plante moran | Audit. Tax. Consulting. Wealth Management.

CU*Answers, Inc.

SOC 1 Type 2 Report

Report on the CU*BASE Application Processing and Managed Hosting Services System throughout the period October 1, 2022 to September 30, 2023

Contents

Plante & Moran, PLLC
Suite 400
1000 Oakbrook Drive
Ann Arbor, MI 48104
Tel: 734.665.9494
Fax: 734.665.0664
plantemoran.com

Independent Service Auditor's Report

To Management
CU*Answers, Inc.

Scope

We have examined CU*Answers, Inc.'s (CU*Answers) description of its information technology general control system titled "CU*Answers, Inc.'s Description of its CU*BASE Application Processing and Managed Hosting Services System" throughout the period October 1, 2022 to September 30, 2023 (the "description") and the suitability of the design and operating effectiveness of CU*Answers' controls included in the description to achieve the related control objectives stated in the description based on the criteria identified in "CU*Answers, Inc. Management's Assertion" (the "assertion"). The controls and control objectives included in the description are those that management of CU*Answers believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the information technology general control system for the CU*BASE Application Processing and Managed Hosting Services System that are not likely to be relevant to user entities' internal control over financial reporting.

The information included in Section 5, "Other Information Provided by Management of CU*Answers, Inc.," is presented by management of CU*Answers to provide additional information and is not a part of CU*Answers' description of its information technology general control system for the CU*BASE Application Processing and Managed Hosting Services System made available to user entities during the period October 1, 2022 to September 30, 2023. Information about CU*Answers' management response to deviations has not been subjected to the procedures applied in the examination of the description of the information technology general control system for the CU*BASE Application Processing and Managed Hosting Services System and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the information technology general control system for the CU*BASE Application Processing and Managed Hosting Services System, and, accordingly, we express no opinion on it.

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

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

Service Organization's Responsibilities

In Section 2 of this report, CU*Answers' management 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. CU*Answers' management is responsible for preparing the description and the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; selecting the criteria 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.

PRAXITY
Empowering Business Globally

To Management
CU*Answers, Inc.

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 October 1, 2022 to September 30, 2023. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Performing procedures to obtain evidence about the fairness of the presentation of the description and 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 and 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

Service Auditor's Independence and Quality Control

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

Inherent Limitations

Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in its information technology general control system. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design and operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section 4 of this report. The scope of our engagement did not include tests to determine whether controls not listed in Section 4 were achieved; accordingly, we express no opinion on the achievement of controls not included in Section 4.

Opinion

In our opinion, in all material respects, based on the criteria described in CU*Answers management's assertion:

- The description fairly presents the information technology general control system for the CU*BASE Application Processing and Managed Hosting Services System that was designed and implemented throughout the period October 1, 2022 to September 30, 2023.

- 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, 2022 to September 30, 2023 and the subservice organizations and user entities applied the complementary controls assumed in the design of CU*Answers' controls throughout the period October 1, 2022 to September 30, 2023.

To Management
CU*Answers, Inc.

- The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2022 to September 30, 2023 if complementary subservice organization and user entity controls assumed in the design of CU*Answers' controls operated effectively throughout the period October 1, 2022 to September 30, 2023.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4 of this report, is intended solely for the information and use of management of CU*Answers; user entities of the information technology general control system for the CU*BASE Application Processing and Managed Hosting Services System throughout the period October 1, 2022 to September 30, 2023; 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 risk of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than those specified parties.

Plante & Moran, PLLC

May 10, 2024

May 10, 2024

Plante & Moran, PLLC

To Service Auditors:

We have prepared the description of CU*Answers, Inc.'s (CU*Answers) information technology general control system entitled, "CU*Answers, Inc.'s Description of its CU*BASE Application Processing and Managed Hosting Services System" throughout the period October 1, 2022 to September 30, 2023 (description), 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 subservice organizations and user entities of the system themselves when assessing the risks of material misstatement of user entities' financial statements.

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

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

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

a. The description fairly presents the information technology general control system made available to user entities of the system for user entities of the system during some or all of the period October 1, 2022 to September 30, 2023 as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

   i. Presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable
      1) the types of services provided, including as appropriate, the classes of transactions processed; the types of services provided;
      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 reports and other information prepared for user entities of the system;
      3) how the system captures and addresses significant events and conditions other than transactions;
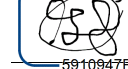   4) the process used to prepare reports and other information for user entities;

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

6) the specified control objectives and controls designed to achieve those objectives including as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls, and control objectives that are specified by law, regulation, or another party; and

7) 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 to user entities of the system.

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

iii. does not omit or distort information relevant to the 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 information technology general control system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period October 1, 2022 to September 30, 2023 to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of CU*Answers' controls throughout the period October 1, 2022 to September 30, 2023. The criteria we used in making this assertion were that:

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

Very truly yours,

Geoff Johnson, Chief Executive Officer

Section 3. CU*Answers, Inc.'s Description of its CU*BASE Application Processing and Managed Hosting Services System

A. Company Overview

CU*Answers, Inc. is incorporated under Michigan law and chartered as a Credit Union Service Organization (CUSO), and as a cooperative. Formerly known as West Michigan Computer CO-OP, Inc. (WESCO), CU*Answers has been providing core and peripheral data processing services to its client credit unions since 1970. CU*Answers is currently owned by more than 150 credit unions. Each credit union owns an identical block of 200 shares and receives one vote. There are no other ownership rights in the cooperative. All credit union owners have the right to be represented by its top professional managing executive as a member of CU*Answers' Board of Directors. There are seven seats on CU*Answers' Board of Directors and members are elected to serve three-year terms.

CU*Answers' business model is as a cooperative, and CU*Answers operates its business based on the Seven Cooperative Principles:

Principle 1: Voluntary and Open Membership - CU*Answers is open to all entities able to use CU*Answers' services and willing to accept the responsibilities of membership.

Principle 2: Democratic Member Control - CU*Answers has democratic member control. Members actively participate in setting policies and making decisions. Elected representatives are accountable to the membership. Members have equal voting rights (one member, one vote).

Principle 3: Member Economic Participation - CU*Answers is an enterprise in which members contribute equitably to, and democratically control, the capital of their co-operative.

Principle 4: Autonomy and Independence - CU*Answers is an autonomous, self-help organization controlled by members. Agreements with other organizations, including governments, are done on terms that ensure democratic control by their members and maintain their co-operative autonomy.

