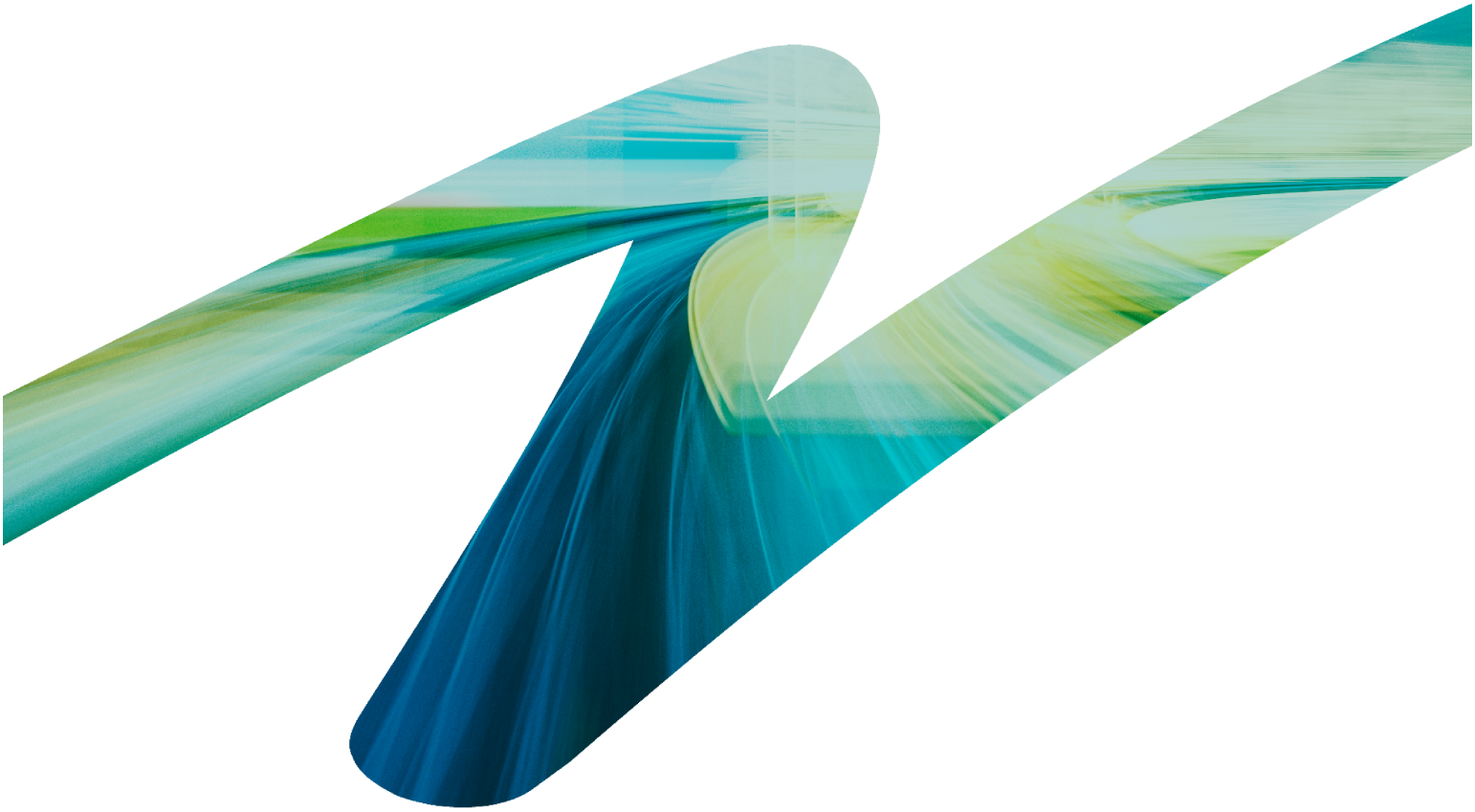
plante moran | Audit. Tax. Consulting. Wealth Management.



CU*Answers, Inc.

