CONFIDENTIALITY AGREEMENT
AVIDXCHANGE AUDIT AND SECURITY INFORMATION

AvidXchange, Inc. (together with its affiliates, "AvidXchange"), with its principal office at 1210 AvidXchange Lane, Charlotte, NC 28206, provides accounts payable and payment automation services (together with any ancillary services, the "Services"). You have requested, and AvidXchange has agreed to provide, certain confidential or proprietary information relating to the security and audit practices of AvidXchange with respect to the Services subject to the terms and conditions contained in this Confidentiality Agreement (the "Agreement"). As a condition to AvidXchange disclosing this information to you, you hereby represent and agree that: (a) you are an authorized representative of, and are requesting this information on behalf of, a business that is a current or prospective customer or business partner of AvidXchange or a professional advisor (e.g., financial, legal or technical professional) to a customer or business partner of AvidXchange (such business and you are referred to collectively herein as, the "Recipient"); (b) you and any other Recipient will comply with the terms of this Confidentiality Agreement (the "Agreement") and use it for the sole purpose of evaluating the Services for the AvidXchange customer, prospect or business partner; and (c) you are at least 18 years old and otherwise legally competent to enter into this Agreement.

AGREEMENT

1. Proprietary Information. "Proprietary Information" shall mean non-public information regarding AvidXchange or any of its subsidiaries or their respective assets or businesses which is or has been furnished to Recipient, directly or indirectly, in any form or media. Proprietary Information includes, without limitation, the audit and/or security report concerning AvidXchange that is included with this Agreement and any other information concerning the infrastructure or security of AvidXchange's Services, such as the technology used to provide the Services, its network or computing environment or information processes, procedures, systems or vendor relationships. All rights in and to Proprietary Information are reserved by AvidXchange and no license to Recipient under any trade secret, trademark, patent or copyright, or applications which are now or may hereafter be owned by AvidXchange is either granted or implied by the disclosure of Proprietary Information to Recipient.

2. Purpose. Recipient may use the Proprietary Information solely for the purpose of evaluating security and compliance policies and procedures of AvidXchange with respect to the Services (the "Purpose") solely in its capacity as a Recipient or potential Recipient of AvidXchange.

3. Confidentiality. Recipient shall keep secret, and prevent unauthorized duplication, use and disclosure of, the Proprietary Information in the same manner as it protects its own confidential information, but with no less than a reasonable degree of care. Recipient will not, and will not permit any of its authorized representatives to, use any Proprietary Information for any reason other than the Purpose, and will not make any Proprietary Information available to any third parties, except for those of its officers, directors, employees and financial, technical or legal advisors (collectively, "Authorized Representatives") who have a need to know it solely in connection with the Purpose and who have agreed to protect it as required by the Agreement. A breach of the Agreement by any Authorized Representative shall be deemed a breach by Recipient. Recipient shall promptly notify AvidXchange in writing at the address first written above (Attn: Legal Department) if it learns of any unauthorized duplication, use or disclosure of the Proprietary Information. Promptly upon request, Recipient shall return to AvidXchange, or destroy and certify to AvidXchange the destruction of, any materials of any kind containing Proprietary Information.

If Recipient receives any valid, legally enforceable demand to disclose Proprietary Information from any judicial or governmental entity, Recipient shall promptly notify AvidXchange in writing at the address first written above (Attn: Legal Department), so that AvidXchange may seek a protective order or other appropriate remedy. If such protective order or other remedy is not obtained or available, Recipient may disclose only that portion of the Proprietary Information which is legally required to be disclosed.

4. Nature of Information. All Proprietary Information is provided "as is" without any warranties of any kind. Recipient acknowledges and agrees that it is not acquiring any rights against any auditor of AvidXchange or the auditor's respective affiliates, partners, agents, representatives or employees (collectively, "Auditor") and that Auditor is not assuming any liability or duty to Recipient with respect to the Services or any report prepared by Auditor. Further, Recipient acknowledges and agrees Auditor has made no representation or warranty to Recipient with respect to the Services or any report or audit prepared or performed by Auditor.

5. Term. Proprietary Information will cease to be considered as such, and all protections will cease to be required, when and if it becomes generally available to the public other than as a result of breach of this Agreement.

6. Miscellaneous. The Agreement is the entire agreement and understanding between the parties and supersedes all prior agreements, written or oral, with respect to the subject matter hereof. Recipient acknowledges that the confidentiality obligations contained herein are in furtherance of any other terms and conditions contained in any separate agreement(s) between Recipient and AvidXchange and that provisions contained herein do not modify, supersede or limit any such agreement(s). The Agreement shall be deemed made in and governed by the laws of the state of North Carolina without reference to the conflicts of law principles of any jurisdiction. If any provision of the Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the Agreement shall be modified to reflect the intent of the invalid or unenforceable provision to the greatest possible extent, with all other provisions remaining in full force and effect. The failure of AvidXchange to enforce any right or provision in the Agreement shall not constitute a waiver of such right or provision unless acknowledged and agreed to by AvidXchange in writing. No waiver shall be deemed a continuing waiver or waiver in respect of any subsequent breach or default, whether of similar or different nature, unless expressly so stated in writing. The Agreement may be executed and transmitted electronically, and any such electronically executed and/or transmitted copies shall be deemed to be valid as originals.

ACCEPTANCE

Recipient is agreeing to be bound by the terms of this Agreement and you are representing that you are authorized to sign this Agreement on behalf of Recipient. If you are not so authorized or Recipient does not agree to all of the terms contained in the Agreement, do not view the audit and/or security report concerning AvidXchange that is included with this Agreement, immediately close it, and permanently destroy it.

January 5, 2021

Dear AvidXchange Customer,

Our outside auditor, Parsons CPA PLLC, examined the general controls of AvidXchange, Inc. for the period ending September 30, 2020, and issued a report summarizing our control objectives, internal control activities and test results. A copy of this report was recently provided to your organization.

We confirm, to the best of our knowledge and belief, that in providing this report, we have supplied you with all significant, relevant information of which we are aware, and we confirm that we have fairly described the controls of AvidXchange, Inc. In addition, we confirm, to the best of our knowledge and belief, the following:

- The description of controls contained in the report presents fairly, in all material respects, the aspects of our controls that may be relevant to a user organization's internal control.
- We believe our controls are suitably designed to achieve the specified control objectives.
- There have been no significant changes in controls since our last examination.
- The controls described have been in operation since the conclusion of the reporting period and through December 31, 2020.

If you have any questions about information provided in the SOC 1 report, please contact me at aharmon@avidxchange.com.