Principle 5: Education, Training, and Information - CU*Answers has a comprehensive education and training program for members, elected representatives, managers and employees so they can contribute effectively to the development of the company and their own credit union. In turn, these people inform the general public – particularly young people and opinion leaders – about the nature and benefits of co-operation.

Principle 6: Cooperation Among Cooperatives - CU*Answers serves members most effectively and strengthen the co-operative movement by working together through local, national, regional and international structures.

Principle 7: Concern for Community - CU*Answers is engaged in the sustainable development of CU*Answers' communities through policies approved by our members.

Services Overview

CU*BASE is the member data processing system combining member information databases, marketing tools, presentation tools, processing capability and flexible configuration, all with a graphical interface that significantly shortens the staff learning curve.

CU*BASE is an independent and wholly-owned data processing software product, supported and maintained by CU*Answers. CU*BASE can be integrated with other third-party service providers to support additional financial products and services.

CU*BASE is delivered to credit unions as both an application services provider/service bureau (ASP) and fully "turn-key" (self-processing) solution, offering a credit union or a group of credit unions the ability to be shared processors. The key is that CU*BASE provides identical functionality across all delivery methods and allows credit unions the flexibility to pick and choose, and even move from one delivery method to another based upon a credit union's business plan.

B. Scope of Report

The report covers the CU*BASE Application Processing and Managed Hosting Services System and includes the infrastructure, backup, and security of the CU*BASE application and related data hosted in the CU*Answers private cloud.

The locations in-scope are the offices within Grand Rapids, MI and Kentwood, MI:

- 6000 28th St SE, Grand Rapids, MI 49546
- Airport Technical Center B, 4695 44th St SE, Kentwood, MI 49512
- Airport Technical Center C, 4635 44th St SE, Kentwood, MI 49512

Significant Changes in the System and Controls

There were no significant changes in the system or controls during the period October 1, 2022 to September 30, 2023.

Subsequent Events

Management is not aware of any relevant events that occurred subsequent to the end of the reporting period through the date of the service auditor's report that would have a significant effect on management's assertion.

C. Subservice Organizations

Management of CU*Answers assumed, in the design of CU*Answers' CU*BASE Application Processing and Managed Hosting Services System that certain controls at subservice organizations are necessary, in combination with controls at CU*Answers, to provide reasonable assurance that CU*Answers' control objectives would be achieved. These complementary subservice organization controls and the related control objectives are described below. Subservice organizations are responsible for implementing such controls.

The following are the subservice organizations used by CU*Answers, services provided by them, and the control objectives that are applicable to the services that they provide:

- **Site-Four, LLC** - Data Center Hosting

Applicable Control Objectives	Expected Controls to be Implemented by the Subservice Organizations
Control Objective 4: Controls provide reasonable assurance that backup procedures and disaster recovery plans are in place, including insurance coverage to cover losses if incurred.	Business continuity and disaster recovery plans are updated at least annually.
Control Objective 5: Controls provide reasonable assurance that logical access to systems and data is restricted to authorized users.	Logical access is restricted to necessary personnel only.

Applicable Control Objectives	Expected Controls to be Implemented by the Subservice Organizations
Control Objective 6: Controls provide reasonable assurance that safeguards and/or procedures are used to protect the organization against intrusions, fire, and other hazards.	All entrances to the buildings and data centers are locked and access is properly restricted. Environmental controls are in place to protect the data center against fire and other hazards.

D. Entity Level Management Processes

Control Environment

A seven-member Board of Directors meets regularly to review company status. The Board of Directors is comprised of members independent from management. Board members are elected by the stockholders, and are required to meet the qualifications outlined in the Board member handbook. The Board meets no less than quarterly to monitor the development and performance of internal controls.

Organizational Structure

An organizational model is in place which clearly defines roles and responsibilities and lines of authority. The organizational model is updated as needed, but no less than annually, and is reviewed and approved every two years by upper management and the Board of Directors. CU*Answers is organized into functional groups to support and achieve the Company's objectives which are outlined in the Organizational Model. Human Resources also maintains written position descriptions for each role which are updated as roles change and are reviewed by management periodically.

Human Resources Policies and Practices

Management has established and periodically updates standards for hiring. Employees are provided with company policies and procedures upon hire and annually thereafter. Training and awareness programs are provided to employees to promote ethical behavior throughout the organization and to develop and retain sufficient and competent personnel. Training is provided upon hire to familiarize new employees with CU*Answers and ongoing training is required to help employees gain the appropriate skills and knowledge to perform their job responsibilities. Employee performance is evaluated annually by management.

Risk Assessment

CU*Answers follows a formal risk management program. The program's risk assessment is performed by the Internal Audit Team, on no less than an annual basis and directed against the foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of member information or member information systems. This risk assessment will assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of member information. The risk assessment outlines the risks associated with business objectives, including the risk of fraud. The risk assessment assesses the sufficiency of policies, procedures, member information systems, and other arrangements in place to control risks. The overall risks are revaluated by a broader segment of company leaders annually and new risks are identified or removed as appropriate. The risk management program results are reported to the Board of Directors and approved by the Board of Directors and executive management annually.

Internal Audit creates and documents an audit plan annually based on the updated risk assessment. The audit plan is updated, as needed, and is reviewed and approved by executive management and the Board of Directors. Internal and external audits are conducted throughout the year to monitor the effectiveness of internal controls in accordance with the audit plan. Updates on testing results and management responses are provided to executive management and the Board of Directors no less than quarterly and are tracked for remediation.

The Company also maintains an IT Strategic report that is reviewed annually.

Information and Communication

Policy, Standards, Procedures, and Guidelines

Workplace conduct standards and policies and procedures outlining internal controls are formally documented in the Employee Handbook and Policy Manual. Both documents are revised, as needed, and are formally reviewed and approved every two years by executive management and the Board of Directors. CU*Answers maintains a security policy which is updated and approved by executive management and the Board of Directors every two years that addresses key elements pertaining to the protection of non-public personal information which is provided to both internal and external users. This includes policies and procedures for data security, disposal of obsolete equipment, and destruction of confidential documents and media.

Communication

CU*Answers management has multiple channels to communicate important information externally and internally, including email notices, online message boards, phone calls to clients, posting on internally and externally facing websites, on-demand videos, and press releases.

CU*Answers has also implemented other methods of communication with subscribers, providers, clients, agents, and benefit representatives. There are newsletters summarizing significant events, a website, and an opportunity to meet with the team on-premises. The Customer Service and Education Department provides ongoing communication with clients.