SOC 2 Type 2 Report

Report on the CU*BASE System and Network Management Services throughout the period October 1, 2023 to September 30, 2024

Contents

Plante & Moran, PLLC
P.O. Box 307
3000 Town Center, Suite 100
Southfield, MI 48075
Tel: 248.352.2500
Fax: 248.352.0018
plantemoran.com

Independent Service Auditor's Report

To Management
CU*Answers, Inc.

Scope

We have examined management of CU*Answers, Inc.'s (CU*Answers) accompanying description of its CU*BASE System and Network Management Services titled "CU*Answers, Inc.'s Description of its CU*BASE System and Network Management Services" throughout the period October 1, 2023 to September 30, 2024 (the "description") based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (AICPA, *Description Criteria*) (the "description criteria"), and the suitability of the design and operating effectiveness of CU*Answers' controls stated in the description throughout the period October 1, 2023 to September 30, 2024 to provide reasonable assurance that CU*Answers' service commitments and system requirements were achieved based on the trust services criteria for security, availability, processing integrity, confidentiality, and privacy (the "applicable trust services criteria") set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

CU*Answers uses a subservice organization for data center hosting. The subservice organization is provided in the description of the system. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at CU*Answers, to achieve CU*Answers' service commitments and system requirements based on the applicable trust services criteria. The description presents CU*Answers' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of CU*Answers' controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by 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 complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at CU*Answers, to achieve CU*Answers' service commitments and system requirements based on the applicable trust services criteria. The description presents CU*Answers' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of CU*Answers' controls. Our examination did not include 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

CU*Answers is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that CU*Answers' service commitments and system requirements were achieved. CU*Answers' management has provided the accompanying assertion titled "CU*Answers, Inc. Management's Assertion" (the "assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. CU*Answers' management is also 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; selecting the applicable trust services criteria; stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of the controls stated in the description based on our examination.

To Management
CU*Answers, Inc.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. 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:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that the controls were not suitably designed and operating effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of those controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

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

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature and inherent limitations, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of the controls is subject to the risks that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of our tests are presented in Section 4 of this report. The scope of our engagement did not include tests to determine whether trust services categories, related criteria, and control activities 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:

- The description presents CU*Answers' CU*BASE System and Network Management Services that was designed and implemented throughout the period October 1, 2023 to September 30, 2024 in accordance with the description criteria.

- The controls stated in the description were suitably designed throughout the period October 1, 2023 to September 30, 2024 to provide reasonable assurance that CU*Answers' service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout the period October 1, 2023 to September 30, 2024 and if the subservice organization and user entities applied the complementary controls assumed in the design of CU*Answers' controls throughout the period October 1, 2023 to September 30, 2024.
- The controls stated in the description operated effectively throughout the period October 1, 2023 to September 30, 2024 to provide reasonable assurance that CU*Answers' service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of CU*Answers' controls operated effectively throughout the period October 1, 2023 to September 30, 2024.

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 CU*Answers; user entities of CU*Answers' CU*BASE System and Network Management Services throughout the period October 1, 2023 to September 30, 2024; business partners of CU*Answers subject to risks arising from interactions with the system; practitioners providing services to such user entities and business partners; prospective user entities; and business partners and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization’s system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization’s service commitments and system requirements
- User entity responsibilities and how they may affect the user entity’s ability to effectively use the service organization’s services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization’s service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

April 17, 2025

CU*ANSWERS
A CREDIT UNION SERVICE ORGANIZATION

6000 28TH STREET S.E. • GRAND RAPIDS, MI 49546
phone: 616.285.5711 • 800.327.3478 • fax: 616.285.5735
visit us on the web: www.cuanswers.com

April 17, 2025

Plante & Moran, PLLC

To Service Auditors:

We have prepared the accompanying description of CU*Answers, Inc.'s (CU*Answers) CU*BASE system and network management services system titled "CU*Answers, Inc.'s Description of its CU*BASE System and Network Management Services System" throughout the period October 1, 2023 to September 30, 2024 (description) based on the criteria DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about CU*Answers' CU*BASE system and network management services system that may be useful when assessing the risks arising from interactions with the CU*BASE system and network management services system, particularly information about system controls that CU*Answers has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

CU*Answers uses a subservice organization for data center hosting. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at CU*Answers, to achieve CU*Answers' service commitments and system requirements based on the applicable trust services criteria. The description presents CU*Answers' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of CU*Answers' controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at CU*Answers, to achieve CU*Answers' service commitments and system requirements based on the applicable trust services criteria. The description presents CU*Answers' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of CU*Answers' controls.