Sincerely,

Tony Harmon
Sr. Director, Internal Audit

SYSTEM AND ORGANIZATION CONTROLS REPORT (SOC 1 - Type 2)

Report on AvidXchange, Inc.'s Description of Its Systems and on the Suitability of the Design and Operating Effectiveness of Its Controls

For the Period from October 1, 2019, to September 30, 2020

ParsonsCPA

TABLE OF CONTENTS

SECTION I – INDEPENDENT SERVICE AUDITORS' REPORT

ParsonsCPA

Parsons CPA, PLLC
927 East Boulevard
Charlotte, NC 28203

Tel: (704) 332-4000
Fax: (704) 332-7088
www.parsonscpa.com

INDEPENDENT SERVICE AUDITORS' REPORT

To the Board of Directors of AvidXchange, Inc.:

Scope

We have examined AvidXchange, Inc.'s ("AvidXchange" or the "Company") description of its Software-as-a-Service ("SaaS") System (the "System") entitled "Description of the Software-as-a-Service System Provided by AvidXchange, Inc." for processing user entities' transactions throughout the period October 1, 2019, to September 30, 2020 (the "description") and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "AvidXchange, Inc.'s Management Assertion" (the "assertion"). The controls and control objectives included in the description are those that management of the Company believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the System that are not likely to be relevant to user entities' internal control over financial reporting.

Certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the Company'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.

The Company uses several subservice organizations to provide data center operations, check, and e-payment processing, as well as other monetary transaction functions. The description includes only the control objectives and related controls of the Company and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by the Company can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. Our examination did not extend to controls of the subservice organizations and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

In Section II, the Company 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. The Company is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditors’ 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 October 1, 2019, 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 and operating effectiveness of controls involves:

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management’s assertion.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

Inherent Limitations

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

Description of Tests of Controls

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

Opinion

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

a. The description fairly presents the System that was designed and implemented throughout the period October 1, 2019, 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 October 1, 2019, to September 30, 2020, and subservice organizations and user entities applied the complementary controls assumed in the design of the Company's controls throughout the period October 1, 2019, 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 October 1, 2019, to September 30, 2020, if complementary subservice organizations and user entity controls assumed in the design of the Company's controls operated effectively throughout the period October 1, 2019, to September 30, 2020.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of the Company, user entities of the Company's System during some or all of the period October 1, 2019, 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 misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Parsons CPA PLLC

Parsons CPA, PLLC
Charlotte, North Carolina

December 18, 2020

SECTION II – AVIDXCHANGE, INC.'S MANAGEMENT ASSERTION

AvidXchange, Inc.’s Management Assertion

We have prepared the description of AvidXchange, Inc.’s (“AvidXchange” or the “Company”) Software-as-a-Service System entitled “Description of the Software-as-a-Service System Provided by AvidXchange, Inc.” for processing user entities’ transactions throughout the period October 1, 2019, to September 30, 2020 (the “description”), for user entities of the System during some or all of the period October 1, 2019, to September 30, 2020, and their auditors who audit and report on such user entities’ financial statements or internal control over financial statement reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the System themselves when assessing the risks of material misstatement of user entities’ financial statements.

The Company uses several subservice organizations to provide data center operations, check, and e-payment processing, as well as other monetary transaction functions when processing user entities’ transactions. The description includes only the control objectives and related controls of the Company 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.

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

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

1) The description fairly presents the Company’s Software-as-a-Service System made available to user entities of the System during some or all of the period October 1, 2019, to September 30, 2020, for processing user entities’ transactions as it relates to controls that are likely to be relevant to user entities’ internal control over financial reporting. The criteria we used in making this assertion were that the description:

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

      i) The types of services provided, including, as appropriate, the classes of transactions processed.
      ii) The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the System.
      iii) The information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
      iv) How the System captures and addresses significant events and conditions other than transactions.

v) The process used to prepare reports and other information for user entities.

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

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

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

b) Includes relevant details of changes to the Software-as-a-Service System during the period covered by the description.

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

2) The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period October 1, 2019, to September 30, 2020, to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of the Company's controls throughout the period October 1, 2019, to September 30, 2020. The criteria we used in making this assertion were that:

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

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

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

Angelic Gibson
Chief Information Officer

Joel Wilhite
Chief Financial Officer

SECTION III – DESCRIPTION OF THE SOFTWARE-AS-A-SERVICE SYSTEM PROVIDED BY AVIDXCHANGE, INC.

Overview of Operations

AvidXchange, Inc. is an industry leader in automating the "Purchase-to-Pay" processes for mid-market companies throughout North America. With a nineteen-year history, AvidXchange provides software-as-a-service ("SaaS") solutions and services to more than 6,000 clients spanning multiple industries, including real estate, financial services, energy, healthcare, education, and construction. Solutions include electronic invoice capture, intelligent workflow routing, and automated payments, resulting in reduced costs, improved productivity, and elimination of paper from the traditional accounts payable and payment processes.

Company Background

Founded in 2000, AvidXchange has completed several strategic acquisitions that have expanded the customer relationships available to subscribe to its payment services and its suite of specialized payment solutions. In 2010, the Company acquired substantially all of the assets and liabilities of EnergySolve, L.L.C. through its wholly owned subsidiary, AvidXchange Financial Services, Inc. ("AFS"). AFS specializes in the processing and analytics of utility bills for corporations and state and local government agencies. In 2014, AvidXchange acquired the stock of Piracle, Inc. ("Piracle"), a bill payment company with both SaaS and client server check printing solutions primarily targeted to the real estate and construction industries. In 2015, AvidXchange acquired Strongroom Solutions, Inc. ("Strongroom"), a provider of accounts payable software for financial institutions and companies that manage invoices and payments for homeowner associations (HOAs) nationwide. In 2017, AvidXchange acquired the assets and liabilities of Ariett Business Solutions, Inc., a company serving customers primarily in the software/technology, business services, non-profit, healthcare, and education industries.

Control Environment

The overall environment reflects the Committee of Sponsoring Organizations (COSO) Internal Control framework. The framework consists of five interrelated components and seventeen principles which include:

Internal Control Component	Principles
Control environment	1. Demonstrate commitment to integrity and ethical values 2. Ensure that the Board exercises oversight responsibility 3. Establish structures, reporting lines, authorities and responsibilities 4. Demonstrate commitment to a competent workforce 5. Hold people accountable
Risk assessment	6. Specify appropriate objectives 7. Identify and analyze risks 8. Evaluate fraud risks 9. Identify and analyze changes that could significantly affect internal controls

Internal Control Component	Principles
Control activities	10. Select and develop control activities that mitigate risks 11. Select and develop technology controls 12. Deploy control activities through policies and procedures
Information and communication	13. Use relevant, quality information to support the internal control function 14. Communicate internal control information internally 15. Communicate internal control information externally
Monitoring	16. Perform ongoing or periodic evaluations of internal controls (or a combination of the two) 17. Communicate internal control deficiencies

These components form an integrated system that provides information to management to enable proactive responses to changing conditions. Controls are most effective when they are built into the infrastructure and are a part of the fundamental business activities. The control system at AvidXchange is integrated within its operating activities. The control environment sets the tone of the Company influencing control consciousness of all personnel. It is the foundation for all other components of control, providing discipline and structure.