To help employees understand their individual roles and responsibilities, CU*Answers has orientation and training for newly hired employees, as well as ongoing training for all employees. CU*Answers also communicates important policies and procedures, including security policies via the Employee Handbook and Policy Manual. Policies and procedures are available at any time on the CU*Answers intranet and printed copies are available in the HR suite of the main office.

In addition to policies and procedures, CU*Answers' intranet summarizes both current and planned significant events and changes. The site also contains management reports, department and corporate objectives, and the quality manual, and it acts as a central repository for manuals and industry specific information. CU*Answers' executive management gives annual update meetings and distributes the strategic plan to all employees. Electronic messages are used to communicate time-sensitive messages and information.

Training

People are the closest security layer to the data, and social engineering attacks have historically been the most effective way to compromise networks. Therefore, both technical and non-technical staff are regularly trained on the latest security techniques and procedures and social engineering tactics and defenses.

Monitoring

CU*Answers has established a layered approach to monitor the quality of services provided to clients. Management and supervisory staff play an important role in monitoring quality as a routine responsibility of their function. Management relies on various reports to measure the efficiency and effectiveness of client transactions, including reports of processing capacity, system availability, and response times. Internal Audit provides validation that the established policies and procedures are followed as directed by senior management and the Board of Directors. Regular Board of Directors meetings are held to review operational and financial results, and to discuss audit findings. The Board of Directors reviews reports issued by Internal Audit, Federal regulators, and third-party audit vendors.

Internal Audit

CU*Answers is subject to reviews by Internal Audit on a regular basis. The Internal Auditing team has experience in accounting, law, network infrastructure, client support, and system auditing. The intent of CU*Answers is to create the proper separation of responsibilities to ensure operations are constantly reviewed. CU*Answers approaches all audits with candid and transparent accountability to allow owners and clients to feel confident that the organization's solutions and capabilities are built with the intent of being a leader in the industry and an operator of the utmost quality. Internal Audit assists executive management in accomplishing objectives by bringing a disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. Internal Audit focuses on providing initial assessments to identify risks and to design internal controls at the beginning of a project.

CU*Answers monitors and audits activities including program moves, device firmware updates, user activity, terminal security, and off-site and on-site tape backup libraries. As a company, CU*Answers also monitors and audits network systems, including managed hosting networks, for configuration changes, current anti-virus pattern files, resource utilization, significant system events, invalid sign-on attempts and software patch levels. CU*Answers also undergoes regular regulatory examinations by state and federal authorities and schedules external audits that include a review of segregation of responsibilities.

The Board of Directors and management are provided with information on the effectiveness of the system of internal controls. This information is gathered internally by the internal auditor, by certified public accounting firms or by state or federal regulatory agencies through audits of financial, operational, compliance and information systems on an ongoing or periodic basis (or any combination thereof).

E. Components of the System

Infrastructure

Credit unions that are part of the CU*Answers network are provided CU*BASE from the Kentwood data center. In the event of a disruption of service, core processing is redirected to the High Availability center located at Site-Four, LLC (Site-Four). Mission critical client databases are replicated in real-time from the production system at the Kentwood data center to the identical High Availability system at Site-Four over a private fiber high speed connection.

CU*BASE operates using a variety of IBM Midrange and Intel-based computers in the Kentwood and Site-Four facilities. Primary hardware consists of IBM iSeries servers. iSeries operating systems are standard OS/400 Releases and are upgraded as needed.

CU*Answers also has an internal Storage Area Network (SAN) powered by Nimble and Dell EqualLogic. Mission critical databases are backed up to the SAN system.

Software

The following is the primary application in-scope:

Application	Description
CU*BASE	Member data processing system

The primary application is supported by the following:

Application	Description
Fortinet	Client Firewalls and Firewall Backups
Kaseya	Windows Patching
Nagios	Network Monitoring

Application	Description
TrendMicro	Anti-virus
SonicWall	Internal Firewalls
VMWare	Virtual Machines
ConnectWise	Ticketing System
iTera Echo2	Replication for iSeries
Arctic Wolf	Internal Network Monitoring

People

CU*Answers is organized into the following groups which assist in the performance of internal controls:

- Board of Directors - The Board of Directors is comprised of members independent from management and are responsible for the development and performance of internal controls.

- Human Resources - Responsible for the organizational strategic planning, employee development, and the development and tracking of client interaction standards and expectations.

- Internal Audit - Responsible for providing assurance to management to ensure assets are safeguarded, internal controls are operating effectively, and compliance is maintained with prescribed laws and company policies.

- Network Services - Responsible for the performance of internal controls relating to the network, hardware, capacity, and patching. Also, provides external support of hardware, network configurations, and communications issues that arise from the performance of the in-scope applications.

- Operations - Responsible for the completeness, timeliness, and accuracy of data utilized by clients. Also, performs the maintenance of iSeries systems and backups.

- Programming Team - Responsible for the development and support of the in-scope applications.

Data

The CU*BASE application processes all electronic transactions containing sensitive financial information for credit unions. The application performs the following:

- Account Management - Configuration options for savings, certificates, and loans

- Teller/Member Services - Teller Cash Dispenser/Recycler integration including automated funds transfer and check transfers

- Lending and Collections - Online credit reports, loan underwriting, and loan tracking tools

Procedures

Organization and Administration

The Employee Handbook requires employees to take at least five consecutive days away from job functions each year, which is tracked by Human Resources (HR) to ensure compliance. Upon hire and periodically upon update of the Employee Handbook and Policy Manual, employees are required to sign an Employee Acknowledgment Form acknowledging receipt and agreement to abide by the rules and conditions outlined in the Employee Handbook and Policy Manual.

Job descriptions are documented which define roles and responsibilities. Prior to being hired, employees are subjected to a screening process, including a background check.

Communication with Clients

Commitments are communicated to new clients via formal contracts, including confidentiality and privacy commitments and user responsibilities.

Senior management, including the SVPs of Technology, consider developments in technology and the impact of applicable laws or regulations on the entity's security policies on no less than an annual basis. Considerations are documented in the IT Strategic Report and are reviewed by executive management and the board of directors annually.

Internal audits are conducted throughout the year to monitor the effectiveness of internal controls in accordance with the audit plan. Updates on testing results and management responses are provided to executive management and the Board of Directors no less than quarterly and are tracked for remediation.

Vendor Management

Management has a formal vendor management program that identifies critical vendors and their functions and cross-references the vendors to the appropriate department. Initial and ongoing due diligence, including annual assessment of critical vendors, is performed to mitigate and manage risks. Management reviews third party audit reports over service organization controls to ensure controls are implemented and performed as documented for critical vendors.

