 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 American Institute of Certified Public Accountants. 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 of January 1, 2020, to September 30, 2020. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design of the controls to achieve the related control objectives stated in the description, based on the criteria in the management's assertion.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed 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.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in financial accounting and cash management software. Also, the projection to the future of any suitability of the design of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Opinion

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

a. the description fairly presents the financial software service system that was designed and implemented throughout the period of January 1, 2020, to September 30, 2020.

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period January 1, 2020, to September 30, 2020, and subservice organizations and user entities applied the complementary controls assumed in the design of BankTEL Systems, LLC's controls throughout the period of January 1, 2020, to September 30, 2020.

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period of January 1, 2020, to September 30, 2020, if complementary subservice organization and user entity controls assumed in the design of BankTEL Systems, LLC's controls operated effectively throughout the period of January 1, 2020, to September 30, 2020.

Restricted Use

This report is intended solely for the information and use of management of BankTEL Systems, LLC, user entities of BankTEL Systems, LLC's financial software service system throughout the period of January 1, 2020, to September 30, 2020, 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 misstatements of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than the specified parties.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

November 4, 2020

SECTION II:
BANKTEL SYSTEMS, LLC'S ASSERTION

BANKTEL SYSTEMS, LLC'S ASSERTION

We have prepared the description of BankTEL Systems, LLC's financial software service system entitled "BankTEL Systems, LLC's Description of Its Financial Software Service System," for developing user entities' financial accounting and cash management software throughout the period January 1, 2020, to September 30, 2020, for user entities of the system during some or all of the period January 1, 2020, to September 30, 2020, and their auditors who audit and report on such user entities' financial statements or internal controls over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities themselves, when obtaining an understanding of user entities' information and communication systems relevant to financial reporting.

BankTEL Systems, LLC uses Rackspace and Jack Henry & Associates to store customer data, and CyberlinkASP is used for BankTEL's internal network. The description includes only the control objectives and related controls of BankTEL Systems, LLC and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice 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 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 BankTEL Systems, LLC's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

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

a. the description fairly presents the financial software service system made available to user entities of the system during some or all of the period January 1, 2020, to September 30, 2020, for financial accounting and cash management software 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, if applicable

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

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

3) 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.

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

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

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

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

8) other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

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 service organization's 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 financial software service 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 operating effectively throughout the period January 1, 2020, to September 30, 2020, to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of BankTEL Systems, LLC's controls throughout the period of January 1, 2020, to September 30, 2020. 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 management of the service organization.

ii. 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.

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

SECTION III:
BANKTEL SYSTEMS, LLC'S DESCRIPTION OF ITS SYSTEM

OVERVIEW OF SERVICES PROVIDED

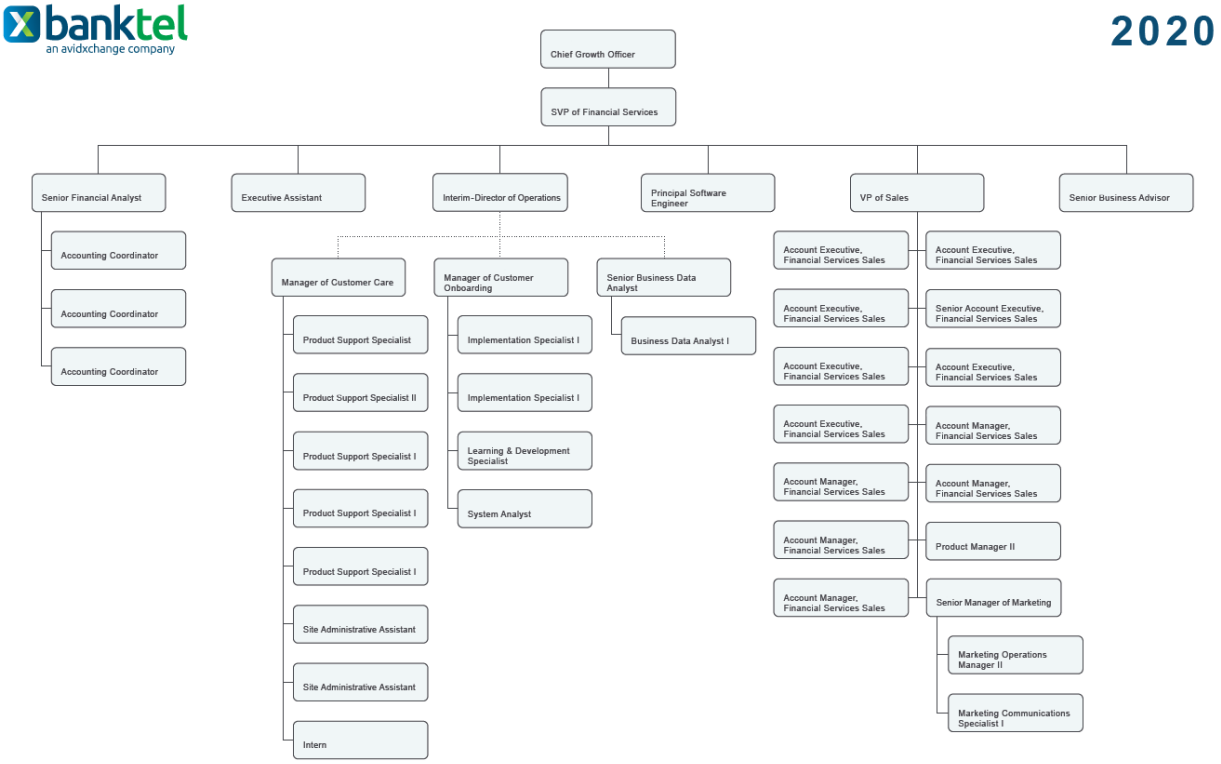
BankTEL Systems (BankTEL), a division of BTS Alliance, LLC and an AvidXchange company, develops and markets specific financial software systems for use in financial institutions. BankTEL maintains its headquarters in Columbus, Mississippi. The products known as BankTEL Systems consist of over a dozen different products and services. BankTEL currently serves over 1,700 financial institutions in all 50 states in the United States and in several countries. These systems are designed to assist clients in improving operational efficiency and increasing compliance, and the BankTEL Systems product offerings include the following:

- Accounts Payable
- Invoice Approval Workflow
- Remote Scanning
- Expense Reports
- Management Reports
- Pre-Paid & Accruals
- Fixed Asset Management
- Vendor Management
- Purchase Order Systems
- Vendor Portal
- Shareholder Management

Organization

BankTEL maintains a traditional hierarchy with functional departments and clear reporting lines, and a formal organizational chart (below) is maintained illustrating this hierarchy and established departments. The organizational chart is reviewed, updated, and approved annually. BankTEL's functional departments include the following:

- Accounting & Finance
- Customer Care
- Customer Onboarding
- Data
- Software Engineering
- Sales & Marketing



Management Control

Management uses several methods to communicate organizational tone and direction to personnel, including trainings, meetings, and policy documentation. Management conducts weekly, quarterly, and annual meetings to communicate organizational tone, direction, standards, and objectives to all personnel. BankTEL reviews, updates, and approves all organizational policies annually and as needed, and the Leadership Team is responsible for this review process. The organization's formal policies, processes, and procedures include the following:

- Acceptable Use Policy
- AvidXer Handbook
- Baseline Server Hardening
- Change Management Policy & Process
- Client Data Policies and Procedures
- Compliance with Regulatory Measures
- Daily Operational Security Procedures
- Data Classification Policy
- Data Workflow
- Disaster Recovery and Business Continuity Plan
- Employee Background Check Policy
- Encryption Policy
- Event Response Policy & Process
- Identity and Access Management Standard
- Incident Response Policy
- Information Security Policy
- Offboarding People Leader Guide
- Network Access and Authentication Policy
- Password Policy
- Patch Management Policy
- Physical Security Policy
- Policy Review Policy
- Risk Assessment
- Risk Assessment Data Systems
- Security Awareness Training Policy
- Software Development Process
- Technology Equipment Disposal Policy
- Vendor Management Policy
- Vulnerability Management Standard

Integrity and Ethics

BankTEL maintains a formal Code of Conduct outlining its integrity and ethics values, and personnel are required to review and acknowledge this Code of Conduct upon hire and annually thereafter. The Code of Conduct describes the company's expectations of how employees, customers, suppliers, and other stakeholders conduct business practices and address ethical and legal principles and set standards of professionalism and integrity for all employees and operations worldwide.

Management conducts quarterly all-hands meetings to communicate its Code of Conduct and organizational standards and objectives.

Controls Related to Personnel

BankTEL uses a formal employee handbook (AvidXer Handbook) to communicate its mission, tone, direction, standards, and requirements to all personnel, and controls related to personnel are implemented via this handbook. The handbook is available for personnel review at all times, and this handbook and other onboarding documents are required to be acknowledged by personnel upon hire. The handbook also includes the following statements, codes, and information:

- Code of Conduct
- Statement on Ethics
- Information confidentiality
- Background and reference checks
- Progressive discipline

Job Descriptions

BankTEL maintains formal job descriptions for its critical job functions that document roles, responsibilities, and required qualifications for each position. Functions that the organization considers critical include the following:

- Manager of Customer Onboarding
- Director of Operations
- Manager of Customer Care

Hiring, Termination, and Personnel Changes

BankTEL maintains formal onboarding and offboarding checklists to guide its onboarding and offboarding processes, including the assignment and revocation of access. An Offboarding People Leader Guide is established and used to guide management regarding the offboarding of terminated or separating employees.

The organization maintains and collects all required documentation necessary for the secure onboarding of its new hires, including the following required documentation used in its onboarding processes:

- Avid Security
- Talent Release
- Facilities and Sports Waiver
- Confidentiality Agreement
- AvidXer Handbook
- Health Insurance Marketplace Coverage Options
- Code of Business Conduct
- Information Security Policy
- Travel Expense and Mobile Policies
- BSA AML Compliance Program
- OFAC Compliance Policy

BankTEL maintains a formal Background Check Policy used to guide its background check process, requiring all new hires to clear various checks, including identity, employment, and education verifications, criminal history checks, and drug screenings.