Internal Environment

Through the internal environment, management can influence the way business activities are structured. Objectives are established and risks assessed. They influence control activities, information and communication systems and monitoring processes. AvidXchange's managerial culture instills an enterprise-wide attitude of integrity and control consciousness and sets a positive "tone at the top". Management has established methods that foster shared values and teamwork in pursuit of these objectives.

AvidXchange provides services to highly regulated industries where risk management, control, and reputation are critical. AvidXchange maintains numerous enterprise-wide and division-specific policies and programs to promote an appropriate control environment.

Corporate Structure and Organization

The organizational structure of AvidXchange provides the overall framework for planning, directing and controlling the operations by segregating personnel and business functions into departments according to job responsibilities.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of AvidXchange's control environment, affecting the design, administration and monitoring of other components.

Integrity and ethical behavior are the product of AvidXchange's ethical and behavioral standards, how they are communicated and how they are reinforced in practice.

They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal or unethical acts. They also include the communication of the Company's values and behavioral standards to personnel through policy statements and codes of conduct.

Specific control activities that AvidXchange has implemented in this area are described below:

- Critical organizational and security policies are assigned an owner, reviewed, edited and approved periodically.

- Version control is utilized, and current versions are published and communicated as appropriate.

- All new employees are required to sign an acknowledgement form indicating they have read and understand their responsibilities contained in the employee handbook and confidentiality agreement.

- Hiring practices include screening candidates for qualifications, experience and performing background checks, which includes criminal history and credit checks.

- The governance committee holds weekly management meetings to discuss management activities, operational issues and strategic objectives; and

- Insurance coverage is maintained to protect against dishonest acts that may be committed by AvidXchange personnel.

Board of Directors and Audit Committee Participation

AvidXchange's control consciousness is influenced significantly by its Board of Directors and Audit Committee participation.

Specific control activities that AvidXchange has implemented in this area are described below:

- A Board of Directors oversees management activities and Company operations.

- The governance committee holds weekly management meetings to discuss management activities, operational issues, and strategic objectives.

- An external audit is performed on an annual basis to monitor financial statement reporting practices and management's compliance with the Company's objectives.

- An Audit Committee and internal audit function oversee internal controls, responsibilities relating to registered public accounting firms and complaints received regarding accounting or auditing matters.

Management's Philosophy and Operating Style

AvidXchange's management philosophy and operating style encompasses a broad range of characteristics. Such characteristics include management's approach to handling and monitoring business risks and management's attitudes toward information processing, accounting functions and personnel.

Specific control activities that AvidXchange has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting services provided.
- Management meetings are held on a periodic basis to discuss operational issues; and
- Discussions from these meetings are documented by management in meeting minutes.

Organizational Structure and Assignment of Authority and Responsibility

AvidXchange's organizational structure provides the framework within which its activities for achieving Company-wide objectives are planned, executed, controlled and monitored. AvidXchange's management believes that establishing a relevant organizational structure includes consideration of key areas of authority and responsibility, as well as appropriate lines of reporting. AvidXchange has developed an organizational structure suited to meet its needs. This organizational structure is based, in part, on its size and the nature of its activities.

AvidXchange's assignment of authority and responsibility activities include the establishment of reporting relationships and the establishment of authorization hierarchies. It also includes policies relating to appropriate business practices, knowledge and experience of key personnel, in addition to the resources necessary for carrying out these duties. Furthermore, it includes policies and communications directed at ensuring that all personnel understand the Company's objectives, recognize how their individual actions interrelate and contribute to those objectives, and comprehend that they will be held accountable.

Specific control activities that AvidXchange has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority, responsibility and the appropriate lines of reporting to personnel. These charts are communicated to employees and updated as needed.
- AvidXchange's operating goals and objectives are communicated to the entire Company during periodic staff meetings, employee performance reviews and other written communications; and
- AvidXchange has established segregation of duties, which is based upon role-based job responsibilities.

Human Resource Policies and Practices

AvidXchange's human resource policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation and disciplinary activities.

Specific control activities that AvidXchange has implemented in this area are described below:

- Hiring practices include screening candidates for qualifications, experience and performing background checks, which includes criminal history and credit checks.
- All new employees are required to sign an acknowledgement form indicating they have read and understand their responsibilities contained in the employee handbook.
- Performance reviews are performed for all employees annually.
- Human Resources' personnel use a new hire guide for all new hires, to ensure that specific elements of the hiring process are consistently executed.

Management utilizes a termination workflow to manage employee terminations to ensure consistency within the termination process and ensure timely removal from critical applications.

Training

Training is an important part of management's commitment to excellence. Management provide security awareness training to all new employees and then annually thereafter. Management also encourages employee participation in outside continuing education.

Confidentiality

All employees are required to review and sign AvidXchange's confidentiality agreement prior to gaining access to client data. The agreement provides employees with clear guidelines of the employee's role in protecting client information. Management reviews the confidentiality guidelines at regularly scheduled staff meetings.

Commitment to Competence

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

Specific control activities that AvidXchange has implemented in this area are described below:

- Management has defined job descriptions that clearly indicate job responsibilities and required skills and qualifications; Management encourages ongoing training and development to maintain and enhance the skill levels of its personnel.
- Performance reviews are performed for all employees annually.; and
- Each new employee undergoes an initial training on Company values, mission, and other relevant on-boarding topics.

Risk Assessment

Management is responsible for identifying the risks that threaten the achievement of control objectives stated in management's description of the services and systems. Management has implemented a process for identifying relevant risks. This process includes estimating the significance of identified risks, assessing the likelihood of their occurrence, and deciding about actions to address them. However, because control objectives relate to risks that controls seek to mitigate, management thoughtfully identified control objectives when designing, implementing, and documenting their System.

Objective Setting

AvidXchange establishes objectives in order for management to identify potential events affecting their achievement. AvidXchange has placed into operation a risk assessment process to identify and manage risks that could affect the Company's ability to provide reliable compliance processing for user entities. Objective setting enables management to identify measurement criteria for performance, with focus on success factors.

AvidXchange has established certain broad categories including:

- Changes in operating environment
- Changes in personnel
- New or revamped information systems
- Rapid growth
- New technology
- New business models, products, vertical markets or activities
- Corporate restructurings
- Expanded operations
- New accounting pronouncements

AvidXchange's risk strategy is reflected in policies and procedures designed to avoid, selectively transfer and/or control risk exposures, while providing reasonable assurance that business outcomes are consistent with the Company's goals and risk tolerance. Each AvidXchange business unit designs, implements and manages controls in order to ensure that core business goals will be achieved in a manner consistent with both senior management's and customers' fiduciary expectations.

The controls evaluated in this report have been placed into operation by AvidXchange to ensure the actions of management and staff enhance the likelihood that established objectives will be achieved.

Risk Event Identification

Regardless of whether an objective is stated or implied, a Company's risk-assessment process should consider risks that may occur. It is important that risk identification be comprehensive. AvidXchange has considered significant interactions between itself and relevant third parties and risks that could affect the Company's ability to provide reliable service to its user entities.