Backup and Recovery Procedures

CU*Answers has a formal written contingency plan that addresses risks related to potential business disruptions. The plan is tested and documented by management at least annually.

Vital files are backed up daily and replicated to redundant systems at the offsite location. Backups are monitored daily by Operations. All mission critical database servers are replicated to the secured servers at the offsite facility throughout the day. Backup performance is reviewed daily by Network Services.

CU*Answers has a hot-site agreement to provide equipment and facilities backup should the service organization site be destroyed or rendered inoperable.

Production iSeries systems are monitored daily using third party software which provides alerts to staff regarding the capacity and availability of network resources. Monitoring is documented on the daily Network Services checklist which includes tracking alerts to resolution.

The service organization maintains current cyber insurance policies.

Logical Access

An access request process exists for iSeries that is used to document management authorization and approval of new user accounts. The requests are submitted through an access form to the IT staff for internal and external users. iSeries access for terminated employees is removed from the system within one business day of termination. The system will automatically disable accounts after 92 days of inactivity.

An access request process exists for AD that is used to document management authorization and approval of new user accounts. The requests are approved by HR or employee's manager and is submitted through an access form to the IT staff. Active Directory access for terminated employees is removed from the system within one business day of termination by IT staff.

User access reviews to ensure terminated employees' access to the network has been disabled are performed by Internal Audit and reported to the Board on a quarterly basis.

The following password parameters are in place for the internal network:
-Minimum Length: 7 Characters
-Complexity: Enabled
-Max Age: 30 days
-History: 24 Passwords
-Lockout Threshold: 3 Attempts
-Inactivity Timeout: 10 minutes

The following password parameters are in place to authenticate into the CU*BASE application:
-Minimum Length: 8
-Complexity: Enabled
-Max Age: 30 Days
-History: 32 Passwords
-Lockout Threshold: 3 Attempts

Logical access to data is restricted to authorized administrators. Access to a client data library is restricted to users authorized by the user organization. User credit unions have the ability to define sensitive access restrictions based on security profile configurations. Access to source code stored on the development iSeries is restricted to authorized individuals based on job responsibility. Access is reviewed annually by Internal Audit to ensure terminated employee's access has been disabled.

The firewall logs suspicious and unauthorized access attempts. Network Services personnel review these logs on a daily basis. The firewalls and routers have been configured to restrict access from the internet, member credit unions, other financial institutions, and business partners to only authenticated users that have access to the internal network. ArcticWolf monitors the internal network and sends alerts to the Network Services Team related to intrusion prevention and malware. Critical events that require additional investigation are communicated via phone or email to the Network Services Team and are monitored and tracked to resolution.

Data is transmitted securely between the host and client application. Data communication lines are either internet or MPLS dedicated lines and secured using VPN tunnels.

iSeries security reports that identify login, changes in access, and production changes are automatically generated and reviewed daily by Internal Audit. If an issue is identified, it is escalated via the incident response protocol. Production system logs are configured to record specified system events and the logs are retained for a minimum of 21 days. The logs are reviewed by Network Services as part of the daily checklist.

Physical Security

Access to the facilities is restricted via key fob. Visitors to the facilities are required to sign-in and are issued a visitor badge upon arrival. Internal Audit reports any physical access violations to the Board of Directors at least quarterly.

Access to the data centers and network closets is restricted via the key fob system and is limited to personnel requiring access based on job responsibilities.

Data centers are equipped with the following environmental controls:
•Heat and smoke detectors connected to a monitored alarm system
•Fire suppression/fire extinguishers
•Dedicated air conditioning units
•Uninterruptible Power Supply (UPS)
•Server Racks
•Temperature/Humidity Monitoring

A generator is installed to provide continued power to the facility in the event of a long-term power outage. The generator is tested weekly to ensure operability in the event of an outage.

Change Management

System development and change control policies have been created to formally direct system modifications. The policies are updated, reviewed, and approved by IT Management and the Board of Directors every two years.

All program changes are required to be authorized, tested, and documented (including design, development and configuration information) within a project tracking ticket.

New server operating system versions are authorized by management prior to implementation.

Computer Operations

iSeries hardware is maintained under contract with the vendor.

Control features within the operating system software note any hardware errors occurring during processing. Multi-level monitoring procedures are in place to ensure errors are properly investigated and remediated by Network Services. Network Services monitors the health and security of internal network systems by performing daily checks using runsheets. Issued are tracked to resolution within the ticketing system.

The system is configured such that output reports and customer statements are downloaded daily to the applicable credit union's library. The Imaging Solutions team monitors the files for successful import and processing. Processing exceptions are documented within the Operations runsheets. CU*Answers management reviews and resolves identified issues on a daily basis. For incoming ACH, totals from FEDLINE are compared to system totals prior to processing by Operations. The comparison is documented within the Operations runsheet. Procedures are documented in the Operations runsheet for job processing streams with sequential processing required so that prior processing steps are completed before proceeding with the next processing step. System restart/rerun procedures are in place and assist in the proper recovery of application processing should a program abnormally terminate and is monitored daily by Operations in their daily runsheet. The Operations department utilizes a daily runsheet for processing. The runsheet is reviewed by an Operations supervisor for completeness.

F.   Control Objectives and Related Controls

The Company's control objectives, and the related controls designed to provide reasonable assurance that the service organization's control objectives were achieved, are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section and repeating them in Section 4. Although the control objectives and related controls are presented in Section 4, they are an integral part of the entity level management process and description of system used to provide services.

G.   Complementary User Entity Controls

Management of CU*Answers assumed, in the design of CU*Answers' CU*BASE Application Processing and Managed Hosting Services System that certain controls will be implemented by user entities, and those controls are necessary, in combination with controls at CU*Answers, to provide reasonable assurance that CU*Answers' control objectives would be achieved. These complementary user entity controls and the related control objectives are described below. User entities are responsible for implementing such controls.

- Verify and balance all incoming third-party files, such as ATM, ACH, and share drafts. (Control Objective 8)

- Balance system generated general ledger entries to reconcile the general ledger interface against the member trial balance. (Control Objective 8)

- Balance application totals to the independently posted general ledger to verify the overall accuracy of the daily processing results. (Control Objective 8)

H.   User Entity Responsibilities

User entities may have responsibilities when using the system. Those responsibilities are necessary for the user entity to derive the intended benefits of using the services of CU*Answers. User entity responsibilities are as follows:

- Establish report retention procedures to provide backup of data output.