Training

Employees are required to complete onboarding and continued upon hire and annually thereafter. The organization requires personnel to complete trainings regarding the following topics:

- Sexual harassment
- Anti-money laundering
- PCI DSS
- Privacy
- Cybersecurity
- Workplace violence
- Security awareness

Regulatory Requirements

BankTEL complies with the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA), and formal documentation is maintained regarding these regulations that personnel are required to review and acknowledge. The organization maintains a confidential data policy that communicates its confidentiality and privacy requirements and commitments used to adhere to its applicable regulatory requirements.

RISK ASSESSMENT

BankTEL risk assessments are based upon industry-accepted best practices and standards and are performed annually and as needed. The organization's risk assessment identifies and assesses changes that could significantly impact the system of internal control, identifies risk mitigation activities for risks arising from potential business disruptions, and addresses risks associated with vendors and business partners. The Information Security Policy addresses the steps taken to analyze the environment and determine whether there are any internal threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems. The likelihood and potential damage of these threats is assessed, taking into consideration the sensitivity of customer information.

MONITORING

BankTEL maintains several teams to monitor the business operations of the organization, including the Board of Directors and the Leadership Team. The Board of Directors provides organizational tone, direction, and objectives, and the Leadership Team is responsible for monitoring business operations. This team meets weekly to review and discuss operations, and this review includes the review and analysis of all collected reports and alerts generated by BankTEL's daily operational security and monitoring procedures.

Description of Computerized Information Systems

BankTEL maintains a network diagram (below) that illustrates the company infrastructure. BankTEL also obtains network diagrams from its third-party providers—CyberlinkASP, Jack Henry & Associates (JHA), and Rackspace—that illustrate their architecture and how their functions are supported.

BankTEL stores, transmits, and processes client data relevant to its business operations and services provided and delivered. A formal data flow diagram (below) is maintained, illustrating the flow of data throughout its systems and environments.

The organization uses an automated tool to compile a system inventory of all physical and virtual systems and assets, and an accurate software inventory documenting all critical software in use and relevant licensing is maintained manually. The organization's critical software in use includes the following:

- ASNA
- Bomgar
- CyberlinkASP
- DevExpress Document Server 17.1
- DevExpress DXperience Components 17.1
- Dynamic Web TWAIN
- ESET
- Malwarebytes
- Red-Gate SQL Dev Bundle
- Salesforce
- ScheduleOnce
- Telax Call Center
- Unifi

BankTEL maintains publicly available marketing materials accurately describing the scope of its services.

General IT Controls

Information Security Program

BankTEL's formal Information Security Policy communicates information security responsibilities for all organizational personnel, including executive management. This Information Security Policy is reviewed and updated annually, and personnel are required to review and acknowledge this policy annually or upon significant change.

The organization maintains formal complementary user-entity controls to guide end users on the best use practices of the organization's services, and BankTEL informs third-party users of its services with training regarding the best-use practices of the organization's services

delivered. All clients and customers of the organization are required to complete the Ascend Agreement.

Incident Response

BankTEL maintains a formal incident response policy and incident response procedures to detect, assess, and remediate incidents, and the organization tests its incident response procedures regularly.

BankTEL provides its users and clients contact information by which to report potential security breaches or complaints to be handled by responsible organizational personnel.

Environmental Security

BankTEL's facilities are equipped with various environmental controls to protect its facilities and assets from potential business disruptions or environmental hazards, and these controls include the following:

- A climate control system
- Thermostat sensors
- Smoke detectors
- Uninterruptible power supplies (UPSs)
- Backup generators

The effectiveness of the organization's backup generator is tested weekly.

Physical Security

BankTEL maintains a formal physical security policy outlining its requirements and standards for the physical security of its facilities, and this policy is reviewed, updated, and approved annually. The organization's sensitive areas are protected by various physical security controls, including the use of door locks and badge access systems, physical intrusion detection systems, and video security surveillance.

Access to the organization's facilities is restricted and monitored using a badge access card system that automatically generates access logs. BankTEL's facilities are equipped with an alarm system, including motion sensors, that generates alerts sent to the organization upon the detection of unauthorized access. The organization's facilities are monitored using a security surveillance system, with cameras monitoring all ingress and egress points and sensitive areas, and BankTEL retains footage generated by its surveillance systems for a minimum of three months to allow proper review of footage. Daily operational security procedures that include the monitoring of the physical security of BankTEL's facilities are performed to ensure security.

BankTEL maintains a formal technology equipment disposal policy that outlines the organization's standards and requirements regarding the secure destruction of unneeded media. A third-party vendor is employed to securely destroy its decommissioned media, and certificates verifying the secure destruction of media are collected and retained to ensure information security.

The organization maintains formal visitor procedures, including the required use of a visitor log, the assignment of a visitor badge, and the requirement to escort all visitors while on the premises. The visitor log documents all relevant details regarding the visitor, and these logs are retained for at least one year for future review. The details documented in these visitor logs include the following:

- Visitor name
- Date and time
- Non-disclosure agreement (NDA)
- Confidentiality statement
- Agreement to NDA

Logical Access

BankTEL maintains formal identity and access management standards to govern its logical access procedures and assignment of access, and the organization assigns all personnel logical access using the principle of least privilege. Several logical access systems are used to restrict access to its organizational assets and information, and all access is assigned using the principle of least privilege.

Formal personnel account creation processes are maintained and used to request, approve, and implement new-hire access, and the organization requires all access change requests to be documented, tracked, and approved prior to implementation. BankTEL requires all personnel to be assigned a unique user ID before granting access to organizational assets and information. The organization immediately revokes personnel logical access privileges upon personnel termination or separation.

A formal customer and client onboarding process is maintained and implemented, and clients manage their own logical access once the client onboarding process is complete.

BankTEL also maintains formal password parameters and lockout configurations that are used to ensure the security of its organizational assets. The organization requires its passwords to be encrypted at rest and in transit, and BankTEL encrypts its emails in transit.

The organization requires the use of multi-factor authentication (MFA) when accessing its networks and systems remotely.

Network Monitoring

BankTEL's monitoring and logging activities are managed by an employed third party, and all detected incidents and anomalies are communicated to the organization for analysis and remediation. The organization reviews alerts generated by its outsourced monitoring activities daily to ensure the security of its systems and networks. BankTEL also employs a third-party subservice organization to monitor its wireless access points, file integrity, and intrusion detection and prevention systems (IDSs/IPSs).

A third party is employed to implement organizational firewalls and edge security systems and controls, ensuring the managed monitoring and security of the organization's systems, networks, and assets.

BankTEL's network monitoring controls are monitored by its subservice organizations and third-party vendors, and controls related to network monitoring have been omitted from this report using the carve-out method. Interested parties should collect and review the relevant, independent third-party assessments of these subservice organizations and vendors.

Configuration Management

BankTEL's formal Identity and Access Management Standard documents and implements the organization's configuration standards for all systems, networks, and standards. Group policies are used to enforce the organization's formal configuration standards, and BankTEL reviews, updates, and approves its formal configuration standards annually.

The organization's Security Operations Team reviews and analyzes security publications to determine potential impacts to the organization, and Security Team members periodically evaluate automated reports from the vulnerability management software to continuously improve detection and remediation capabilities. The Security Team also reviews industry best-practice configuration standards continuously to determine any necessary changes to its configuration standards. BankTEL's configuration standards are based upon industry-accepted best practices (SANS), and training regarding these best practice standards are required to be completed by personnel biannually.

Change Management

BankTEL maintains a formal change management policy used to govern its change management processes, which includes the following steps:

- Submission of a formal change request
- The categorization and prioritization of changes
- The analysis and justification of the change
- The approval of the change
- Change planning and implementation
- The performance of a post-implementation review

The organization's change request tickets are submitted for review and approval, and these change request tickets document all relevant information regarding the requested change. BankTEL requires all changes requests to include identified roles and responsibilities and a risk analysis of the change; all changes are required to be tested prior to implementation, and recovery plans must be documented. BankTEL requires all requested changes to be reviewed and approved by the Security Board prior to implementation.

Vulnerability Management

BankTEL uses an antivirus solution to monitor and protect its organizational assets and systems from malicious software and unauthorized access. The organization maintains antivirus configuration settings that include the performance of continual updates and the automatic generation of alerts and logs documenting identified security incidents. BankTEL antivirus solutions perform incremental scans daily and full scans of all systems weekly, and logs generated by its antivirus solution are retained for 30 days to allow appropriate review and recovery activities.

BankTEL maintains a formal patch management policy governing the organization's implementation of necessary patches within two weeks of initial release.

The organization employs an independent third party to conduct annual web application penetration tests.

Data Security

BankTEL's formal Client Data Policies and Procedures govern the organization's use, handling, and retention of client data in compliance with its regulatory requirements. Client data is retained for one year, and personnel human resources information is retained indefinitely, in compliance with the organization's regulatory requirements.

The organization maintains a data classification policy used to ensure that the organization's data is categorized, handled, and retained in accordance with the organization's regulatory requirements. BankTEL's formal data classifications include the following:

- Public
- Organizational
- Confidential
- Critical

BankTEL maintains a formal encryption policy to govern the organization's use and management of encryption keys and encryption algorithms. The organization requires the use of Secure Sockets Layer (SSL) encryption certificates to protect its data at rest in transmission within its web applications.

Business Continuity and Disaster Recovery

BankTEL's maintains a formal disaster recovery and business continuity plan to restore business operations in the events of a disruption to business operations or a potential disaster or environmental hazard, and this plan is reviewed, updated, and approved annually.