Management considers risks that can arise from both external and internal factors including:

External Factors

- Technological developments
- Changing customer needs or expectations
- Competition
- New legislation and regulation
- Natural catastrophes
- Economic changes

Internal Factors

- A disruption in information systems processing
- Quality of personnel hired, and methods of training utilized
- Changes in management responsibilities
- Environmental conditions in the data center
- Acquisition and integration activities
- Types of fraud and fraud opportunities

Risk Assessment/Analysis

AvidXchange's methodology for analyzing risk varies, largely because many risks are difficult to quantify. Nonetheless, the process includes:

- Estimating the significance of the risk
- Assessing the likelihood of the risk occurring
- Considering how the risk should be mitigated

Risk analysis is an essential process to AvidXchange's success. It includes identification of key business processes where potential exposures to some consequences exist. Once the significance and likelihood of the risk have been assessed, management considers how the risk should be mitigated. This involves judgment based on assumptions about the risk and reasonable analysis of costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood of the risk occurring.

As a part of the risk assessment process, AvidXchange performs annual risk assessments to determine the minimum set of controls required to reduce and maintain risk at an acceptable level. Additional evaluations are completed when significant changes occur that potentially cause risk.

Response

AvidXchange has implemented proactive programs, such as impact analysis and integrated operational contingency plans to ensure that effective risk response plans can be implemented and coordinated in a timely and effective manner.

To ensure that activities related to actual risk events are effectively coordinated, each business unit and corporate resource division has developed and implemented event management and escalation processes. Pre-established notification lists and response procedures ensure that subject matter experts, customers and other stakeholders are appropriately involved in problems resolution.

DESCRIPTION OF SERVICES PROVIDED

Products

AvidXchange's product suite (Avid Suite) helps both buyers and suppliers better manage the processes of paying and getting paid.

For buyers, AvidXchange delivers software-as-a-service solutions that increase the efficiency of strategic value of the accounts payable processes. The Avid Suite of solutions is divided into the following categories:

- Procurement Solutions
  - Solutions designed to help customers process and distribute purchase orders to suppliers (Avid Buy, Avid Ariett, etc.)
- AP Automation Solutions
  - Solutions designed to help customers eliminate paper from the invoicing process, automate coding and approvals, and strengthen internal controls (Avid Invoice, Avid Strongroom, Ascend, etc.)
- Payment Solutions
  - Solutions designed to help customers eliminate paper checks through full-service payment outsourcing and spend optimization (Avid Pay Network)
  - Software tools designed to help customers self-manage payment execution by augmenting the capabilities of the customer's accounting system (Create-a-Check, Avid-for-Netsuite, etc.)
- Utility Solutions
  - Solutions designed to help customers analyze consumption data and manage the complexities associated with the utility bill payment process (Avid Utility)

For suppliers, AvidXchange offers solutions to enhance visibility, control cash flow, and streamline key elements of the accounts receivable (AR) process.

- Supplier Financing Solutions
  - Services designed to help suppliers better control their cash flow by accelerating payment upon request (Invoice Accelerator, powered by Avid Cashflow Manager)

Services

AvidXchange provides comprehensive services to meet diverse needs. These services include acclimating clients to the new processes offered by these products, training them to effectively use and manage the applications and assisting them in realizing the full value of their technology investments over time.

- Scanning Services
  - Provides clients with outsourced scanning of paper accounts payable documents in addition to the ability to receive electronic invoices, data files and images directly into the inbox of the AvidXchange Network
- Indexing Services
  - Uses a combination of technology and human quality assurance processes to provide clients with the means to outsource the manual data entry of invoice header information
- E-Payment Conversion Services
  - Services designed to help buyers convert suppliers away from checks towards more favorable (to both the buyer and the supplier) e-Payment options
- AP Payment Services (Buyers)
  - Services designed to help buyers reduce labor costs associated with payment aging, escheatment, managing supplier payment inquiries, communication of remittance advice, etc.
- AR Payment Services (Suppliers)
  - Services designed to help suppliers accurately and efficiently receive funds and apply payments within the AR modules of their accounting system.
- Onboarding Services
  - The AvidXchange Services Group applies technology and industry-best practices to help clients adapt to new processes made possible by AvidXchange applications
- Support Services
  - The Support Team within the Services Group ensures that the clients' applications are performing optimally and are available to provide end-user technical assistance

Information Technology and Systems Security

AvidXchange provides technological solutions to its clients and understands the critical and sensitive nature of maintenance operations. Physical access to computer equipment and storage media is restricted to properly authorized individuals. Current technology is employed to ensure that data is secure and that appropriate access to information is given only to authorized users. The AvidXchange information technology team is responsible for implementing all hardware and software changes. Procedures are in place to review, approve, and properly implement all infrastructure changes.

Description of AvidXchange, Inc.'s Information Technology (IT) Team

The Chief Information Officer (CIO) is responsible for all technology strategy, including infrastructure strategy, cloud operations, quality and service delivery. The CIO, with the assistance of the team managers and staff, assesses the needs of each client and user to plan the proper hardware and software necessary for each area to efficiently complete required duties. Resources are planned, allocated and implemented as needed. The CIO has the primary responsibility for implementing the plans.

Description of Computerized Information Systems

AvidXchange Pay Application, AvidXchange Invoice Application, AvidXchange Utility, Cashflow Manager and API Toolkit are custom-developed applications delivered via a Software-as-a-Service (SaaS) model.

AvidXchange's SaaS model is based on Microsoft Windows Servers (Web and .net application) and Microsoft SQL Server databases.

AvidXchange's solution stack utilizes network load balancing and is protected by a firewall that utilizes Intrusion Detection Services (IDS).

Changes to Control Environment During the Audit Period

AvidXchange continues to leverage Microsoft's Azure Cloud environment for scalability of lower and production environments as well as for specialized data center operations and disaster recovery capabilities.

Control Objectives and Related Control Activities

Selection and Development of Control Activities

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

The Company's control objectives and related control activities are included in Section IV of this report and have been removed from the description to eliminate redundancy. The control objectives listed in Section IV are, nevertheless, an integral part of the Company's description of controls.

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

Integration with Risk Assessment

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

Information and Communication

Information is identified, captured, processed and reported by information systems. Employees receive the information that they need on a timely basis in order to be able to do their jobs. Relevant information includes applicable external sources, such as economic and regulatory information, as well as internally generated information.

Communication is defined, in a broad sense, by the expectations and responsibilities of individuals and groups. AvidXchange expects employees to be truthful in all of their communications, including those with customers, management and other Company personnel. Misrepresentations, including omissions of important facts, are unacceptable. The accuracy of employee, customer and other business records is critical to the quality of service that AvidXchange is able to offer to its customers. Employees are required to adhere to AvidXchange's policies and procedures that are designed to ensure that all corporate records and other documents are maintained accurately and completely.

To help align AvidXchange's business strategies and goals with operating performance and controls, the Company has implemented various methods of communication to ensure that all employees understand their individual roles and responsibilities and to ensure that all significant events are communicated in a timely manner. These methods include orientation and training programs for newly hired employees, regular management meetings for updates on business performance and other matters and the use of electronic mail messages to communicate time-sensitive information as well as the Company's intranet for maintaining Company-wide documents and policies.