- Have a business continuity plan in place and share this plan with CU*Answers to ensure operations can be restored in the event of an unplanned disruption.

- Clients that manage their own systems should establish procedures to monitor their systems activity.

- Develop internal data security and employee access to system features, as well as all key parameter configurations.

- Control the distribution of reports to user personnel to ensure reports are distributed to only authorized personnel.

- Perform an annual review and approval of all security authorizations to verify security levels are appropriate for each operator, and to identify any potential conflict of duties.

- Maintain a log of CU*Answers' access and communicate any unusual activity to CU*Answers.

- Review on a monthly basis the Member File Maintenance, General Transaction Register, General Journal Report and the Employee Activity Audit for changes made by CU* Answers employees.

- Develop internal data security and employee access to system features, as well as all key parameter configurations.

- Periodically consolidate and revise as necessary the manuals and any supplementary notes which comprise the documentation of each user department's data processing procedures to help ensure the user's proper understanding of the system and to facilitate future training of new employees.

- Review and document on a checklist the reports generated by the system each day to determine all reports have been received.

- Monitor daily exception reports and application suspense accounts.

- Independently verify the master file change listing to help ensure the accuracy and propriety of file maintenance posting.

- Independently monitor usage of interest and accounts payable checks printed by the data processing department to safeguard and maintain accountability for such items.

- Review ACH reports and ACH errors daily to identify batch errors and exceptions. Any items previously sent as ACH transactions that have been returned by the ACH operator must be corrected and retransmitted. Any incoming ACH items that have been rejected need to be manually posted and corrective action needs to be taken to prevent errors in the future.

- Assign each teller override levels to prevent a teller from performing certain transactions.

SECTION 4. CONTROL OBJECTIVES, CU*ANSWERS, INC.'S DESCRIPTION OF RELATED CONTROLS AND SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

This section presents the following information provided by CU*Answers:

- The control objectives specified by the management of CU*Answers.

- The controls established and specified by CU*Answers to achieve the specified control objectives.

Also included in this section is the following information provided by the service auditor:

- A description of the tests performed by the service auditor to determine whether the service organization's controls were operating with sufficient effectiveness to provide reasonable assurance that the specified control objectives were achieved. The service auditor determined the nature, timing, and extent of the testing performed.

- The results of the service auditor's tests of controls.

The service auditor performed observation and inspection procedures as they relate to system-generated reports, queries, and listings to assess the accuracy and completeness of the information used in the service auditor's tests of controls.

1. Organization and Administration

Control Objective: Controls provide reasonable assurance that CU*Answers is organized with defined roles and responsibilities, employees are subject to background checks upon hire, and periodically attest to agreement with CU*Answers policies and procedures.

Description of Controls

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
1. An organizational model is in place which clearly defines roles and responsibilities and lines of authority. The organizational model is updated as needed, but no less than annually, and is reviewed and approved every two years by upper management and the Board of Directors.	Inspected the organizational model to determine that organizational structures, reporting lines, authorities, and responsibilities were defined.	No deviations noted.
	Inspected meeting minutes to determine the organizational model was approved by management and the Board of Directors during the period.	No deviations noted.
2. Job descriptions are documented which define roles and responsibilities.	Inspected job descriptions for a sample of active employees to determine roles and responsibilities were defined.	No deviations noted.
3. Prior to being hired, employees are subjected to a screening process, including a background check.	Inspected background screening documentation for a sample of new employees to determine if background screening was completed prior to hire.	No deviations noted.
4. Workplace conduct standards and policies and procedures outlining internal controls are formally documented in the Employee Handbook and Policy Manual. Both documents are revised, as needed, and are formally reviewed and approved every two years by executive management and the Board of Directors.	Inspected the Employee Handbook and Policy Manual to determine that internal control policies and procedures, including confidentiality and privacy policies, are described.	No deviations noted.
	Inspected meeting minutes to determine the Employee Handbook and Policy Manual was reviewed and approved by executive management and the Board of Directors within the period.	No deviations noted.

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
5. Upon hire and periodically upon update of the Employee Handbook and Policy Manual, employees are required to sign an Employee Acknowledgment Form acknowledging receipt and agreement to abide by the rules and conditions outlined in the Employee Handbook and Policy Manual. There were no major updates to the Employee Handbook and Policy Manual during the period. Therefore, there were no circumstances that warranted the performance of the control.	Inspected signoff forms for a sample of new employees during the period to determine if the employee handbook and policy manual was acknowledged upon hire.	No deviations noted.
	There were no instances of this control during the period. Therefore, there were no circumstances that warranted the performance of the control. Inspected the Employee Handbook and Policy Manual and Board Meeting Minutes to determine there were no major updates during the period.	Not applicable.
6. The Employee Handbook requires employees to take at least five consecutive days away from job functions each year, which is tracked by Human Resources (HR) to ensure compliance.	Inspected records maintained by HR for a sample of employees to determine if five consecutive days away from job functions was completed during the period.	No deviations noted.
7. CU*Answers maintains a security policy which is updated and approved by executive management and the Board of Directors every two years that addresses key elements pertaining to the protection of non-public personal information which is provided to both internal and external users. This includes policies and procedures for data security, disposal of obsolete equipment, and destruction of confidential documents and media.	Inspected the security policy to determine if it addresses key elements pertaining to the protection of non-public personal information and is provided to both internal and external users.	No deviations noted.
	Inspected meeting minutes to determine the security policy was reviewed and approved by executive management and the Board of Directors within the period.	No deviations noted.

2.   Communication with Clients

Control Objective: Controls provide reasonable assurance that CU*Answers user responsibilities are communicated and CU*Answers controls are internally monitored and subject to oversight.

Description of Controls

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
1. Commitments are communicated to new clients via formal contracts, including confidentiality and privacy commitments and user responsibilities.	Inspected a sample of customer contracts for new clients during the period to determine if responsibilities, including confidentiality and privacy practices, are communicated.	No deviations noted.
2. Senior management, including the SVPs of Technology, consider developments in technology and the impact of applicable laws or regulations on the entity's security policies on no less than an annual basis. Considerations are documented in the IT Strategic Report and are reviewed by executive management and the board of directors annually.	Inspected the Strategic Technology Plan and Board of Directors minutes to determine if the plan was updated, reviewed by management, and approved by the Board of Directors annually.	No deviations noted.
3. Internal audits are conducted throughout the year to monitor the effectiveness of internal controls in accordance with the audit plan. Updates on testing results and management responses are provided to executive management and the Board of Directors no less than quarterly and are tracked for remediation.	Inspected internal audit reports and Board of Directors meeting minutes for a sample quarter to determine if internal control testing occurred and results were presented to management and the Board of Directors and tracked until remediation.	No deviations noted.