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

a. the description presents CU*Answers' CU*BASE system and network management services system that was designed and implemented throughout the period October 1, 2023 to September 30, 2024 in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period October 1, 2023 to September 30, 2024 to provide reasonable assurance that CU*Answers' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if subservice organizations and user entities applied the complementary controls assumed in the design of CU*Answers' controls throughout that period.

CU*ANSWERS
A CREDIT UNION SERVICE ORGANIZATION

6000 28TH STREET S.E. • GRAND RAPIDS, MI 49546
phone: 616.285.5711 • 800.327.3478 • fax: 616.285.5735
visit us on the web: www.cuanswers.com

c. the controls stated in the description operated effectively throughout the period October 1, 2023 to September 30, 2024 to provide reasonable assurance that CU*Answers' service commitments and system requirements would be achieved based on the applicable trust services criteria and if complementary subservice organization controls and complementary user entity controls assumed in the design of CU*Answers' controls operated effectively throughout that period.

Very truly yours,

5910947BA06F416...

Geoff Johnson, Chief Executive Officer

SECTION 3. CU*ANSWERS, INC.'S DESCRIPTION OF ITS CU*BASE SYSTEM AND NETWORK MANAGEMENT SERVICES

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

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.

Network Services

The Network Services division of CU*Answers provides a complete offering of network management services. CU*Answers Network Services is a full-service network technology solution offering:

- LAN/WAN design, implementation and management; network security
- Firewall management; cloud-based services and storage
- IP telephony VOIP (voice-over-Internet protocol) solutions
- Electronic records management
- Managed hosting solutions (facilities management), compliance and security audits (HIPAA/GLBA/SOX)
- Strategic technology planning services, remote support services, high availability solutions
- Web site engineering, server, storage, network, PC hardware sales and support services

In addition to financial cooperatives, CU*Answers Network Services department provides network services and consulting to the education, retail, legal, medical, manufacturing, real estate, hospitality, and financial services industries as well as court systems and regional municipalities. CU*Answers Network Services performs 24×7 real-time monitoring and manages thousands of devices and hundreds of networks across the U.S.

B. Scope of Report

The scope of this report is limited to CU*Answers' CU*BASE System and Network Management Services throughout the period October 1, 2023 to September 30, 2024 based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, Description Criteria) (description criteria), and the controls to achieve CU*Answers' service commitments and system requirements based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

CU*Answers is considered a data processor for the purpose of the Privacy Criteria. The locations in-scope are the offices within Grand Rapids, MI and Kentwood, MI.

As noted in Section 3 of the report, CU*Answers does not collect personal information directly from or communicate directly with data subjects, this is the responsibility of the credit unions. Therefore, controls related to the following criteria are not applicable:

- Privacy 1.1, "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."
- Privacy 2.1, "The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented."

- Privacy 3.2, "For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy."
- Privacy 6.1, "The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy," as it relates to the explicit consent of data subjects.
- Privacy 7.1, "The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy," as it relates to the collection of personal information.

As noted in Section 3 of the report, Credit unions are responsible for providing the data subjects with access to their information and notifying CU*Answers of any data changes. Therefore, controls related to the following criteria are not applicable:

- Privacy 5.1, "The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy."
- Privacy 5.2, "The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy."
- Privacy 6.7, "The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objective related to privacy."
- Privacy 8.1, "The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner," as it relates to the communication with data subjects.

Significant Changes in the System and Controls

There were no significant changes in the system or controls during the period October 1, 2023 to September 30, 2024.