Every employee has a written job description, and every job description includes the responsibility to communicate significant issues and exceptions to an appropriate higher level of authority within the Company in a timely manner.

AvidXchange has also implemented various methods of communication with customers. These methods ensure that the customers understand the role and responsibilities of AvidXchange in providing its services, and they ensure that significant events are communicated to customers in a timely manner.

One of these methods is a web portal, which employs a secure interface for the customer to access information, project plans, and statistics on their environment as well as notification regarding any facility-wide changes or scheduled outage events. Customers also rely on the portal to place support cases for infrastructure or engineering concerns. Customers also are encouraged to communicate any questions and problems, which are logged and tracked until resolved, to AvidXchange support personnel.

Monitoring

Monitoring requires the following:

- A clear understanding of processes and their relationships to key risks
- Progress towards addressing highest rated risks
- On-going risk exposure and effectiveness of managing the risk

Management monitors controls to consider whether they are operating as intended and are modified appropriately for changes in conditions. AvidXchange management performs monitoring activities to continually assess the quality of internal controls over time. Activities are monitored on a continuous basis and necessary corrective actions are taken as required to correct deviations from Company policy and procedures. This process is accomplished through on-going monitoring activities, separate evaluations, or a combination of the two.

The AvidXchange management team conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through firm meetings, department meetings, client conference calls, and informal notifications.

Management's close involvement in the operations can identify significant variances from expectations regarding internal controls. Upper management immediately evaluates the specific facts and circumstances with any suspected control breakdowns. A decision for addressing any control weakness is made based on whether the incident was isolated or requires a change in the Company's procedures or personnel.

The goal of this process is to ensure legal and regulatory compliance and to maximize the performance of AvidXchange personnel.

Reporting Deficiencies

Deficiencies in management's internal control system surface from many sources, including the Company's on-going monitoring procedures, separate evaluations of the internal control system, and external parties. Management has developed protocols to help ensure that findings of internal control deficiencies are reported not only to the individual responsible for the function or activity involved, who is in position to take corrective action, but to at least one level of management above the directly responsible person.

This process enables that individual to provide needed support or oversight for taking corrective action and to communicate with others in the Company that may be affected.

Management evaluates the specific facts and circumstances related to deficiencies in internal control procedures. Management then makes decisions for addressing deficiencies based on whether the incident was isolated or requires a change in the Company's procedures or personnel.

Monitoring of Subservice Organizations

AvidXchange uses the services of external organizations to perform certain functions in delivering the System services (all hereinafter collectively referred to as the "carved-out subservice organizations"). The functions performed by these organizations include:

- Data center services
- Disaster recovery services
- Check and e-Payment processing
- Monetary transactions and banking services

This description includes only those controls and related control objectives at AvidXchange and does not include controls and related control objectives of the carved-out subservice organizations.

Complementary Controls at User Entities

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

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

Complementary Control	Control Objective
1. Notification is provided to AvidXchange of any issues identified with the application.	Objective 5.1, 6.1, 6.2, 6.3, 6.4
2. Physical and logical access to systems sending data to and receiving data from AvidXchange should be restricted to authorized personnel. Periodic reviews of authorized personnel should be performed.	Objective 3.1
3. Client-assigned user IDs within the application are properly defined and kept confidential and accurate. Client-assigned generic user IDs are identified and disabled, where required.	Objective 3.1
4. Client-defined password settings for client applications are properly and securely configured. Passwords are changed on a periodic basis and user IDs are updated for personnel changes.	Objective 3.1
5. Client new user and modified user access to client applications are approved by authorized personnel before the access is implemented. Roles and features are granted according to job requirements and frequently reviewed by the client for appropriateness.	Objective 3.1
6. Terminated client users are removed from the application timely.	Objective 3.5
7. Administrative privileges are restricted within the applications to authorized personnel.	Objective 3.5
8. Client is required to immediately notify AvidXchange of any actual or suspected information security breaches, including compromised user accounts related to the application.	Objective 3.4, 5.1
9. Approval workflows within the application are accurately maintained and monitored by the client on a regular basis.	Objective 6.2, 6.3
10. The client's legacy information (general ledger, vendor information, etc.) is reviewed and approved for accuracy.	Objective 6.1
11. Clients are responsible for approving all invoices to be paid, approving specified payments meeting clients' business rules, for reconciling banks statements for checks processed and for managing the relationships with vendors for payments made.	Objective 6.3, 6.4
12. Authorized client personnel should be properly trained on AvidXchange applications and processes as they relate to their job functions.	Objective 6.1, 6.2, 6.3, 6.4
13. New client accounts and installations should be reviewed for accuracy. Unusual items noted should be reported to AvidXchange immediately.	Objective 4.1, 6.1, 6.2, 6.3, 6.4

Complementary Control	Control Objective
14. Data transmitted to and received from AvidXchange, as well as reports received, should be compared or reconciled to the source data to determine whether the data transmissions and other transaction processing are complete and accurate. Data sent to AvidXchange should be encrypted.	Objective 3.5, 6.1, 6.2, 6.3, 6.4
15. Processing activity conducted within AvidXchange applications should be reviewed in a timely manner to determine that transactions were completely and accurately processed where authorized.	Objective 6.1, 6.2, 6.3, 6.4
16. Bank accounts through which AvidXchange executes transactions should be reconciled on a timely basis and compared to transaction detail; unusual transactions should be reported to AvidXchange for investigation, as necessary, as soon as identified.	Objective 6.1, 6.2, 6.3, 6.4

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

SECTION IV – INFORMATION PROVIDED BY THE INDEPENDENT AUDITOR

Control Objectives, Related Controls and Tests of Operating Effectiveness

Control Objective 1 – Control Environment

	Controls Specified by Management	Testing Performed by ParsonsCPA	Test Results
Objective 1.1 – Control activities provide reasonable assurance that policies and procedures are in place to ensure effective communication and oversight of key organizational and information security practices.			
1.1.1	Critical organizational and security policies are assigned an owner, reviewed, edited, and approved periodically. Version control is utilized, and current versions are published and communicated as appropriate.	Inspected the Information Security Policy to determine that critical organizational and security policies are assigned an owner, reviewed, edited, and approved periodically.	No exceptions noted.
1.1.2	All new employees are required to sign an acknowledgment form indicating they have read and understand their responsibilities contained in the employee handbook.	For a selected sample of new hires, inspected the employee handbook acknowledgments to determine that employees signed a statement confirming acknowledgment of all policies and procedures in the employee handbook.	No exceptions noted.
1.1.3	Hiring practices include screening candidates for qualifications, experience, and performing background checks, which includes criminal history and credit checks.	For a selected sample of new hires, inspected the background screening reports to determine that during the hiring process, a background check was performed on potential employees before they began employment with the Company.	No exceptions noted.