3.   Vendor Management

Control Objective: Controls provide reasonable assurance that CU*Answers has a vendor management program in place to identify and perform due diligence on critical vendors.

Description of Controls

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
1. Management has a formal vendor management program that identifies critical vendors and their functions and cross-references the vendors to the appropriate department. Initial and ongoing due diligence, including annual assessment of critical vendors, is performed to mitigate and manage risks.	Inspected the vendor management program to determine it documents the items noted within the control description.	No deviations noted.
	Inspected the vendor risk assessment to determine if critical vendors are identified and associated risks are annually assessed.	No deviations noted.
	Inspected the due diligence for a sample of new vendors to determine it was completed during onboarding.	No deviations noted.
2. Management reviews third party audit reports over service organization controls to ensure controls are implemented and performed as documented for critical vendors.	Inspected management's review of third party audit reports for a sample of critical vendors to determine if they evaluated controls at the service organization.	No deviations noted.

4. Backup and Recovery Procedures

Control Objective: Controls provide reasonable assurance that backup procedures and disaster recovery plans are in place, including insurance coverage to cover losses if incurred.

Description of Controls

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
1. The service organization maintains current cyber insurance policies.	Inspected cyber insurance policy to determine it is in place and covers the period.	No deviations noted.
2. CU*Answers has a formal written contingency plan that addresses risks related to potential business disruptions. The plan is tested and documented by management at least annually.	Inspected the business continuity plan and documented testing results to determine if the plan addresses risks related to business disruptions.	No deviations noted.
	Inspected the results of the most recent business continuity plan test to determine testing is conducted annually.	No deviations noted.
3. Vital files are backed up daily and replicated to redundant systems at the offsite location. Backups are monitored daily by Operations.	Inspected the Backup Runsheets for a sample of days to determine if daily iSeries file backup and replication tasks were completed.	No deviations noted.
4. All mission critical database servers are replicated to the secured servers at the offsite facility throughout the day. Backup performance is reviewed daily by Network Services.	Inspected Network Services checklists for a sample of days to determine if daily database server backup tasks were completed.	No deviations noted.
5. CU*Answers has a hot-site agreement to provide equipment and facilities backup should the service organization site be destroyed or rendered inoperable.	Inspected hot-site agreement to determine if equipment and backup facility requirements are defined and included for use if a disaster occurs.	No deviations noted.
6. Production iSeries systems are monitored daily using third party software which provides alerts to staff regarding the capacity and availability of network resources. Monitoring is documented on the daily Network Services checklist which includes tracking alerts to resolution.	Inspected Network Services checklists for a sample of days to determine if monitoring activities in response to output from the tool regarding the capacity and ability of network resources were completed daily.	No deviations noted.

5. Logical Access

Control Objective: Controls provide reasonable assurance that logical access to systems and data is restricted to authorized users.

Description of Controls

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
1. Logical access to data is restricted to authorized administrators.	Inspected the listing of Active Directory and iSeries administrators to determine logical access to data is restricted to personnel requiring access based on their job responsibilities.	No deviations noted.
2. The following password parameters are in place for the internal network: -Minimum Length: 7 Characters -Complexity: Enabled -Max Age: 30 days -History: 24 Passwords -Lockout Threshold: 3 Attempts -Inactivity Timeout: 10 minutes	Inspected password parameters for Active Directory to determine it contains the items noted within the control description.	No deviations noted.
3. The following password parameters are in place to authenticate into the CU*BASE application: -Minimum Length: 8 -Complexity: Enabled -Max Age: 30 Days -History: 32 Passwords -Lockout Threshold: 3 Attempts	Inspected password parameters for the CU*BASE application to determine it contains the items noted within the control description.	No deviations noted.
4. An access request process exists for AD that is used to document management authorization and approval of new user accounts. The requests are approved by HR or employee's manager and is submitted through an access form to the IT staff.	Inspected access request forms for a sample of new AD user accounts added during the period to determine the access request process is documented and approved by HR or the employee's manager.	No deviations noted.
5. An access request process exists for iSeries that is used to document management authorization and approval of new user accounts. The requests are submitted through an access form to the IT staff for internal and external users.	Inspected access request forms for a sample of new iSeries internal and external user accounts added during the period to determine the access request process is documented and approved.	No deviations noted.

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
6. Active Directory access for terminated employees is removed from the system within one business day of termination by IT staff.	Inspected tickets for a sample of terminated employees to determine access to Active Directory was removed within one business day of termination by IT staff.	Deviations noted. CU*Answers could not demonstrate Active Directory access was disabled within one business day of termination for two out of 10 sampled terminated employees. CU*Answers provided evidence access was terminated after one business day of termination.
	Inspected user listings for a sample of terminated employees to determine access to Active Directory was removed by IT staff.	No deviations noted.
7. iSeries access for terminated employees is removed from the system within one business day of termination. The system will automatically disable accounts after 92 days of inactivity.	Inspected tickets for a sample of terminated employees to determine access to iSeries was removed within one business day of termination.	Deviations noted. CU*Answers could not demonstrate iSeries access was removed within one business day of termination for one out of 10 sampled terminated employees. CU*Answers provided evidence access was terminated after one business day of termination.
	Inspected iSeries configurations settings to determine iSeries accounts are automatically disabled after 92 days of inactivity.	No deviations noted.
8. User access reviews to ensure terminated employees' access to the network has been disabled are performed by Internal Audit and reported to the Board on a quarterly basis.	Inspected Internal Audit report results and selected a sample of quarters to determine a review of terminated employees access was performed and reported to the Board.	No deviations noted.