The organization's Disaster Recovery and Business Continuity Plan includes a list of critical components and software and defined notification and team responsibilities for the Recovery Response Team. The Recovery Response Team is responsible for implementing the organization's business continuity and recovery procedures.

The organization tests its Disaster Recovery and Business Continuity Plan at least annually, and the results of these tests are analyzed by management to determine and necessary changes or adjustments to the plan.

Vendor Management

BankTEL maintains a formal vendor management policy and vendor qualification and screening process to perform due diligence on all potential vendors. The organization's due-diligence process includes the performance of vendor reference checks and financial status checks, and the organization monitors its vendors' service delivery and compliance statuses by collecting and reviewing annual independent third-party audits of vendor controls.

Application Development

BankTEL maintains a formal software development process to guide its software development processes. The organization requires all of its pushes to production to be approved by senior management prior to implementation, and all of its pushes to production quarterly. BankTEL notifies its clients and customers of upcoming pushes to production or changes to existing applications or software.

The organization's application and software development, production, and testing environments are logically and physically separated from each other to ensure authorized access and the segregation of duties. Access to the organization's source code repository is restricted using a team foundation server (TFS), and version control is implemented using a TFS.

BankTEL requires all of its Software Developers to pursue and maintain additional continuing professional education credits every five years.

The organization employs an independent third-party to conduct annual application penetration tests.

Application Change Management

Application development-related changes must adhere to the organization's formal Change Management Policy, including the submission of change requests via the organization's ticketing system.

Application, software, or code change requests must be reviewed and approved by the Principal Software Engineer and the Senior Vice President. Technical specifications are developed for significant application, software, and code changes. Testing strategies are developed and implemented for all application development-related changes, and these strategies are developed and implemented by the Senior Vice President and Product Support Specialists. Back-out procedures are documented for all application development-related changes. Changes to source code, programs, applications, or software are tested in a separate, controlled environment prior to implementation.

SUBSERVICE ORGANIZATIONS

BankTEL uses industry-recognized subservice organizations to achieve operating efficiency and to obtain specific expertise. BankTEL performs ongoing monitoring to ensure that potential issues are identified promptly to maintain the effectiveness of internal control. The following evaluations are conducted:

- Reviewing and reconciling output reports
- Holding periodic discussions with the subservice organization
- Making regular site visits
- Testing controls at the subservice organization
- Reviewing independent audit reports
- Monitoring external communications

The following are the principal subservice organizations used by BankTEL:

- Rackspace – houses all servers related to Ascend
- Jack Henry & Associates – houses servers related to Ascend at this location
- CyberlinkASP – houses all servers used for internal and daily work

USER CONTROL CONSIDERATIONS

BankTEL's services are designed with the assumption that certain controls will be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report. BankTEL's management makes control recommendations to user organizations and provides the means to implement these controls in many instances. BankTEL also provides best practice guidance to clients regarding control elements outside the sphere of BankTEL responsibility.

This section describes additional controls that should be in operation at user organizations to complement the BankTEL controls. User control recommendations include:

- User organizations should implement sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with BankTEL.

- User organizations should ensure timely removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with BankTEL's services.

- Transactions for user organizations relating to BankTEL's services should be appropriately authorized, secure, timely, and complete.

- For user organizations sending data to BankTEL, data should be protected by appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation.

- User organizations should implement controls requiring additional approval procedures for critical transactions relating to BankTEL's services.

- User organizations should report to BankTEL in a timely manner any material changes to their overall control environment that may adversely affect services being performed by BankTEL.

- User organizations are responsible for notifying BankTEL in a timely manner of any changes to personnel directly involved with services performed by BankTEL. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by BankTEL.

- User organizations are responsible for adhering to the terms and conditions stated within their contracts with BankTEL.

- User organizations are responsible for developing, and if necessary, implementing a business continuity and disaster recovery plan (BCDRP) that will aid in the continuation of services provided by BankTEL.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Therefore, each client's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

SECTION IV:
CONTROL OBJECTIVES AND RELATED CONTROLS

TEST METHODOLOGY

Section IV outlines the controls in place by BankTEL Systems, LLC, an AvidXchange Company, (BankTEL) and describes the tests of their effectiveness performed by the independent service auditor. The following methodologies were used in testing the suitability of the design and operating effectiveness of BankTEL's controls:

Test Methodology	Description
Interview	The auditor inquired of relevant personnel to corroborate control placement or activity.
Review	The auditor obtained and read relevant BankTEL documentation.
Observation	The auditor directly witnessed control placement or activity or evidence thereof.

The tables on the following pages outline the control objectives, controls in place, and independent testing relevant to the independent assessment of BankTEL's control environment throughout the period January 1, 2020, to September 30, 2020.

Control Objective 1 – Organization and Administration			
Control Objective 1: Controls provide reasonable assurance that management provides oversight, segregates duties, and guides consistent implementation of security practices.			
Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
1.1	The organization maintains a board of directors used to provide tone, direction, and objectives.	Interviewed the Sr. Financial Analyst regarding the Board of Directors and verified that a board of directors consisting of AvidXchange personnel is maintained Observed the AvidXchange website and verified that the organization's board members align as described	No Relevant Exceptions Noted
1.2	The organization maintains a leadership team that is responsible for monitoring business operations, and this team meets weekly to review and discuss operations.	Interviewed the Sr. Financial Analyst regarding management monitoring activities and verified that the Leadership Team meets weekly to discuss operations and to review policies as needed and that all departments heads monitor their department and report to upper management Observed calendar invites and meeting notes and verified that weekly leadership meetings are held to discuss department status	No Relevant Exceptions Noted
1.3	The organization's networks are maintained by a third party, and various network diagrams are maintained illustrating the architecture of the organization's network.	Reviewed the JHA Network Diagram, the Rackspace Network Diagram, and the BankTEL diagram (dated June 30, 2020) and verified that various network diagrams are maintained illustrating the organization's networks Observed a walkthrough of the facility and verified that no sensitive systems exist in the facility, that the network is only used for internet access, and that all sensitive systems are kept and managed by a third party	No Relevant Exceptions Noted
1.4	The organization stores, transmits, and processes client data relevant to its business operations and services provided and delivered.	Interviewed the Sr. Financial Analyst regarding the types of data stored, transmitted, or processed in the organization and verified that client financial data is stored, transmitted, and processed by the organization, and this includes accounts payable and general ledger data	No Relevant Exceptions Noted

		Observed a demo of the application and verified that it is aligned with the results of the interview	
1.5	The organization maintains a data flow diagram illustrating the flow of data throughout its systems and environments.	Reviewed the BankTEL Data Workflow diagram (dated July 1, 2020) and verified that the organization documents the flow of sensitive data through the organization	No Relevant Exceptions Noted
1.6	The organization uses an automated tool to compile a system inventory of all organizational physical and virtual systems and assets.	Interviewed the Sr. Financial Analyst regarding the inventory management of the organization and verified that the organization uses ServiceNow for inventory management and that this is an automated process that reads configurations and software that has been installed and reports any fluctuations from the standard Observed ServiceNow and verified that an automated tool is used to maintain the inventory of the organization	No Relevant Exceptions Noted
1.7	The organization manually maintains an accurate software inventory documenting all critical software in use and relevant licensing.	Reviewed the 2020 Software Inventory and verified that software and licensing is managed manually Observed a walkthrough of systems and verified that the software represented in the interview accurately describes the software and licensing of the organization	No Relevant Exceptions Noted
1.8	The organization employs an independent third-party to conduct annual web application penetration tests.	Interviewed the Sr. Financial Analyst regarding the scanning performed during the last 12 months and verified that the organization has performed an annual web application penetration test Observed a BankTEL draft report and verified that a web application penetration test was performed that did not detect any critical or high vulnerabilities	No Relevant Exceptions Noted
1.9	The organization maintains publicly available marketing materials accurately describing the scope of its services.	Observed marketing materials and verified that they align with the website and contract	No Relevant Exceptions Noted
1.10	The organization maintains a traditional hierarchy with functional departments and clear reporting lines.	Interviewed the Sr. Financial Analyst regarding the organizational structure of the company and verified that AvidXchange oversees the organization and that BankTEL is separated into multiple departments, including the following:	No Relevant Exceptions Noted

		• Accounting & Finance • Customer Care • Customer Onboarding • Data • Software Engineering • Sales & Marketing Observed a walkthrough of the organization and verified that the organizational structure aligns with the results of the interview	
1.11	The organization maintains a formal organizational chart illustrating its traditional hierarchy, clear reporting lines, and functional departments.	Observed BankTEL Org Chart 2020 Interim and verified the following: • The organizational chart is aligned with the results of the interview • The organizational chart is up to date • The Director of Operations, who is the Information Security Officer, reports directly to the Senior Vice President • The organization operates under a traditional hierarchy	No Relevant Exceptions Noted
1.12	The organization maintains a formal Code of Conduct outlining its integrity and ethics values, and personnel are required to review and acknowledge this Code of Conduct upon hire and annually thereafter.	Reviewed the AvidXchange Code of Business Conduct and verified that all employees are required to acknowledge this policy annually Interviewed the Sr. Financial Analyst regarding how management communicates and oversees the Code of Conduct and verified that the Employee Handbook and the Code of Conduct are reviewed and acknowledged by all employees annually	No Relevant Exceptions Noted
1.13	The organization maintains a formal employee handbook that is available for personnel at all times via the organization's intranet.	Reviewed the AvidXchange Handbook and verified that all employees are required to acknowledge this annually Observed OneHub and verified that all employee policies are made available to all employees through this central intranet	No Relevant Exceptions Noted
1.14	Management conducts quarterly all-hands meetings used to communicate its Code of Conduct and organizational standards and objectives.	Observed a slide deck from a quarterly all-hands meeting and verified that the Code of Conduct is communicated during these meetings	No Relevant Exceptions Noted
1.15	Management uses several methods to communicate organizational tone and direction to personnel, including trainings, meetings, and policy documentation.	Observed examples of the following demonstrating methods management uses to set the tone and direction for the company: • Onboarding and continued training • Dissemination of policy documentation	No Relevant Exceptions Noted