Control Objective 1 – Control Environment (Continued)

	Controls Specified by Management	Testing Performed by ParsonsCPA	Test Results
1.1.4	Management utilizes a termination workflow to manage employee terminations to ensure consistency within the termination process and ensure timely removal from critical applications.	For a selected sample of terminated users, inspected the application access removal tickets to determine that management utilized termination workflows to manage employee terminations to ensure consistency within the termination process and ensure timely removal from critical applications.	No exceptions noted.
1.1.5	Formal security awareness training takes place upon hire and annually thereafter for employees responsible for designing, developing, implementing, operating, monitoring, and maintaining the system.	For a selected sample of new hires and active employees, inspected the training compliance logs to determine that staff were given Security Awareness training during their new hire orientation and then updated on an annual basis.	No exceptions noted.

Control Objective 1 – Control Environment (Continued)

	Controls Specified by Management	Testing Performed by ParsonsCPA	Test Results
Objective 1.2 – Control activities that provide reasonable assurance that discipline and structure are an integral part of the Company and influence the control consciousness of its personnel.			
1.2.1	Organizational charts are in place to communicate key areas of authority, responsibility, and the appropriate lines of reporting to personnel. These charts are communicated to employees and updated as needed.	Inspected the organizational chart to determine that documentation was in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.	No exceptions noted.
1.2.2	Management has defined job descriptions that clearly indicate job responsibilities and required skills and qualifications.	Inspected the job descriptions to determine they were in place and described the roles and responsibilities of the position.	No exceptions noted.
1.2.3	Performance reviews are performed for all employees annually.	For a selected sample of employees, inspected the performance review log to determine that employee evaluations were performed on an annual basis.	No exceptions noted.
1.2.4	Management has formal processes in place to apply corrective action plans for employees with escalation process leading to termination.	Inspected the corrective process communications and the employee handbook to determine that management has formal processes in place to apply corrective action plans for employees with escalation process leading to termination.	No exceptions noted.

Control Objective 1 – Control Environment (Continued)

	Controls Specified by Management	Testing Performed by ParsonsCPA	Test Results
1.2.5	Management has adopted a comprehensive risk management strategy, to identify and consider threats and risks and formally addressing risk in a proactive fashion. Entity wide risk assessment is updated at least annually.	Inspected the Enterprise Risk Management Charter and the Risk Steering Committee meeting agenda to determine that the Company had a comprehensive risk management program to address risks in a proactive fashion and updated annually.	No exceptions noted.
Objective 1.3 – Control activities provide reasonable assurance that appropriate corporate governance measures are in place to ensure effective governance and oversight of Company operations.			
1.3.1	The governance committee holds weekly management meetings to discuss management activities, operational issues, and strategic objectives.	Inspected the meeting agendas for a selected sample of weeks to determine that the governance committee held weekly management meetings to discuss management activities, operational issues, and strategic objectives.	No exceptions noted.
1.3.2	An external audit is performed on an annual basis to monitor financial statement reporting practices and management's compliance with the Company's objectives.	Inspected the most recent external audit report to determine that an external audit was performed on an annual basis to monitor financial statement reporting practices and management's compliance with the Company's objectives.	No exceptions noted.
1.3.3	An Audit Committee oversees internal controls, responsibilities relating to registered public accounting firms, and complaints received regarding accounting or auditing matters.	Inspected the Audit Committee charter to determine that an Audit Committee oversees internal controls, responsibilities relating to registered public accounting firms, and complaints received regarding accounting or auditing matters.	No exceptions noted.

Control Objective 1 – Control Environment (Continued)

	Controls Specified by Management	Testing Performed by ParsonsCPA	Test Results
Objective 1.4 – Control activities provide reasonable assurance that third-party providers meet or exceed Service Level Agreements.			
1.4.1	Management maintains a Third-Party Security Policy and performs a risk assessment on third-party vendors each calendar year, including a review of service level agreements and SOC reports, where applicable, from third-party vendors and subservice providers.	Inspected the Third-Party Security Policy, the risk assessments for a selected sample of vendors, and conducted a corroborative inquiry of management to determine that management maintains a Vendor Risk Management Policy and performed a risk assessment on third-party vendors each calendar year, including a review of service level agreements and SOC reports, where applicable.	No exceptions noted.

Control Objective 2 – Physical Security and Environmental Controls

	Controls Specified by Management	Testing Performed by ParsonsCPA	Test Results
Objective 2.1 – Control activities provide reasonable assurance that business premises and critical infrastructure are protected from unauthorized access, damage, and interference.			
2.1.1	Facility entry access requires a badge to ensure access is authorized based on job function, recorded, and appropriately monitored.	Observed and inspected via virtual walk-through procedures the access management procedures, the access management system, and the access logs to determine that access to the facility requires a badge and badge access is recorded and monitored.	No exceptions noted.
2.1.2	Physical access to building and computing infrastructure rooms and locations are restricted to authorized personnel.	Inspected the access management system and observed via virtual walk-through procedures the server room access procedures to determine that access is restricted to authorized personnel.	No exceptions noted.
2.1.3	Visitors are escorted at all times within sensitive areas and access is logged. Logs are appropriately maintained.	During virtual onsite procedures, observed the front desk security and inspected the visitor log repository to determine that visitors were escorted at all times and visitor logs were appropriately maintained.	No exceptions noted.
2.1.4	Terminated employees' or contractors' access to facilities, application systems, and physical assets is removed in a timely manner.	For a selected sample of terminated users, inspected the access control profiles to determine that the access control system terminations were properly documented and conducted timely.	No exceptions noted.

Control Objective 2 – Physical Security and Environmental Controls (Continued)

	Controls Specified by Management	Testing Performed by ParsonsCPA	Test Results
2.1.5	Policies, standards, and procedures for restricting visitor physical access are documented, in use, and known to all affected parties.	Inspected the Visitor Access Program to determine that the Company had policies and procedures governing visitor physical security controls that limit access to the facility to authorized individuals.	No exceptions noted.
2.1.6	Media containing sensitive information is physically secured and at all times.	Observed via virtual walk-through procedures the server room access procedures to determine that access to the server room was restricted at all times.	No exceptions noted.
2.1.7	Video cameras are deployed at sensitive entry points to provide real-time monitoring and periodic forensic review.	Observed via virtual walk-through procedures the use of security cameras and inspected the video footage repository to determine that real-time monitoring was in place and forensic review was available.	No exceptions noted.

Control Objective 2 – Physical Security and Environmental Controls (Continued)

	Controls Specified by Management	Testing Performed by ParsonsCPA	Test Results
Objective 2.2 – Control activities provide reasonable assurance that physical computing assets are appropriately protected from damage or destruction.			
2.2.1	Fire detection and suppression mechanisms are appropriately maintained to ensure operation if called upon to operate.	Observed via virtual walk-through procedures the fire suppression system testing tags to determine that systems were appropriately maintained.	No exceptions noted.
2.2.2	An uninterruptible power supply (UPS) system is maintained and periodically tested to ensure a controlled shut down in the event of a prolonged power outage.	Observed the UPS system during onsite procedures and inspected the UPS test results to determine that tests and inspections were performed on a periodic basis to ensure proper operation.	No exceptions noted.