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
9. Access to source code stored on the development iSeries is restricted to authorized individuals based on job responsibility. Access is reviewed annually by Internal Audit to ensure terminated employee's access has been disabled.	Inspected the listing of users with access to source code to determine it is restricted to authorized individuals based on job responsibility.	No deviations noted.
	Inspected Internal Audit report results to determine a review of terminated employees was performed for development iSeries access within the period.	No deviations noted.
10. Access to a client data library is restricted to users authorized by the user organization. User credit unions have the ability to define sensitive access restrictions based on security profile configurations.	Inspected system configuration settings to determine security profiles are utilized to restrict user access within the system.	No deviations noted.
	Inspected client data libraries to determine individual data libraries are in place to restrict access to users authorized by the client.	No deviations noted.
	Inspected data libraries and security profiles for a sample of new clients to determine data libraries and security profiles are in place.	No deviations noted.
11. The firewall logs suspicious and unauthorized access attempts. Network Services personnel review these logs on a daily basis.	Inspected Network Services checklists for a sample of days to determine if firewall logs and critical events were reviewed.	No deviations noted.
12. The firewalls and routers have been configured to restrict access from the internet, member credit unions, other financial institutions, and business partners to only authenticated users that have access to the internal network.	Inspected firewall and router configurations to determine access restriction rules are configured and only authenticated users have access to the internal network.	No deviations noted.

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
13. ArcticWolf monitors the internal network and sends alerts to the Network Services Team related to intrusion prevention and malware. Critical events that require additional investigation are communicated via phone or email to the Network Services Team and are monitored and tracked to resolution.	Inspected the Arctic Wolf escalation procedures and performed an observation with the Network Services Team to determine Arctic Wolf monitors the internal network and the Network Services Team monitors and tracks the received security events until resolution.	No deviations noted.
14. Data is transmitted securely between the host and client application.	Inspected the encryption certificate chain for connections to the host to determine if data is transmitted securely.	No deviations noted.
15. Data communication lines are either internet or MPLS dedicated lines and secured using VPN tunnels.	Inspected network diagrams within the BCP to determine they document VPN or MPLS dedicated line utilization for client network connections.	No deviations noted.
	Inspected configurations for a sample of routers to determine VPN tunnels were established.	No deviations noted.
16. iSeries security reports that identify login, changes in access, and production changes are automatically generated and reviewed daily by Internal Audit. If an issue is identified, it is escalated via the incident response protocol.	Inspected iSeries reports for a sample of days to determine if the reports were automatically generated and any issues identified were escalated and documented within Internal Audit's report to the Board of Directors.	No deviations noted.
17. Production system logs are configured to record specified system events and the logs are retained for a minimum of 21 days. The logs are reviewed by Network Services as part of the daily checklist.	Inspected Network Services checklists for a sample of days to determine if system logs were reviewed for specified system events by Network Services.	No deviations noted.

6.   Physical Security

Control Objective: Controls provide reasonable assurance that safeguards and/or procedures are used to protect the organization against intrusions, fire, and other hazards.

Description of Controls

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
1. Access to the facilities is restricted via key fob.	Performed an observation of the key fob system at all in-scope facilities to determine facility access is restricted via key fob.	No deviations noted.
2. Access to the data centers and network closets is restricted via the key fob system and is limited to personnel requiring access based on job responsibilities.	Performed an observation of in-scope data centers and network closets to determine access is restricted via key fob.	No deviations noted.
	Inspected a listing of users with access to in-scope data centers and network closets to determine access is restricted based on the individual's job responsibilities.	No deviations noted.
3. Data centers are equipped with the following environmental controls: •Heat and smoke detectors connected to a monitored alarm system •Fire suppression/fire extinguishers •Dedicated air conditioning units •Uninterruptible Power Supply (UPS) •Server Racks •Temperature/Humidity Monitoring	Performed an observation of the in-scope data centers to determine they are equipped with the items noted within the control description.	No deviations noted.
	Inspected the contract for the alarm vendor to determine the fire and smoke detection system is monitored.	No deviations noted.

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
4. A generator is installed to provide continued power to the facility in the event of a long-term power outage. The generator is tested weekly to ensure operability in the event of an outage.	Performed an observation of the generator at in-scope locations to determine it is in place.	No deviations noted.
	Inspected the generator testing logs for a sample of weeks to determine testing was performed.	No deviations noted.
5. Internal Audit reports any physical access violations to the Board of Directors at least quarterly.	Inspected Internal Audit Reports for a sample of quarters to determine physical access violations were reported to the Board of Directors.	No deviations noted.
6. Visitors to the facilities are required to sign-in and are issued a visitor badge upon arrival.	Performed an observation of the visitor process at in-scope locations to determine visitors are required to sign in and are provided with a visitor badge.	No deviations noted.

7. Change Management

Control Objective: Controls provide reasonable assurance that changes to system software are authorized, tested, and reviewed, prior to implementation.

Description of Controls

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
1. All program changes are required to be authorized, tested, and documented (including design, development and configuration information) within a project tracking ticket.	Inspected project tracking tickets for a sample of changes to determine authorization and testing were documented.	No deviations noted.
2. The production team discusses the status of projects in the development, testing, and implementation stages to provide oversight and address any issues on at least a monthly basis. Changes that are ready for production are approved during these meetings.	Selected a sample of months and inspected meeting minutes to determine if the production team discussed the status of projects, took actions in response to identified issues, and approved changes for production.	No deviations noted.
3. System development and change control policies have been created to formally direct system modifications. The policies are updated, reviewed, and approved by IT Management and the Board of Directors every two years.	Inspected the Software Development Life Cycle (SDLC) document, developer guidelines, and the Network Services playbook to determine if they address system modification and change control processes.	No deviations noted.
	Inspected meeting minutes to determine the Software Development Life Cycle (SDLC) was updated, reviewed, and approved by management and the Board of Directors within the period.	No deviations noted.
4. New server operating system versions are authorized by management prior to implementation. There were no new server operating system versions during the period. Therefore, there were no circumstances that warranted the performance of the control.	There were no instances of this control during the period. Therefore, there were no circumstances that warranted the performance of the control. Inspected the listing of servers and performed corroborative inquiries with Internal Audit and Network Engineers to verify there no new server operating system versions during the period.	Not applicable.