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. Principal Service Commitments and System Requirements

CU*Answers has communicated the following principal service commitments to their clients relevant to the Security, Availability, Confidentiality, Processing Integrity, and Privacy of their CU*BASE System and Network Management Services:

- **Security** - CU*Answers commits to keeping data secure by restricting user access to authorized individuals and providing a notification of any breach within a reasonable time period.
- **Availability** - CU*Answers commits to maintaining the availability of resources in the event of a disaster.

- **Confidentiality** - CU*Answers commits to maintaining confidentiality of non-public personal information and be in compliance with regulatory requirements related to data retention and data destruction.
- **Processing Integrity** - CU*Answers commits to responding to written reports of errors or failures of the system in accordance with the CU*Answers Response Incident Procedures and correct any errors affecting after-hours batch transaction processing in a reasonable time frame.
- **Privacy** - CU*Answers commits to protecting the privacy of non-public personal information and providing a notification of any unauthorized disclosures within a reasonable time period.

CU*Answers has established operational requirements that support the achievement of the service commitments. These operational requirements are communicated through CU*Answers' policies and procedures.

- **User Access Review** - 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.
- **Privileged Access** - Administrative access to iSeries and Active Directory is restricted to IT personnel based on job responsibilities.
- **Security Monitoring** - 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.
- **Encryption** - Data is encrypted at rest. Additionally, data is transmitted securely between the host and client application.
- **Incident Response** - An Incident Response Plan is in place within the Policy Manual documenting the process for identifying, investigating, remediating, and recovering from a security incident.
- **Data Retention and Destruction** - Data retention and destruction procedures have been established and documented in a records information management policy, and the disaster recovery manual.
- **Disaster Recovery** - A formal written contingency plan is in place that addresses risks related to potential business disruptions. The plan is tested and documented by management at least annually.
- **Operations Processing** - The Operations department utilizes a daily runsheet to monitor the completeness, accuracy, and timeliness of processing.

D. Subservice Organizations

Management of CU*Answers assumed, in the design of CU*Answers' CU*BASE System and Network Management Services that certain controls at subservice organizations are necessary, in combination with controls at CU*Answers, to provide reasonable assurance that CU*Answers' service commitments and system requirements would be achieved. These complementary subservice organization controls and the related trust services criteria are described below. Subservice organizations are responsible for implementing such controls.

The following is the subservice organization used by CU*Answers, services provided by them, and the trust services criteria that are applicable to the services that they provide:

- **Site-Four, LLC** - Data center hosting

Applicable Trust Services Criteria	Expected Controls to be Implemented by the Subservice Organizations
Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Administrative access is restricted to necessary personnel only. Remote access connections are encrypted via VPN. Only authorized users are provisioned logical access and terminated users are deprovisioned timely.
Common Criteria 6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	All entrances to the buildings and data centers are locked and access is properly restricted.
Availability Criteria 1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Business continuity and disaster recovery plans are updated at least annually. Environmental controls are in place to protect the data center against fire and other hazards.

E. 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 the Board of Directors and executive management. 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.

Human Resources Policies and Practices

Management has established 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 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 that must be completed within seven business days, as well as annual 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 trained on the latest security techniques and procedures and social engineering tactics and defenses within seven business days of hire and annually thereafter.

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 quarterly 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.

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).

F. Components of the System

Infrastructure

CU* BASE

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.

Network Services

CU*Answers Network Services maintains a highly available network infrastructure utilizing:

- Redundant internet connections via fiber backbones
- Multiple ISPs to provide divergent routes to the internet

- Redundant border gateway firewalls with Layer 7 security and integrated intrusion prevention and optionally available redundant load-balancing hardware for high availability applications
- Real-time failover
- Traffic load-balancing over multiple servers
- Custom traffic directing rules to support any web-enabled application as well as an available SSL (Secure Sockets Layer) accelerator hardware to improve performance of secure web applications

CU*Answers Network Services' network has been engineered for virtualized technologies. CU*Answers Network Services cloud computing infrastructure leverages highly scalable SAN technologies with select virtualization technologies to provide a flexible and secure managed storage and compute services environment.