Control Objective 3 – Logical Security

	Controls Specified by Management	Testing Performed by ParsonsCPA	Test Results
Objective 3.1 – Control activities provide reasonable assurance that networks, network devices, and network users are appropriately configured to protect against unauthorized or unintentional use, modification, addition, or deletion.			
3.1.1	Logical separation exists between AvidXchange networks, devices, user and networks which support customer processing to ensure processing and access integrity.	Inspected the network diagram and the network configuration to determine that logical separation exists between Avid networks, devices, user, and networks.	No exceptions noted.
3.1.2	A formal Security Incident Response Standard is reviewed at least annually to ensure that escalation, handling, root cause, remediation, and resolution processes are adhered to and remain relevant.	Inspected the Security and Privacy Incident Response Plan to determine that the Security Incident Response Standard was reviewed at least annually to ensure that escalation, handling, root cause, remediation, and resolution processes were adhered to and remained relevant.	No exceptions noted.
3.1.3	A third-party penetration test is performed annually to identify potential security gaps. Issues are prioritized and remediated in a timely manner.	Inspected the penetration testing reports to determine that third-party penetration tests were performed annually to identify potential security gaps.	No exceptions noted.
3.1.4	The data that enters the AvidXchange environment is secured and monitored through the use of properly configured firewalls.	Inspected the firewall ruleset configurations and conducted a corroborative inquiry of management to determine that a firewall was in place and configured to eliminate known attack vectors.	No exceptions noted.

Control Objective 3 – Logical Security (Continued)

	Controls Specified by Management	Testing Performed by ParsonsCPA	Test Results
3.1.5	Network users are authenticated via individually assigned and unique user accounts and passwords.	Inspected the access role listing to determine that network users were issued a unique ID which restricts access to resources pursuant to their job functions.	No exceptions noted.
3.1.6	The AvidXchange network is configured based on documented policy to enforce password requirements for: • Password history (4) • Maximum age (90 days for users, 30 days for administration) • Forced change upon first log-in • Minimum length (8 for users, 16 for administration) • Complexity requirements (1 upper case, 1 lower case, 1 digit, 1 special) • Account lock-out after 6 failed attempts	Inspected the network password configurations and conducted a corroborative inquiry of management to determine that network passwords were configured to enforce the requirements.	No exceptions noted.
Objective 3.2 – Control activities provide reasonable assurance that technology infrastructure is monitored for internal and external threats to ensure availability.			
3.2.1	An intrusion prevention system (IPS) is utilized to analyze network events and report possible or actual network security breaches through automated alerts.	Inspected threat prevention configurations, monitoring dashboards, alert log, and conducted a corroborative inquiry of management to determine that an IPS was in place, monitoring the network continuously, and logged alerts for administrators.	No exceptions noted.

Control Objective 3 – Logical Security (Continued)

	Controls Specified by Management	Testing Performed by ParsonsCPA	Test Results
Objective 3.3 – Control activities provide reasonable assurance that security software, tools and processes are appropriately maintained to ensure infrastructure and applications are protected.			
3.3.1	System patches and/or updates are reviewed, tested, and implemented in a timely manner.	Inspected the patch compliance tracker and the patching tickets to determine that a patch management process was in place.	No exceptions noted.
3.3.2	New devices are deployed with the approved system image/configuration.	Inspected the configuration standards, the configuration procedures, and conducted a corroborative inquiry of management to determine that devices were deployed with the approved system image/configuration.	No exceptions noted.
3.3.3	IT Security personnel respond appropriately and in a timely manner to events which trigger an alert through monitoring software or other avenues.	Inspected the monitoring dashboards, the security event logs, and conducted a corroborative inquiry of management to determine that monitoring tools were configured to log alerts when certain events occurred.	No exceptions noted.
3.3.4	Vulnerability scanning occurs weekly. Critical and high-risk vulnerabilities are logged and resolved in a timely manner.	Inspected the vulnerability scan reports to determine that vulnerability scanning occurs weekly.	No exceptions noted.

Control Objective 3 – Logical Security (Continued)

	Controls Specified by Management	Testing Performed by ParsonsCPA	Test Results
Objective 3.4 – Control activities provide reasonable assurance that users are appropriately restricted to protect against unauthorized or unintentional use, modification, addition, or deletion of data.			
3.4.1	Domain administrative access is restricted to authorized personnel through a privileged access management technology.	Inspected the administrator listings, the administrative access review, and conducted a corroborative inquiry of management to determine that network administrator rights were restricted to certain authorized personnel as described.	No exceptions noted.
3.4.2	Domain administrator access is reviewed periodically to ensure appropriateness and authorization.	Inspected the administrator review documentation and conducted a corroborative inquiry of management to determine that domain administrator access was periodically reviewed to ensure access is commensurate with job responsibilities.	No exceptions noted.
3.4.3	Sensitive websites are protected via TLS encryption with a trusted certificate authority.	Inspected the encryption certificates and conducted a corroborative inquiry of management to determine that the server was being utilized as described.	No exceptions noted.
3.4.4	Multi-factor authentication is applied to privileged and remote access.	Inspected the privileged and remote access authentication configurations and conducted inquiry of management to determine that remote access to that privileged and remote access requires multi-factor authentication.	No exceptions noted.

Control Objective 4 – Application Implementation and Change Management

	Controls Specified by Management	Testing Performed by ParsonsCPA	Test Results
Objective 4.1 – Control activities provide reasonable assurance that changes to production programs are properly authorized, tested, approved, implemented, and documented.			
4.1.1	An approved business requirements document is maintained by customer solutions group as Agile Stories to communicate strategy and high-level requirements for system enhancements.	Inspected the Change Management Policy and Procedures and conducted a corroborative inquiry of management to determine that an approved business requirements document is in place to communicate strategy and high-level requirements for system enhancements.	No exceptions noted.
4.1.2	The application change management process is documented and periodically reviewed for relevance and accuracy.	Inspected the IT Change Management Policy to determine that the application development process is documented and periodically reviewed for quality improvement.	No exceptions noted.
4.1.3	Dev, Test, QA, and production environments are logically separated.	Inspected the network diagram, the change pipeline stages, and conducted a corroborative inquiry of management to determine the environments were logically separated.	No exceptions noted.
4.1.4	Code changes in production are reviewed and approved through a multi-level process where the developers cannot approve their own code.	For a selected sample of changes, inspected the change documentation and conducted a corroborative inquiry of management to determine that all code changes in production are reviewed and approved through a multi-level process where the developers cannot approve their own code.	No exceptions noted.