8. Computer Operations

Control Objective: Controls provide reasonable assurance that computer operations and data control procedures are used to help ensure complete, authorized, and accurate processing.
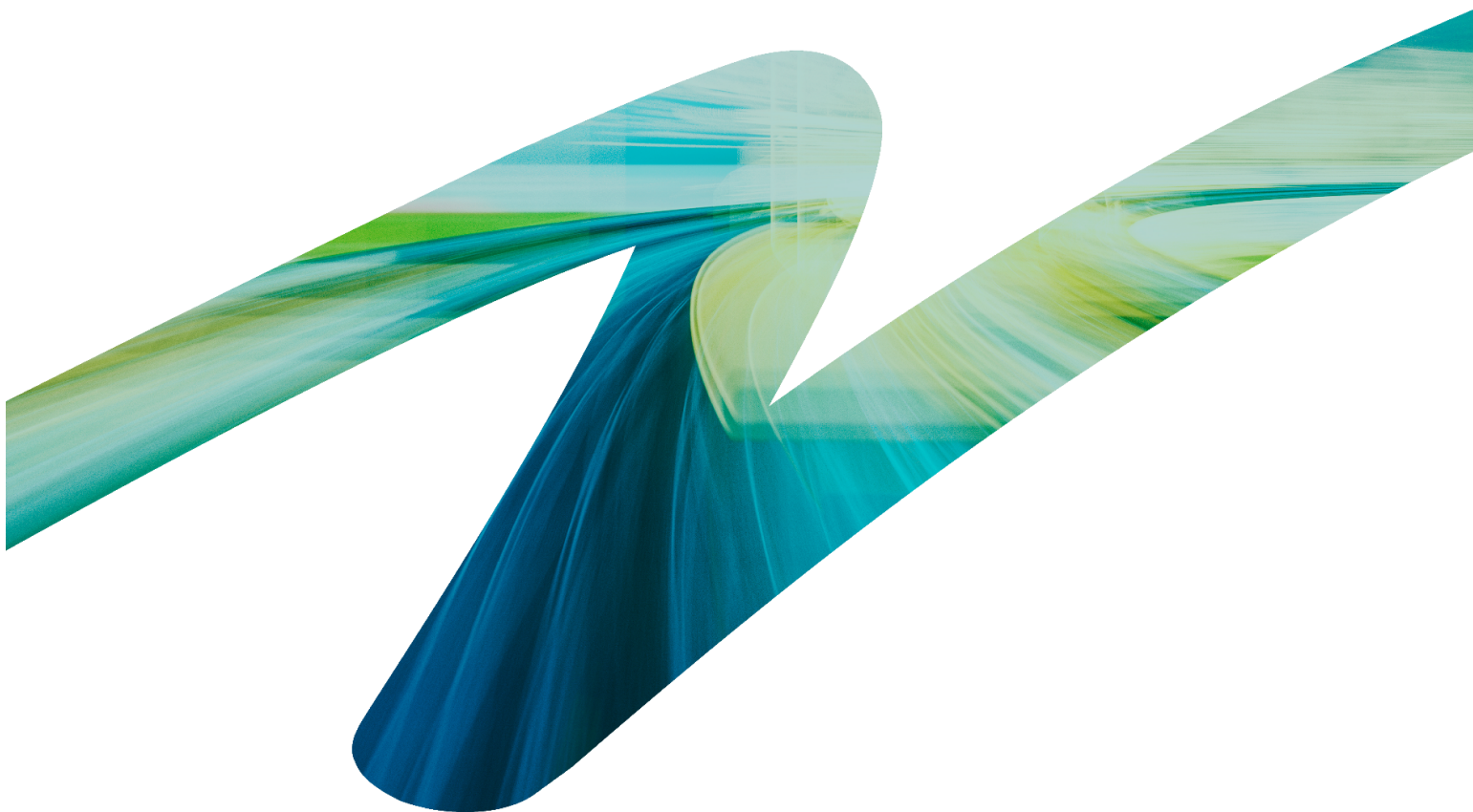
Description of Controls

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
1. Control features within the operating system software note any hardware errors occurring during processing. Multi-level monitoring procedures are in place to ensure errors are properly investigated and remediated by Network Services.	Inspected Network Services checklists for a sample of days to determine if hardware errors during processing are monitored, investigated and resolved by Network Services.	No deviations noted.
2. The system is configured such that output reports and customer statements are downloaded daily to the applicable credit union's library. The Imaging Solutions team monitors the files for successful import and processing.	Inspected Operations runsheets for a sample of days to determine if the daily report import process successfully executed and identified issues were resolved by the Imaging Solutions team.	No deviations noted.
3. The Operations department utilizes a daily runsheet for processing. The runsheet is reviewed by an Operations supervisor for completeness.	Inspected Operations runsheets for a sample of days to determine if an Operations supervisor acknowledged completeness of each day's runsheet.	No deviations noted.
4. Network Services monitors the health and security of internal network systems by performing daily checks using runsheets. Issued are tracked to resolution within the ticketing system.	Inspected Network Services checklists for a sample of days to determine if internal network systems were monitored and noted issues were resolved by Network Services.	No deviations noted.
5. Processing exceptions are documented within the Operations runsheets. CU*Answers management reviews and resolves identified issues on a daily basis.	Inspected Operations runsheets for a sample of days to determine if an Operations supervisor reviewed the processing exceptions log and noted issues were resolved.	No deviations noted.
6. For incoming ACH, totals from FEDLINE are compared to system totals prior to processing by Operations. The comparison is documented within the Operations runsheet.	Inspected Operations runsheets for a sample of days to determine if ACH totals from FEDLINE were compared with system totals prior to processing.	No deviations noted.

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
7. Procedures are documented in the Operations runsheet for job processing streams with sequential processing required so that prior processing steps are completed before proceeding with the next processing step.	Inspected Operations runsheets for a sample of days to determine if processing steps are outlined and executed sequentially.	No deviations noted.
8. System restart/rerun procedures are in place and assist in the proper recovery of application processing should a program abnormally terminate and is monitored daily by Operations in their daily runsheet.	Inspected Operations runsheets for a sample of days to determine if restart/rerun procedures were followed and issues resolved if an abnormal termination occurred by Operations.	No deviations noted.
9. iSeries hardware is maintained under contract with the vendor.	Inspected the vendor contract to determine if it includes iSeries hardware maintenance coverage.	No deviations noted.

SECTION 5. OTHER INFORMATION PROVIDED BY MANAGEMENT OF CU*ANSWERS, INC.

The section below provides management response to deviations noted in Section 4. This information has been provided by management, and has not been subjected to examination procedures by Plante Moran.

Ref #	Control Objective	Deviation	Management Response
1	Control Objective 5	CU*Answers could not demonstrate Active Directory access was disabled within one business day of termination for two out of 10 sampled terminated employees. CU*Answers provided evidence access was terminated after one business day of termination.	CU*Answers is modifying its processes to provide better documentation regarding the records of any terminated employees.
2	Control Objective 5	CU*Answers could not demonstrate iSeries access was removed within one business day of termination for one out of 10 sampled terminated employees. CU*Answers provided evidence access was terminated after one business day of termination.	CU*Answers is modifying its processes to provide better documentation regarding the records of any terminated employees.

plante moran | Audit. Tax. Consulting.
Wealth Management.