Software

The following applications assist in the performance of the CU*BASE System and Network Management Services:

Primary Software	Function
Fortinet	Client firewalls and firewall backups
Kaseya	Windows patching
Nagios	Network monitoring
TrendMicro	Anti-virus
SonicWall	Internal firewalls
VMWare	Virtual machines
ConnectWise	Ticketing system
iTera Echo2	Replication for iSeries
Arctic Wolf	Internal network monitoring
BitLocker	Device encryption

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

- Operations Team - Responsible for the completeness, timeliness, and accuracy of data utilized by clients. Also, performs maintenance of iSeries systems and backups.
- Client Interaction and Support Area Team - Responsible for responding to client inquiries, developing education tools, writing documentation, and monitoring the effective operations of all of the software applications. Also, includes the Imaging Solutions Team.

Data

CU* BASE

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

Network Services

The Network Management Services System is responsible for client hardware, network configurations, and communications containing sensitive financial information.

Procedures

Logical Security

An access request process exists for Active Directory that is used to document management authorization and approval of new user accounts. The requests are approved by HR or employee's manager and are submitted through an access form to the IT staff. An access request process exists for iSeries that are used to document management authorization and approval of new user accounts. Internal users are approved by CU*Answers management and external users are approved by client management. The requests are submitted through an access form to the IT staff for internal and external users.

An individual data library exists for each credit union. External users are restricted to their organization's specific data library. Credit unions have the ability to define sensitive access restrictions based on security profile configurations for the users.

Active Directory access for terminated employees is removed from the system within one business day of termination by IT staff. The ability to access iSeries 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. User access reviews to ensure terminated employees' access to the network has been disabled are performed by Internal Audit and reported to the Board of Directors on a quarterly basis.

Administrative access to iSeries and Active Directory is restricted to IT personnel based on job responsibilities.

The following password parameters are in place for Active Directory:
-Minimum Length: 12 Characters
-Complexity: Enabled
-Max Age: 365 days
-History: 24 Passwords
-Lockout Threshold: 10 Attempts
-Inactivity Timeout: 10 Minutes

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

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 documented within Internal Audit's report and reported to the Board of Directors.

Asset Management

An asset inventory is manually maintained by the Network Services Team. Newly provisioned and decommissioned devices are tracked in real time within the asset inventory. A server and workstation baseline configuration checklist is in place to provision new servers and workstations. The checklist is utilized by the Network Services Team and manually updated as needed.

Antivirus software is installed on production servers and client servers managed by the Network Services Team. All systems are configured such that real-time scanning is performed and tamper protection is enabled. Daily, the Network Services Team monitors that antivirus definitions are up-to-date and real time scanning is active. Windows patches for client production systems are monitored daily by the Network Services Team and patches are installed as necessary.

Removable media use is restricted for all devices. Exceptions are manually reviewed by the HR and updated by the Network Services Team via exception request form.

Network Monitoring

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. Stateful firewalls have been implemented to monitor and segregate client networks from each other and control traffic between networks. Each security domain is documented and consists of a subnet of addresses as determined by network administrators. Firewall administrators are restricted to IT personnel based on their job responsibilities. The Network Services Team monitors the health and security of managed services clients' systems by performing daily checks using runsheets. Issues are tracked to resolution within the ticketing system. The firewall logs suspicious and unauthorized access attempts. The Network Services Team reviews these logs on a daily basis.

Arctic Wolf monitors the internal network and sends alerts to the Operations Support Specialist 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. Production system logs are configured to record specified system events. The logs are reviewed by the Network Services Team as part of the daily checklist. The Network Services Team monitors the health and security of internal network systems by performing daily checks using runsheets. Issues are tracked to resolution within the ticketing system.

Encryption

Data communication lines are internet dedicated lines and are secured using VPN tunnels. Data is transmitted securely between the host and client application. Laptops are encrypted via BitLocker. Backup tapes are encrypted via AES-256.

Physical Security

Access to the facilities is restricted via key fob. Physical access is approved by HR and documented within the onboarding checklist. Physical access is removed within one business day and is documented within the offboarding checklist. Visitors to the facilities are required to sign-in and are issued a visitor badge upon arrival. 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. Security cameras are in place at all in-scope facilities to monitor facility entrances, data centers, and network closets. Camera footage is retained for at least 90 days.