		• Weekly, quarterly, and annual meetings • Security awareness training • Employee handbook acknowledgements	
1.16	Employees are required to complete onboarding and continued training that includes security awareness requirements upon hire and annually thereafter.	Observed examples of the following demonstrating methods management uses to set the tone and direction for the company: • Onboarding and continued training • Dissemination of policy documentation • Weekly, quarterly, and annual meetings • Security awareness training • Employee handbook acknowledgements	No Relevant Exceptions Noted
1.17	Management conducts weekly, quarterly, and annual meetings used to communicate organizational tone, direction, standards, and objectives to all personnel.	Observed examples of the following demonstrating methods management uses to set the tone and direction for the company: • Onboarding and continued training • Dissemination of policy documentation • Weekly, quarterly, and annual meetings • Security awareness training • Employee handbook acknowledgements	No Relevant Exceptions Noted
1.18	The organization requires all personnel to review and acknowledge its formal employee handbook.	Observed examples of the following demonstrating methods management uses to set the tone and direction for the company: • Onboarding and continued training • Dissemination of policy documentation • Weekly, quarterly, and annual meetings • Security awareness training • Employee handbook acknowledgements	No Relevant Exceptions Noted
1.19	The organization reviews, updates, and approves all organizational policies annually and as needed, and the Leadership Team is responsible for this review process.	Reviewed the BankTEL Policy Review Policy (dated July 29, 2020) and verified that management meets weekly and reviews policies as needed and that the organization reviews all corporate policies annually Interviewed the Executive Assistant Administrator regarding the annual review and update of corporate policies and verified that the Leadership Team meets weekly to discuss important/relevant topics and reviews policies as needed; the Senior	No Relevant Exceptions Noted

		Vice President (SVP) approves policies that are changed as needed and the organization reviews all corporate policies annually	
1.20	The organization's risk assessments are based upon industry-accepted best practices standards and are performed periodically as needed.	Reviewed the AvidXchange enterprise risk management (ERM) Program Charter and verified that the risk assessment is based on an industry-accepted risk assessment standard and that the risk assessment process is performed periodically	No Relevant Exceptions Noted
1.21	The organization's risk assessment identifies and assesses changes that could significantly impact the system of internal control.	Reviewed the 2020 Risk Assessment Data Systems (dated June 1, 2020) and the 2020 Risk Assessment (dated May 1, 2020) and verified that the risk assessment documents the following information: • How the organization identifies and assesses changes that could significantly impact the system of internal control • The organization's risk mitigation activities for risks arising from potential business disruptions • How the organization addresses risks associated with vendors and business partners	No Relevant Exceptions Noted
1.22	The organization's risk assessment identifies risk mitigation activities for risks arising from potential business disruptions.	Reviewed the 2020 Risk Assessment Data Systems (dated June 1, 2020) and the 2020 Risk Assessment (dated May 1, 2020) and verified that the risk assessment documents the following information: • How the organization identifies and assesses changes that could significantly impact the system of internal control • The organization's risk mitigation activities for risks arising from potential business disruptions • How the organization addresses risks associated with vendors and business partners	No Relevant Exceptions Noted
1.23	The organization's risk assessment addresses risks associated with vendors and business partners.	Reviewed the 2020 Risk Assessment Data Systems (dated June 1, 2020) and the 2020 Risk Assessment (dated May 1, 2020) and verified that the risk assessment documents the following information: • How the organization identifies and assesses changes that could significantly impact the system of internal control	No Relevant Exceptions Noted

		• The organization's risk mitigation activities for risks arising from potential business disruptions • How the organization addresses risks associated with vendors and business partners	

Control Objective 2 – Information Security Program			
Control Objective 2: Controls provide reasonable assurance that information security policies are maintained to set the security tone for the company and create security awareness.			
Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
2.1	The organization maintains a formal Information Security Policy that is reviewed and updated annually, and personnel are required to review and acknowledge this policy annually or upon significant change to the policy.	Reviewed the BankTEL Information Security Policy (dated June 30, 2020) and verified that the purpose of this policy includes the following: • Ensure the security and confidentiality of customers' information • Protect against any anticipated threats or hazards • Protect against unauthorized access to customer information • Ensure proper record keeping of company assets Interviewed the Sr. Financial Analyst regarding the Information Security Policy and verified that the Information Security Policy is reviewed and updated annually to make sure that data is protected; the policy explains the security controls of the organization, and all employees must acknowledge this policy annually as it is updated	No Relevant Exceptions Noted
2.2	The organization's Information Security Policy communicates information security responsibilities for all organizational personnel, including executive management.	Reviewed the BankTEL Information Security Policy (dated June 30, 2020) and verified that all employees are responsible for the security of the organization Interviewed the SVP of Financial Services regarding those responsible for information security responsibilities and verified that the organization limits access to the migration team, the CEO, and the CFO	No Relevant Exceptions Noted
2.3	The organization provides third-party users of its services with training regarding the best use practices of the organization's services delivered.	Interviewed the Sr. Financial Analyst regarding how the organization communicates requirements for the proper use of the system and verified that the organization provides documentation to all end users and that all users are trained as they are onboarded	No Relevant Exceptions Noted

		Observed the Help Section of the application and verified that documentation is available to all users of the system	
2.4	All clients and customers of the organization are required to complete the Ascend Agreement.	Reviewed the Ascend Agreement and verified that the contract is the standard agreement for all customers	No Relevant Exceptions Noted
2.5	The organization maintains formal Complementary User-Entity Controls used to guide end users on the best use practices of the organization's services.	Reviewed the Complementary User-Entity Controls Template and verified that the organization agrees to the provided complementary user entity controls Interviewed the Sr. Financial Analyst regarding the guidance provided to clients regarding best practices when using the organization's products or services and verified that the organization agrees to the provided complementary user entity controls	No Relevant Exceptions Noted
2.6	The organization maintains a formal incident response policy and incident response procedures used to detect, assess, and remediate incidents.	Reviewed the Event Response Policy (dated July 1, 2020), the Event Response Procedure (dated July 1, 2020), and the Incident Response Policy.pdf (dated July 1, 2020) and verified that the organization documents a formal incident response policy Interviewed the Executive Assistant Administrator regarding the incident response policies and procedures of the organization and verified that clients report events to the support staff who notify management and management determines the cause and notify clients (when necessary and if approved by the Senior Vice President)	No Relevant Exceptions Noted
2.7	The organization tests its incident response procedures regularly.	Observed the Incident Response Test (dated April 27, 2020) and verified that the organization tests its incident response procedures and document the results	No Relevant Exceptions Noted
2.8	The organization requires all personnel to complete annual training programs regarding physical security, workplace violence, anti-harassment, cybersecurity, PCI DSS, anti-money laundering, and privacy.	Interviewed the Sr. Financial Analyst regarding the training given to personnel with security breach responsibilities and verified that employees must complete physical security and workplace violence, PCI DSS, and cybersecurity training Observed HR Records and verified that from a random sampling of completed	No Relevant Exceptions Noted

		employee trainings (4 of 34) and verified that the following training was conducted: • Sexual harassment • Anti-money laundering • PCI DSS • Privacy • Cyber security • Workplace violence	
2.9	The organization has provided its users and clients with contact information used to report potential security breaches or complaints to be handled by responsible organizational personnel.	Interviewed the Sr. Financial Analyst regarding the ways in which users and clients can report breaches or submit complaints to the organization and verified that an email address is monitored regularly by management for these incidents and that this email address is given to all users, clients, and contractors Observed OneHub and verified that this email address is communicated to users of the organization for the purpose of submitting incidents or complaints through this shared user/client intranet portal; all clients and users can access this policy through OneHub	No Relevant Exceptions Noted
2.10	The organization employs a third-party subservice organization to monitor its wireless access points, file integrity, and intrusion detection and prevention (IDS/IPS).	Interviewed the Sr. Financial Analyst regarding the Incident Response Plan and the monitoring for intrusion detection, file integrity, and unauthorized wireless access points and verified that all edge security is managed and monitored by CyberlinkASP Observed emails from CyberlinkASP and verified that alerts are sent to the organization if events are detected that may affect them	No Relevant Exceptions Noted
2.11	The organization reviews alerts generated by its outsourced monitoring activities daily to ensure the security of its systems and networks.	Interviewed the Sr. Financial Analyst regarding daily operational security procedures and verified that physical security emails from the alarm monitoring service are reviewed and that monitoring reports from third-party managed security service providers (MSSPs) are reviewed daily for events that may need further attention Observed reports from alarm and security monitoring services and verified that these	No Relevant Exceptions Noted

		reports offer physical and logical security posture of the organization	
2.12	The organization maintains a Confidential Data Policy that communicates its confidentiality and privacy requirements and commitments used to adhere to its applicable regulatory requirements.	Reviewed the Confidential Data Policy (dated June 30, 2020) and verified that privacy and confidentiality are addressed within this policy Interviewed the SVP of Financial Services regarding the privacy policies of the organization and verified that this policy is made available to all employees and customer via OneHub portal Observed the One Hub Portal and verified that employees and clients can access the Privacy Policy via OneHub	No Relevant Exceptions Noted

Control Objective 3 – Human Resources

Control Objective 3: Controls provide reasonable assurance that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. Controls ensure the reduction in risk of theft, fraud, and misuse of facilities.

Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
3.1	The organization maintains a formal handbook used to communicate its mission, tone, direction, standards, and requirements to all personnel.	Reviewed the AvidXer Handbook (dated February 18, 2019) and verified that the following attributes exist in the handbook: • Code of Conduct • Statement on Ethics • Information confidentiality • Background and reference checks • Progressive Discipline	No Relevant Exceptions Noted
3.2	The organization's employee handbook is available for personnel review at all times, and this handbook and other onboarding documents are required to be acknowledged by personnel upon hire.	Interviewed the of SVP Financial Services regarding the Employee Handbook and verified that the organization accesses a portal of information through its secure portal, OneHub, and that BankTEL audits the portal to ensure all staff have viewed files; there is an acknowledgement when employees access the portal, and they must agree to continue, and all onboarding documents and organizational policies must be acknowledged within the first week of employment Observed a random sample of completed employee acknowledgements (4 of 34) and verified that personnel acknowledge the employee handbook upon hire	No Relevant Exceptions Noted
3.3	The organization maintains formal job descriptions for its critical job functions that document roles, responsibilities, and required qualifications for each position.	Interviewed the Sr. Financial Analyst regarding the job descriptions of critical functions of the organization and verified that the following three are considered critical positions: • Manager of Customer Onboarding • Director of Operations • Manager of Customer Care Observed the Director of Operations, Manager of Customer Care, and Manager of Customer Onboarding job descriptions and verified that the roles, responsibilities, and qualifications are clearly communicated and documented by these job descriptions	No Relevant Exceptions Noted

3.4	The organization maintains formal onboarding and offboarding checklists used to guide these processes, including the assignment and revocation of access.	Reviewed the Information Security Policy (dated June 30, 2020) and verified that all employees must acknowledge all company policies during onboarding and all access must be terminated during offboarding Observed OneHub and verified that offboarding and onboarding checklists are maintained and used Observed employee files and verified that onboarding and offboarding checklists are completed and kept in the employee files indefinitely	No Relevant Exceptions Noted
3.5	The organization maintains an Offboarding People Leader Guide used to guide management on the offboarding of terminated or separating employees.	Reviewed the Offboarding People Leader Guide and verified that the guide assists managers with the appropriate procedures for employee terminations Interviewed the Sr. Financial Analyst regarding the organization's hiring and termination policies and procedures and verified that onboarding and offboarding checklists are followed to complete all necessary steps according to policy	No Relevant Exceptions Noted
3.6	The organization maintains and collects all required documentation necessary for the secure onboarding of its new hires.	Interviewed the Sr. Financial Analyst regarding the forms, documents, and acknowledgements used in the new-hire process and verified that the following documents are obtained: • Avid Security • Talent Release • Facilities and Sports Waiver • Confidentiality Agreement • Handbook • Health Insurance Marketplace Coverage Options • Code of Business Conduct • Information Security Policy • Travel Expense and Mobile Policies • BSA AML Compliance Program • OFAC Compliance Policy Observed a random sampling of employee document verifications (4 of 34) and verified that personnel complete these documents upon hire	No Relevant Exceptions Noted

3.7	The organization maintains a formal Background Check Policy used to guide its background check process, requiring all new hires to clear various checks, including identity, employment, and education verifications, criminal history checks, and drug screenings.	Reviewed the Employee Background Check Policy (dated July 1, 2020) and verified that the policy requires the following checks to be performed on all new hires: • Name, address, and date of birth verification Official identification/SSN verification • Employment verification • Educational verification • Credit check requirement • Federal or state criminal record check • Reference checks • Drug screenings	No Relevant Exceptions Noted
3.8	The organization complies with the HIPAA and the GLBA, and formal documentation is maintained regarding these regulations that personnel are required to review and acknowledge.	Reviewed the Compliance with Regulatory Measures document and verified that the policy states that the organization follows GLBA and HIPAA regulations Interviewed the Executive Assistant Administrator regarding regulatory requirements followed by the organization and verified that the organization follows regulatory measures for both GLBA and HIPAA and that both GLBA and HIPAA are acknowledged with clients during the review and signature of the license agreements in regarding confidential and proprietary information	No Relevant Exceptions Noted
3.9	The organization requires personnel to complete trainings regarding sexual harassment, anti-money laundering, PCI DSS, privacy, cybersecurity, and workplace violence during its onboarding process.	Observed a random sample of completed personnel trainings (4 of 34) and verified that personnel are required to complete the following trainings: • Sexual harassment • Anti-money laundering • PCI DSS • Privacy • Cyber security • Workplace violence	No Relevant Exceptions Noted

Control Objective 4 – Environmental Security			
Control Objective 4: Controls provide reasonable assurance that physical assets are adequately protected against environmental hazards and related damage.			
Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
4.1	The organization's facilities are equipped with various environmental controls used to protect its facilities and assets from potential business disruptions or environmental hazards.	Observed a walkthrough of the organization's facility and verified that the environmental controls in place include the following: • Climate control system • Thermostat sensor • Smoke detector • UPS • Generator (testing performed every Friday)	No Relevant Exceptions Noted
4.2	The organization's facilities are protected using a climate control system, thermostat sensors, smoke detectors, UPSs and backup generators.	Observed a walkthrough of the organization's facility and verified that the environmental controls in place include the following: • Climate control system • Thermostat sensor • Smoke detector • UPS • Generator (testing performed every Friday)	No Relevant Exceptions Noted
4.3	The effectiveness of the organization's backup generator is tested weekly.	Observed a walkthrough of the organization's facility and verified that the environmental controls in place include the following: • Climate control system • Thermostat sensor • Smoke detector • UPS • Generator (testing performed every Friday)	No Relevant Exceptions Noted

Control Objective 5 – Physical Security			
Control Objective 5: Controls provide reasonable assurance that physical access to critical applications and data is limited to authorized individuals.			
Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
5.1	The organization maintains a formal Physical Security Policy outlining its requirements and standards for the physical security of its facilities, and this policy is reviewed, updated, and approved annually.	Reviewed the Physical Security Policy (dated May 22, 2020) and verified that the purpose of this policy is to protect the company's physical information systems by setting standards for secure operations and that this policy is reviewed, updated, and approved annually	No Relevant Exceptions Noted
5.2	The organization's sensitive areas are protected by various physical security controls, including the use of door locks and badge access systems, physical intrusion detection systems, and video security surveillance.	Observed the existence of physical security controls for the communications closet and other sensitive areas and verified that they include the following: • Locked doors • Card key access controls (badge readers) • Physical intrusion detection system (alarms and motion activated sensors) • Visitor access control procedures • Employee ID badges • Video surveillance and archives	No Relevant Exceptions Noted
5.3	Access to the organization's facilities is restricted and monitored using a badge access card system that automatically generates access logs.	Observed the existence of physical security controls for the communications closet and other sensitive areas and verified that they include the following: • Locked doors • Card key access controls (badge readers) • Physical intrusion detection system (alarms and motion activated sensors) • Visitor access control procedures • Employee ID badges • Video surveillance and archives Observed access control lists and verified that these lists align with the employee roster Observed access control lists and verified that access control logs are retained for the past month and record the following information:	No Relevant Exceptions Noted

		• Date and time • Name • Doorway	
5.4	The organization maintains a formal Technology Equipment Disposal Policy that outlines the organization's standards and requirements regarding the secure destruction of unneeded media.	Reviewed the Technology Equipment Disposal Policy (dated August 25, 2020) and verified that this policy is reviewed, updated, and approved annually	No Relevant Exceptions Noted
5.5	The organization employs a third-party vendor to securely destroy its decommissioned media, and certificates verifying the secure destruction of media are collected and retained to ensure information security.	Interviewed the Executive Assistant Administrator regarding media destruction and verified that any electronic media is destroyed by the BadDog Shredding Company Observed a receipt from BadDog destruction and verified that media is destroyed by local media destruction company and that receipts of destruction are kept	No Relevant Exceptions Noted
5.6	The organization maintains daily operational security procedures that include the monitoring of the physical security of its facilities.	Reviewed the Daily Operational Security Procedures for Columbus Office (dated July 1, 2020) and verified that the policy requires the use of physical access controls and security alarms	No Relevant Exceptions Noted
5.7	The organization's facilities are equipped with an alarm system, including motion sensors, that generates alerts sent to the organization upon the detection of unauthorized access.	Interviewed the SVP Financial Services regarding the security alarm used at the facility and verified that the alarm is monitored constantly by a local third party and that motion sensors are in place to cover all entrances and windows Reviewed the Alarm Agreement, the Alarm Certificate of Installation, and the Alarm Invoice and verified that the alarm monitoring is current and in force	No Relevant Exceptions Noted
5.8	The organization's facilities are monitored using a security surveillance system, with cameras monitoring all ingress and egress points and sensitive areas.	Observed the facility and verified that cameras are strategically placed to cover all entry and exit points and the sensitive areas of the facility including the communications closets Observed historical video recordings going back to April 4, 2019 and verified that video is retained for at least three months	No Relevant Exceptions Noted

5.9	The organization retains footage generated by its surveillance systems for a minimum of three months to allow proper review of footage.	Observed historical video recordings going back to April 4, 2019 and verified that video is retained for at least three months	No Relevant Exceptions Noted
5.10	The organization maintains formal visitor procedures, including the required use of a visitor log, the assignment of a visitor badge, and the requirement to escort all visitors while on the premises.	Reviewed the Daily Operational Security Procedures for Columbus Office (dated July 1, 2020) and verified that visitors must sign visitor logs before being allowed into the facility Interviewed the Sr. Financial Analyst regarding visitor logs and verified that all visitors must sign a visitor log and confidentiality agreement before being allowed in the facility; all visitors must obtain a visitor badge and be escorted at all times, and additional visitor logs are kept in the communications closet	No Relevant Exceptions Noted
5.11	The organization requires all visitors to complete an entry in its visitor log, which documents all relevant details regarding the visitor, and these logs are retained for at least one year for future review.	Observed the use of a visitor log to record physical access to the facility as well as computer rooms and data centers, and verified that these logs are retained for at least one year Observed the organization's visitor log and verified that the log documents the following information regarding visitors: • Visitor name • Date and time • NDA • Confidentiality statement • Agreement to NDA	No Relevant Exceptions Noted

Control Objective 6 – Logical Access

Control Objective 6: Controls provide reasonable assurance that logical access to programs, data, and operating systems is restricted to authorized personnel.

Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
6.1	The organization maintains a formal identity and Access Management Standards used to govern its logical access procedures and assignment of access.	Reviewed the Identity and Access Management Standard (dated September 27, 2019) and verified that all rights and privileges granted to user IDs are done using least privilege	No Relevant Exceptions Noted
6.2	The organization assigns all personnel logical access using the principle of least privilege.	Reviewed the Identity and Access Management Standard (dated September 27, 2019) and verified that all rights and privileges granted to user IDs are done using least privilege	No Relevant Exceptions Noted
6.3	The organization requires all personnel to be assigned a unique user ID before granting access to organizational assets and information.	Reviewed the Identity and Access Management Standard (dated September 27, 2019) and verified that all rights and privileges granted to user IDs are done using least privilege and that all user ID's must be unique and not shared with anyone	No Relevant Exceptions Noted
6.4	The organization maintains logical access procedures used to assign logical access privileges to personnel, including the use of the organization's internal ticketing system to document and track access requests.	Interviewed the Sr. Financial Analyst regarding access rights and privileges and verified that ServiceNow is used as a ticketing system and that once someone enters a ticket in the HR system, a ticket is entered into ServiceNow, and those tickets are reviewed and approved by management Observed ServiceNow dashboard and verified that tickets are entered showing the request for the groups to which they need access, the manager authorizes access, and IT fulfills the request	No Relevant Exceptions Noted
6.5	The organization requires its passwords to be encrypted at rest and in transit.	Interviewed the Sr. Financial Analyst regarding how password files are rendered unreadable during transmission and storage and verified that passwords are normally communicated verbally and that in the event a password must be transmitted, it is done through encrypted email Observed the email system (Office365), and verified that password files are encrypted by the email system before transmission	No Relevant Exceptions Noted

6.6	The organization encrypts its emails in transit.	Observed the email system (Office365), and verified that password files are encrypted by the email system before transmission	No Relevant Exceptions Noted
6.7	The organization immediately revokes personnel logical access privileges upon personnel termination or separation.	Reviewed the Identity and Access Management Standard (dated September 27, 2019) and verified that accounts are revoked immediately to remove access to the network, systems, services, and applications provisioned to the employee Observed the termination workflow and checklist and verified that all employee access is revoked immediately following termination	No Relevant Exceptions Noted
6.8	The organization requires all access change requests to be documented, tracked, and approved prior to implementation.	Reviewed the Identity and Access Management Standard (dated September 27, 2019) and verified that all access change requests must be properly approved and that approval must be documented Observed ServiceNow ticketing system and verified that all access is approved and documented according to the workflow	No Relevant Exceptions Noted
6.9	The organization maintains formal password parameters and lockout configurations used to ensure the security of its organizational assets.	Interviewed personnel responsible for the setup and removal of user accounts and verified that the organization maintains the following password parameters: • Password settings expire after 90 days • Password complexity settings are enabled • Previous 12 passwords are remembered • The minimum password character length is eight • First-time and password reset practices • User must reset password after first login • Invalid login attempt settings include six invalid login attempts and a 30-minute lockout Observed access lists and group memberships from Azure, including last login date for all users and verified that reports show when each system was last accessed by each user	No Relevant Exceptions Noted

6.10	The organization uses several logical access systems used to restrict access to its organizational assets and information according to the principle of least privilege.	Reviewed the Identity and Access Management Standard (dated September 27, 2019) and verified that logical access systems are in place to manage the rights and privileges of the users of the organization Interviewed the Sr. Financial Analyst regarding the logical access control systems and verified that Azure Active Directory is used by the organization. That Group Policy is used to control the configurations of the systems of the organization, that all organization within AD and GP are done geographically, and that rules are established by roles	No Relevant Exceptions Noted
6.11	The organization maintains a customer and client onboarding process, and clients self-manage their own logical access once the client onboarding process is complete.	Interviewed the Sr. Financial Analyst regarding how clients are registered/deregistered and verified that every customer has their own database, that that database is assigned one user per customer, and that the customer then logs in and manages new users Observed the Avid Application and verified that each client has a designated administrator who then manages the users for their associated organization	No Relevant Exceptions Noted
6.12	The organization requires the use of MFA when accessing its networks and systems remotely.	Reviewed the Network Access and Authentication Policy and verified that MFA is required to access all critical systems of the organization	No Relevant Exceptions Noted

Control Objective 7 – Network Monitoring			
Control Objective 7: Controls provide reasonable assurance that network security and monitoring procedures are in place to identify and report unauthorized access attempts.			
Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
7.1	The organization's monitoring and logging activities are managed by an employed third party, and all detected incidents and anomalies are communicated to the organization for analysis and remediation.	Interviewed the Sr. Financial Analyst regarding the logging/monitoring tools of the organization and verified that all logging and monitoring is performed by third party Observed a CyberlinkASP Monitoring ticket and verified that communications about events captured and logged by the third party are communicated to the organization	No Relevant Exceptions Noted
7.2	The organization employs a third party to implement firewalls and edge security systems and controls, ensuring the managed monitoring and security of its systems, networks, and assets.	Interviewed the Sr. Financial Analyst regarding the use of IDSs/IDPs and verified that the organizations edge security is managed by third party, CyberlinkASP, and that they own and manage the firewalls for the organization and log any alerts that are detected using their SolarWinds platform Observed the CyberlinkASP contract and verified that all edge security is managed by this third party	No Relevant Exceptions Noted

Control Objective 8 – Configuration Management			
Control Objective 8: Controls provide reasonable assurance that systems are configured in accordance with documented standards to identify and report unauthorized changes.			
Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
8.1	The organization's formal Identity and Access Management Standard document and implement the organization's configuration standards for all systems, networks, and standards.	Reviewed the Identity and Access Management Standard (dated September 27, 2019) and verified that the policy outlines the configuration standards of the organization	No Relevant Exceptions Noted
8.2	The organization uses group policies to enforce its formal configuration standards.	Interviewed the Sr. Financial Analyst regarding the documentation of system configuration standards and verified that the Identity and Access Management Standard illustrates the configuration requirements for the systems of the organization; all equipment is managed by AvidXchange IT and SCCM is used to deploy standard configuration images to all new laptops Observed that the following group policies are implemented on assets and systems: • Sets up the Windows update servers • The enterprise CA • Not storing the LAN/MAN hash passwords • Kerberos policies • Account lockouts • Password policy • Block removable storage • Users do not have local admin rights • Establishes local admin users • Disables guest account • Managed with InTune and SCCM • Printer shares • Drive mapping	No Relevant Exceptions Noted
8.3	The organization reviews, updates, and approves its formal configuration standards annually.	Reviewed the Identity and Access Management Standard (dated September 27, 2019) and verified that this policy is reviewed, updated, and approved annually	No Relevant Exceptions Noted
8.4	The organization maintains formal Vulnerability Management Standards used to detect, manage, and remediate possible system vulnerabilities.	Reviewed the Vulnerability Management Standards (dated September 30, 2019) and verified that members of the AvidXchange Security Team remain abreast of new and	No Relevant Exceptions Noted

		emerging vulnerabilities using email services, automated news feed boards, and news publications daily to stay informed about emerging threats and vulnerabilities; Security Team members periodically evaluate automated reports from the vulnerability management software to continuously improve detection and remediation capabilities Interviewed the Sr. Financial Analyst regarding how personnel with system configuration responsibilities stay knowledgeable of appropriate ways to securely configure the organization's systems and verified that the Security Operations Team reviews and analyzes security publications to determine potential impacts to the organization	
8.5	The organization's Security Team review industry-best practice configuration standards on a continuous basis to determine any necessary changes to its configuration standards.	Reviewed the Vulnerability Management Standards (dated September 30, 2019) and verified that members of the AvidXchange's Security Team remain abreast of new and emerging vulnerabilities using email services, automated news feed boards, and news publications daily to stay informed about emerging threats and vulnerabilities; Security Team members periodically evaluate automated reports from the vulnerability management software to continuously improve detection and remediation capabilities Interviewed the Sr. Financial Analyst regarding how personnel with system configuration responsibilities stay knowledgeable of appropriate ways to securely configure the organization's systems and verified that the Security Operations Team reviews and analyzes security publications to determine potential impacts to the organization	No Relevant Exceptions Noted
8.6	The organization's Security Team members periodically evaluate automated reports from the vulnerability management software to continuously improve detection and remediation capabilities.	Reviewed the Vulnerability Management Standards (dated September 30, 2019) and verified that members of the AvidXchange's Security Team remain abreast of new and emerging vulnerabilities using email services, automated news feed boards, and news publications daily to stay	No Relevant Exceptions Noted

		informed about emerging threats and vulnerabilities; Security Team members periodically evaluate automated reports from the vulnerability management software to continuously improve detection and remediation capabilities Interviewed the Sr. Financial Analyst regarding how personnel with system configuration responsibilities stay knowledgeable of appropriate ways to securely configure the organization's systems and verified that the Security Operations Team reviews and analyzes security publications to determine potential impacts to the organization	
8.7	The organization's Security Operations Team reviews and analyzes security publications to determine potential impacts to the organization.	Reviewed the Vulnerability Management Standards (dated September 30, 2019) and verified that members of the AvidXchange's Security Team remain abreast of new and emerging vulnerabilities using email services, automated news feed boards, and news publications daily to stay informed about emerging threats and vulnerabilities; Security Team members periodically evaluate automated reports from the vulnerability management software to continuously improve detection and remediation capabilities Interviewed the Sr. Financial Analyst regarding how personnel with system configuration responsibilities stay knowledgeable of appropriate ways to securely configure the organization's systems and verified that the Security Operations Team reviews and analyzes security publications to determine potential impacts to the organization	No Relevant Exceptions Noted
8.8	The organization's configuration standards are based upon industry-accepted best practices (SANS), and training regarding these best practice standards are required to be completed by personnel biannually.	Observed SANS training certificates (dated July 2020 and from Jan 2020) and verified that SANS training is conducted twice per year by members of the Security Team	No Relevant Exceptions Noted
8.9	The organization maintains a formal change management policy used to govern its change management processes, which includes the	Reviewed the Change Management Policy (dated June 15, 2020) and verified that the organization documents a formal change	No Relevant Exceptions Noted