Control Objective 4 – Application Implementation and Change Management (Continued)

	Controls Specified by Management	Testing Performed by ParsonsCPA	Test Results
4.1.5	All code changes to the production environment undergo static code analysis to ensure proper secure coding methodologies.	For a selected sample of changes, inspected the change testing documentation and conducted a corroborative inquiry of management to determine to determine that code changes to the production environment underwent static code analysis to ensure proper secure coding methodologies.	No exceptions noted.
4.1.6	Changes to the production environment are appropriately authorized and approved. Changes to production with the appropriate authorization and approvals are tracked in one system of record.	For a selected sample of changes, inspected the change documentation and conducted a corroborative inquiry of management to determine that all changes to the production environment are appropriately authorized and approved.	No exceptions noted.
4.1.7	Change access to production code resources is appropriately restricted.	Inspected the access listing and conducted a corroborative inquiry of management to determine that management restricted the ability to move code into the production environment to specific personnel.	No exceptions noted.
4.1.8	Back-out procedures are documented within each change implementation to allow for rollback of changes when changes impair system operation.	For a selected sample of changes, inspected the documented Back-Out Plan and conducted a corroborative inquiry of management to determine that back-out procedures were documented within each change implementation to allow for rollback of changes when changes impair system operation.	No exceptions noted.

Control Objective 5 – Computer Operations

	Controls Specified by Management	Testing Performed by ParsonsCPA	Test Results
Objective 5.1 – Control activities provide reasonable assurance that infrastructure components are available and performing optimally to ensure customer satisfaction measurements are met.			
5.1.1	Production infrastructure performance and availability thresholds are defined and configured in the enterprise production monitoring application.	Inspected the monitoring application configuration to determine that the organization utilized monitoring applications to measure production systems performance and availability.	No exceptions noted.
5.1.2	System alerts are generated when performance and availability thresholds are exceeded to ensure timely resolution of problems that could negatively impact customer satisfaction.	Inspected the monitoring application alerting configurations to determine that sufficient notification takes place when predefined thresholds are exceeded.	No exceptions noted.

Control Objective 5 – Computer Operations (Continued)

	Controls Specified by Management	Testing Performed by ParsonsCPA	Test Results
Objective 5.2 – Control activities provide reasonable assurance that critical operating data is appropriately backed-up to ensure timely restoration in the event of system failure or inaccessibility.			
5.2.1	The automated back-up system generates an alert upon failure. Failed back-up jobs are re-run through to completion in a timely manner.	Inspected the back-up reports and conducted a corroborative inquiry of management to determine that that the back-up process is monitored to ensure failures are re-run through to completion in a timely manner.	No exceptions noted.
5.2.2	Database capacity, integrity and performance is monitored at all times to ensure complete, accurate, and timely storage of data and delivery of services.	Inspected the monitoring application and example alert e-mails and conducted a corroborative inquiry of management to determine that database capacity, integrity, and performance was monitored and alerted against when pre-defined thresholds were surpassed.	No exceptions noted.
Objective 5.3 – Control activities provide reasonable assurance that critical nonterminal oriented tasks are scheduled and monitored. Failed jobs are identified and run through to completion in a timely manner.			
5.3.1	Critical data is stored in encrypted format consistent with the AvidXchange data protection standard using AES-256-bit keys with 2048 key length.	Inspected the encryption configuration and conducted inquiry of management to determine that restricted production data is encrypted in transit and at rest.	No exceptions noted.

Control Objective 6 – Controls Over Customer Financial Reporting

	Controls Specified by Management	Testing Performed by ParsonsCPA	Test Results
Objective 6.1 – Control activities provide reasonable assurance that the legacy information (General Ledger, Vendor Information) is accurately reflected in the software records.			
6.1.1	Implementation meetings are held at defined stages of the customer onboarding process to ensure all requirements are met and all necessary system interfaces are configured and tested prior to "Go Live". Customer acknowledgement of their acceptance is required prior to activation.	For a selected sample of new customers, inspected the Scoping and Communication Agreements, the Implementation Forms, and the documented customer approval prior to activation to determine that procedures ensured all requirements were met, all necessary system interfaces were configured and tested prior to "Go Live", and that customer acknowledgment of their acceptance was required prior to activation.	No exceptions noted.
Objective 6.2 – Control activities that provide reasonable assurance regarding the accuracy of processing of accounts payable documents (paper invoices, statements, and credit memos) received from vendors on behalf of clients and procedures in place to monitor performance and quality standards appropriately identify exception(s) to any such document.			
6.2.1	The Company maintains standard Service Level Agreements with all customers. These establish mutually agreed-upon processing expectations concerning timeliness of processing and other critical functions.	Inspected the standard Service Level Agreement to determine that it establishes mutually agreed-upon processing expectations concerning timeliness of processing and other critical functions.	No exceptions noted.
6.2.2	Policies and procedures are in place for invoice and payment exception handling.	Inspected the procedural documentation to determine that policies and procedures are in place for invoice and payment exception handling.	No exceptions noted.

Control Objective 6 – Controls Over Customer Financial Reporting (Continued)

	Controls Specified by Management	Testing Performed by ParsonsCPA	Test Results
6.2.3	All bank account changes requested from the vendor network require a signed Docusign agreement and is independently verified by the supplier management team prior to making the change in the system.	For a selected sample of bank account changes, inspected the signed Docusign agreements to determine that all bank account changes requested from the vendor network required a signed Docusign agreement.	No exceptions noted.
Objective 6.3 – Control activities provide reasonable assurance that the software accurately records valid data completely and ensures proper accounting treatment and inclusion in the proper period. Control activities that provide reasonable assurance the Company's transactions are properly reviewed and analyzed, and a historical record is maintained of all changes to the Company's data file.			
6.3.1	Every purchase order and accounts payable transaction is assigned an approval workflow based on the business rules of the client. Only those users who have approval responsibility for the current workflow step can approve that step.	Inspected the workflow access configuration to determine that purchase order and accounts payable transactions are assigned an approval workflow and only those users who have approval responsibility for the current workflow step can approve that step.	No exceptions noted.
6.3.2	Each critical edit, action, transaction event, and workflow create an audit trail. A full, reportable audit trail, recording all critical actions by user, date, and time is captured. The event log cannot be edited.	Inspected the application workflow, the audit logic, and conducted a corroborative inquiry of management to determine that a full, reportable audit trail, recording all critical actions by user, date, and time is captured.	No exceptions noted.

Control Objective 6 – Controls Over Customer Financial Reporting (Continued)

	Controls Specified by Management	Testing Performed by ParsonsCPA	Test Results
Objective 6.4 – Control activities that provide reasonable assurance regarding the accuracy of processing payments on behalf of clients and procedures in place to monitor performance and quality standards appropriately to any such payment.			
6.4.1	All payments processed through the Avid Pay network are verified to ensure they have been processed and accepted by the vendor.	Inspected the Treasury Supplier Sync Agendas for a selected sample of months to determine that all payments are verified to ensure they have been processed and accepted by the vendor.	No exceptions noted.
6.4.2	A daily reconciliation is performed to ensure payments and funding are processed and recorded correctly.	For a selected sample of days, inspected the reconciliation documentation to determine that a reconciliation was performed daily to ensure payments and funding were processed and recorded correctly.	No exceptions noted.