	submission of a formal change request, the categorization and prioritization of changes, the analysis and justification of the change, the approval of the change, change planning and implementation, and the performance of a post-implementation review.	management policy including the following stages: • Change request • Categorize and prioritize • Analyze and justify • Approve and schedule • Planning and implementation • Post-implementation review	
8.10	The organization's change request tickets are submitted for review and approval, and these change request tickets document all relevant information regarding the requested change.	Observed a ServiceNow ticket requesting to install Qualys and AMP agents on APP1 and DBVM1 for the Ascend system and verified that the organization's change request tickets document the following information for all change requests: • Clearly identified roles and responsibilities • Impact or risk analysis of the change request • Testing prior to implementation of change • Authorization and approval (changes must be approved by the Security Board) • Process for notifying clients prior to changes being made which may impact their service • Post-installation validation • Back-out or recovery plans	No Relevant Exceptions Noted
8.11	The organization requires all changes requests to include identified roles and responsibilities and a risk analysis of the change.	Observed a ServiceNow ticket requesting to install Qualys and AMP agents on APP1 and DBVM1 for the Ascend system and verified that the organization's change request tickets document the following information for all change requests: • Clearly identified roles and responsibilities • Impact or risk analysis of the change request • Testing prior to implementation of change • Authorization and approval (changes must be approved by the Security Board) • Process for notifying clients prior to changes being made which may impact their service • Post-installation validation • Back-out or recovery plans	No Relevant Exceptions Noted

8.12	The organization requires all changes to be tested prior to implementation, and recovery plans to be documented.	Observed a ServiceNow ticket requesting to install Qualys and AMP agents on APP1 and DBVM1 for the Ascend system and verified that the organization's change request tickets document the following information for all change requests: • Clearly identified roles and responsibilities • Impact or risk analysis of the change request • Testing prior to implementation of change • Authorization and approval (changes must be approved by the Security Board) • Process for notifying clients prior to changes being made which may impact their service • Post-installation validation • Back-out or recovery plans	No Relevant Exceptions Noted
8.13	The organization requires all requested changes to be reviewed and approved by the Security Board prior to implementation.	Observed a ServiceNow ticket requesting to install Qualys and AMP agents on APP1 and DBVM1 for the Ascend system and verified that the organization's change request tickets document the following information for all change requests: • Clearly identified roles and responsibilities • Impact or risk analysis of the change request • Testing prior to implementation of change • Authorization and approval (changes must be approved by the Security Board) • Process for notifying clients prior to changes being made which may impact their service • Post-installation validation • Back-out or recovery plans	No Relevant Exceptions Noted

Control Objective 9 – Vulnerability Management

Control Objective 9: Controls provide reasonable assurance that systems, processes, and software are tested periodically to ensure that security is maintained over time and after any changes.

Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
9.1	The organization uses an antivirus solution to monitor and protect its organizational assets and systems from malicious software and unauthorized access.	Interviewed the Sr. Financial Analyst regarding the use of antivirus software and verified that the organization uses Cisco AMP for antivirus and that it is cloud hosted for end user protection Observed the system configuration of CISCO AMP and verified that the organization's antivirus settings include: • The performance of updates every four hours • That local users cannot disable or alter the antivirus settings • That alerts are sent immediately when a potential virus is detected Alerts are sent via reports in emails to Security Operations Team • That logs are generated and retained for 30 days Observed that antivirus scans are performed incrementally daily and fully weekly	No Relevant Exceptions Noted
9.2	The organization maintains antivirus configuration settings that include the performance of continual updates and the automatic generation of alerts and logs documenting identified security incidents.	Interviewed the Sr. Financial Analyst regarding the use of antivirus software and verified that the organization uses Cisco AMP for antivirus and that it is cloud hosted for end user protection Observed the system configuration of CISCO AMP and verified that the organization's antivirus settings include: • The performance of updates every four hours • That local users cannot disable or alter the antivirus settings • That alerts are sent immediately when a potential virus is detected Alerts are sent via reports in emails to Security Operations Team	No Relevant Exceptions Noted

		• That logs are generated and retained for 30 days Observed that antivirus scans are performed incrementally daily and fully weekly	
9.3	The organization's antivirus solutions perform incremental scans daily and full scans of all systems weekly.	Interviewed the Sr. Financial Analyst regarding the use of antivirus software and verified that the organization uses Cisco AMP for antivirus and that it is cloud hosted for end user protection Observed the system configuration of CISCO AMP and verified that the organization's antivirus settings include: • The performance of updates every four hours • That local users cannot disable or alter the antivirus settings • That alerts are sent immediately when a potential virus is detected Alerts are sent via reports in emails to Security Operations Team • That logs are generated and retained for 30 days Observed that antivirus scans are performed incrementally daily and fully weekly	No Relevant Exceptions Noted
9.4	The organization retains logs generated by its antivirus solution for 30 days to allow appropriate review and recovery activities.	Interviewed the Sr. Financial Analyst regarding the use of antivirus software and verified that the organization uses Cisco AMP for antivirus and that it is cloud hosted for end user protection Observed the system configuration of CISCO AMP and verified that the organization's antivirus settings include: • The performance of updates every four hours • That local users cannot disable or alter the antivirus settings • That alerts are sent immediately when a potential virus is detected Alerts are sent via reports in emails to Security Operations Team • That logs are generated and retained for 30 days Observed that antivirus scans are performed incrementally daily and fully weekly	No Relevant Exceptions Noted

9.5	The organization maintains a formal Patch Management Policy governing the organization's implementation of necessary patches within two weeks of initial release.	Reviewed the Patch Management Policy (dated July 1, 2020) and verified that critical security patches are implemented within two weeks	No Relevant Exceptions Noted
9.6	The organization's formal Client Data Policies and Procedures govern the organization's use, handling, and retention of client data in compliance with its regulatory requirements.	Reviewed the Client Data Policies and Procedures (dated June 30, 2020) and verified that all client data is retained for 12 months Interviewed the Sr. Financial Analyst regarding the data retention requirements of the organization and verified that all client data must be kept for 12 months and that HR and financial records are kept indefinitely	No Relevant Exceptions Noted
9.7	Client data is retained for one year and personnel human resources information is retained indefinitely in compliance with the organization's regulatory requirements.	Reviewed the Client Data Policies and Procedures (dated June 30, 2020) and verified that all client data is retained for 12 months Interviewed the Sr. Financial Analyst regarding the data retention requirements of the organization and verified that all client data must be kept for 12 months and that HR and financial records are kept indefinitely	No Relevant Exceptions Noted
9.8	The organization maintains a formal Encryption Policy used to govern the organization's use and management of encryption keys and encryption algorithms.	Reviewed the Encryption Policy (dated July 1, 2020) and verified that the organization documents acceptable encryption algorithms and guidelines for key management Interviewed the Sr. Financial Analyst regarding how the organization manages encryption keys and verified that BitLocker is used to secure the devices of the organization and that the BitLocker keys are managed by AD and SCCM	No Relevant Exceptions Noted
9.9	The organization requires the use of secure shell (SSL) encryption certificates to protect its data at rest in transmission within its web applications.	Interviewed the Sr. Financial Analyst regarding best practices regarding encryption methods for open transmission of sensitive data and verified that the web application of the organization is protected with SSL certificates Observed ImmuniWeb tests and verified that the main host site achieved an "A+" rating, the web application site achieved an "A" rating, and that the web application site achieved a "B" rating	No Relevant Exceptions Noted

9.10	The organization maintains a Data Classification Policy used to ensure that the organization's data is categorized, handled, and retained in accordance with the organization's regulatory requirements.	Reviewed the Data Classification Policy (dated July 1, 2020) and verified that the organization classifies data as personal, public, organizational, confidential, and critical Observed the systems and data of the organization and verified that organizational, confidential, and critical data are used daily and are maintained in compliance with company policies	No Relevant Exceptions Noted
9.11	The organization maintains formal data classifications that determine the proper handling of data, and these classifications include public, organizational, confidential, and critical.	Reviewed the Data Classification Policy (dated July 1, 2020) and verified that the organization classifies data as personal, public, organizational, confidential, and critical Observed the systems and data of the organization and verified that organizational, confidential, and critical data are used daily and are maintained in compliance with company policies	No Relevant Exceptions Noted

Control Objective 10 – Business Continuity and Disaster Recovery

Control Objective 10: Controls provide reasonable assurance that the organization is able to maintain or recover business-critical processing capabilities in the event of the loss of a facility or a major system failure.

Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
10.1	The organization maintains a formal Disaster Recovery and Business Continuity Plan uses to restore business operations in the events of a disruption to business operations or a potential disaster or environmental hazard.	Reviewed the 2020 Disaster Recovery and Business Continuity Plan (dated June 18, 2020) and verified that this policy is reviewed, updated, and approved annually Reviewed the 2020 Disaster Recovery and Business Continuity Plan (dated June 18, 2020) and verified that it includes the following attributes: • Recovery response teams • List of critical components and software • Notifications and team responsibilities • IT restoration procedures • Requirements to retain evidence of BCP maintenance • Management approval	No Relevant Exceptions Noted
10.2	The organization's Disaster Recovery and Business Continuity Plan is reviewed, updated, and approved annually.	Reviewed the 2020 Disaster Recovery and Business Continuity Plan (dated June 18, 2020) and verified that the BCP includes the following attributes: • Recovery response teams • List of critical components and software • Notifications and team responsibilities • IT restoration procedures • Requirements to retain evidence of BCP maintenance • Management approval	No Relevant Exceptions Noted
10.3	The organization's Disaster Recovery and Business Continuity Plan includes a list of critical components and software and defined notification and team responsibilities for the Recovery Response Team.	Reviewed the 2020 Disaster Recovery and Business Continuity Plan (dated June 18, 2020) and verified that the BCP includes the following attributes: • Recovery response teams • List of critical components and software • Notifications and team responsibilities • IT restoration procedures	No Relevant Exceptions Noted

		• Requirements to retain evidence of BCP maintenance • Management approval	
10.4	The organization maintains a Recovery Response Team that is responsible for implementing the organization's business continuity and recovery procedures.	Reviewed the 2020 Disaster Recovery and Business Continuity Plan (dated June 18, 2020) and verified that the BCP includes the following attributes: • Recovery response teams • List of critical components and software • Notifications and team responsibilities • IT restoration procedures • Requirements to retain evidence of BCP maintenance • Management approval	No Relevant Exceptions Noted
10.5	The organization tests its Disaster Recovery and Business Continuity Plan at least annually, and the results of these tests are analyzed by management to determine and necessary changes or adjustments to the plan.	Interviewed the Sr. Financial Analyst regarding testing of the BCP and verified that the plan is tested at least annually and that after testing, the results are reviewed, and adjustments are made to the plan as needed Observed BCP Test Results (dated August 7, 2020) and verified that a desktop exercise was conducted with a client to restore data	No Relevant Exceptions Noted

Control Objective 11 – Vendor Management			
Control Objective 11: Controls provide reasonable assurance that vendors are appropriately vetted, approved, and monitored to define the services provided and limit third-party access to sensitive data.			
Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
11.1	The organization maintains a formal Vendor Management Policy and a formal Vendor Qualification and Screening Process used to perform due diligence on all potential vendors.	Reviewed the BankTEL Vendor Management Policy (dated July 1, 2020) and verified that the policy states the procedures for engaging and monitoring service providers, including the organization's formal Vendor Qualification and Screening Process, which includes the following: • Reference checks • Financial status checks • Use of Argos Risk to manage any risks associated with critical vendors • The Controller is responsible for leading the process and ensuring that all steps are carried out properly	No Relevant Exceptions Noted
11.2	The organization's due diligence process includes the performance of vendor reference checks and financial status checks.	Reviewed the BankTEL Vendor Management Policy (dated July 1, 2020) and verified that the policy states the procedures for engaging and monitoring service providers, including the organization's formal Vendor Qualification and Screening Process, which includes the following: • Reference checks • Financial status checks • Use of Argos Risk to manage any risks associated with critical vendors • The Controller is responsible for leading the process and ensuring that all steps are carried out properly	No Relevant Exceptions Noted
11.3	The organization monitors its vendors' service delivery and compliance statuses by collecting and reviewing annual independent third-party audits of vendor controls.	Reviewed the BankTEL Vendor Management Policy (dated July 1, 2020) and verified that critical third parties are monitored by obtaining annual SOC audit reports from each	No Relevant Exceptions Noted

Control Objective 12 – Application Development			
Control Objective 12: Controls provide reasonable assurance that changes to production systems undergo an implementation process, in which they are tracked and reviewed to check for errors.			
Ctrl #	Controls Specified by Company	Testing Performed by Service Auditor	Test Results
12.1	Application development-related changes must adhere to the organization's formal Change Management Policy, including the submission of change requests via the organization's ticketing system.	Observed a random sample of feature requests (three of six) and verified that notes are documented and retained for reasons why a requested application change was approved or declined, and the following attributes were observed for each of the requests sampled: • Change requests reviewed by the Principal Software Engineer and the Senior Vice President • Technical specifications are developed for significant changes • A testing strategy is prepared by the Senior VP and followed by the Product Support Specialists • Source code is copied to a test environment • Program changes are tested in a separate, controlled environment • The Senior Vice President performs the migration of changes to production in a controlled manner quarterly • Back-out procedures are documented	No Relevant Exceptions Noted
12.2	Application, software, or code change requests must be reviewed and approved by the Principal Software Engineer and the Senior Vice President.	Observed a random sample of feature requests (three of six) and verified that notes are documented and retained for reasons why a requested application change was approved or declined, and the following attributes were observed for each of the following requests sampled: • Change requests reviewed by the Principal Software Engineer and the Senior Vice President • Technical specifications are developed for significant changes • A testing strategy is prepared by the Senior VP and followed by the Product Support Specialists • Source code is copied to a test environment	No Relevant Exceptions Noted

		• Program changes are tested in a separate, controlled environment • The Senior Vice President performs the migration of changes to production in a controlled manner quarterly • Back-out procedures are documented	
12.3	Technical specifications are developed for significant application, software, and code changes.	Observed a random sample of feature requests (three of six) and verified that notes are documented and retained for reasons why a requested application change was approved or declined, and the following attributes were observed for each of the following requests sampled: • Change requests reviewed by the Principal Software Engineer and the Senior Vice President • Technical specifications are developed for significant changes • A testing strategy is prepared by the Senior VP and followed by the Product Support Specialists • Source code is copied to a test environment • Program changes are tested in a separate, controlled environment • The Senior Vice President performs the migration of changes to production in a controlled manner quarterly • Back-out procedures are documented	No Relevant Exceptions Noted
12.4	Testing strategies are developed and implemented for all application development-related changes, and these strategies are developed and implemented by the Senior Vice President and Product Support Specialists.	Observed a random sample of feature requests (three of six) and verified that notes are documented and retained for reasons why a requested application change was approved or declined, and the following attributes were observed for each of the following requests sampled: • Change requests reviewed by the Principal Software Engineer and the Senior Vice President • Technical specifications are developed for significant changes • A testing strategy is prepared by the Senior VP and followed by the Product Support Specialists • Source code is copied to a test environment • Program changes are tested in a separate, controlled environment	No Relevant Exceptions Noted

		• The Senior Vice President performs the migration of changes to production in a controlled manner quarterly • Back-out procedures are documented	
12.5	Back-out procedures are documented for all application development-related changes.	Observed a random sample of feature requests (three of six) and verified that notes are documented and retained for reasons why a requested application change was approved or declined, and the following attributes were observed for each of the following requests sampled: • Change requests reviewed by the Principal Software Engineer and the Senior Vice President • Technical specifications are developed for significant changes • A testing strategy is prepared by the Senior VP and followed by the Product Support Specialists • Source code is copied to a test environment • Program changes are tested in a separate, controlled environment • The Senior Vice President performs the migration of changes to production in a controlled manner quarterly • Back-out procedures are documented	No Relevant Exceptions Noted
12.6	Changes to source code, programs, applications, or software are tested in a separate, controlled environment prior to implementation.	Observed a random sample of feature requests (three of six) and verified that notes are documented and retained for reasons why a requested application change was approved or declined, and the following attributes were observed for each of the following requests sampled: • Change requests reviewed by the Principal Software Engineer and the Senior Vice President • Technical specifications are developed for significant changes • A testing strategy is prepared by the Senior VP and followed by the Product Support Specialists • Source code is copied to a test environment • Program changes are tested in a separate, controlled environment	No Relevant Exceptions Noted

		• The Senior Vice President performs the migration of changes to production in a controlled manner quarterly • Back-out procedures are documented	
12.7	The organization maintains a formal Software Development Process used to guide its software development processes.	Reviewed the Software Development Process (dated August 7, 2020) and verified that Software Developers are required to obtain 20 CPE credits every five years	No Relevant Exceptions Noted
12.8	The organization requires all of its Software Developers to pursue and maintain additional continuing professional education credits every five years.	Reviewed the Software Development Process (dated August 7, 2020) and verified that Software Developers are required to obtain 20 CPE credits every five years	No Relevant Exceptions Noted
12.9	Access to the organization's source code repository is restricted using a TFS.	Reviewed the Software Development Process (dated August 7, 2020) and verified that source code and version control is restricted using Microsoft TFS Interviewed the SVP Financial Services regarding software development and verified that Microsoft TFS is the source code repository and is used for version control; developers have the only access to the TFS repository, and the Development server is isolated and not accessible by other employees and domain users	No Relevant Exceptions Noted
12.10	Version control is implemented using a TFS.	Reviewed the Software Development Process (dated August 7, 2020) and verified that source code is restricted using Microsoft TFS and version control is restricted using Microsoft TFS Interviewed the SVP of Financial Services regarding software development and verified that Microsoft TFS is the source code repository and is used for version control; developers have the only access to the TFS repository, and the Development server is isolated and not accessible by other employees and domain users	No Relevant Exceptions Noted
12.11	The organization's application and software development, production, and testing environments are logically and physically separated from each other to ensure authorized access and the segregation of duties.	Observed the CyberLinkASP Development, Rackspace, and Jack Henry systems and verified that system administration and development staff log into these production and development systems separately and that these systems are unique and separate from each other	No Relevant Exceptions Noted

12.12	The organization requires all of its pushes to production to be approved by senior management prior to implementation.	Observed the approval process and verified that senior management is required to review testing results and approve any pushes to production and that these pushes are conducted quarterly after all customers have been notified of the upcoming changes	No Relevant Exceptions Noted
12.13	The organization conducts all of its pushes to production quarterly.	Observed the approval process and verified that senior management is required to review testing results and approve any pushes to production and that these pushes are conducted quarterly after all customers have been notified of the upcoming changes	No Relevant Exceptions Noted
12.14	The organization notifies its clients and customers of upcoming pushes to production or changes to existing applications or software.	Observed the approval process and verified that senior management is required to review testing results and approve any pushes to production and that these pushes are conducted quarterly after all customers have been notified of the upcoming changes	No Relevant Exceptions Noted
12.15	The organization employs an independent third-party to conduct annual application penetration tests.	Reviewed the Software Development and Infrastructure Security Policy (dated June 25, 2020) and verified that the organization employs an independent third-party to conduct annual application penetration tests	No Relevant Exceptions Noted