Internal Audit reports document quarterly physical access reviews. Internal Audit reports any physical access violations to the Board of Directors at least quarterly.

Systems Operations

A third-party vendor performs an external penetration test of the company's external network security infrastructure on an annual basis. Management reviews the results of testing and determines a plan for remediation. Results of testing and the remediation plan are monitored by the Board of Directors.

Internal vulnerability scans are completed on a quarterly basis. Findings are tracked within ConnectWise and remediated by the Network Services Team.

An Incident Response Plan is in place within the Policy Manual documenting the process for identifying, investigating, remediating, and recovering from a security incident. Security events are identified through multiple sources including network monitoring software and daily reviews. Security events are investigated by the Internal Audit Team, documented within the Internal Audit reports, and remediated as necessary. Security incidents are investigated by the Internal Audit Team and documented within the Internal Audit reports. A root cause analysis and lessons learned are documented as part of the remediation process.

Change Management

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

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. Access to source code stored on the production 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.

All program changes are required to be authorized, tested, and documented (including design, development and configuration information) within a project tracking ticket. Custom client requests require an acceptance letter from the credit union requesting the change prior to release. New server operating system versions for servers are authorized by Network Services Team prior to implementation.

The Programming 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. The Programming Team meets quarterly with senior leadership to review the inventory of projects and ensure they are in alignment with the business plan.

Production, development, and quality control environments are physically segregated within the environment.

Risk Mitigation

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

A formal vendor management program is in place 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 relating to security, availability, confidentiality, processing integrity, and privacy objectives, is performed to mitigate and manage risks. Executive management performs an annual vendor management review for critical vendors that covers the following:
- Access to NPPI
- Risk Dimensions
- Physical Access
- Inherent Risk Level
- Tier Level
- Residual Risk Level

A cyber insurance policy is in place.

Availability

Production iSeries systems are monitored daily by the Network Services Team 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. iSeries hardware is maintained under contract with the vendor.

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

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

Files are backed up daily and replicated to redundant systems at the offsite location. Backups are monitored daily by the Operations Team. All mission critical database servers are replicated to the secured servers at the offsite facility throughout the day. Backup performance is reviewed daily by the Network Services Team. Client firewall configurations are backed up on a daily basis.

Confidentiality

File retention procedures have been established and documented in the Policy Manual and Business Continuity Plan. Internal Audit tests compliance of the retention procedures as part of the annual audit. In accordance with policies and procedures, employees are instructed to dispose of confidential records via shred bins located throughout the facility. The shred bins are locked and are only accessible by Facilities Management and a third-party service organization that comes onsite and securely destroys the records on a regular basis. The third-party provides the organization with certification that records have been shredded securely and in accordance with the service agreement.

A checklist for decommissioning equipment is required to be completed by the Network Services Team, in accordance with policies and procedures, prior to the discontinuation of logical or physical protections of organizational assets. Electronic devices are destroyed and/or data is erased prior to disposal. The Client Interaction and Support Area Team maintains a log for electronic data removals. The log details the client data libraries that are deleted due to mergers or deconversions.

Processing Integrity

The Operations Team utilizes a daily runsheet for processing. The runsheet is reviewed by an Operations supervisor for completeness. Procedures are documented in the 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. Processing exceptions are documented within the runsheets. The Operations supervisors review and resolve identified issues on a daily basis. For incoming ACH transactions, totals from FEDLINE are compared to system totals prior to processing by Operations. The comparison is documented within the runsheet. 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 the Network Services Team. 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.

Privacy

CU*Answers maintains a security policy 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. Unauthorized disclosures are investigated by the Internal Audit Team and documented within the Internal Audit reports. For vendors with access to personal information, a contract that includes privacy service commitments is signed and in place. Inquiries, complaints, and disputes are responded to by the General Counsel and Director of Internal Audit. Those that are identified will be documented to resolution within the Internal Audit reports.

G. Applicable Trust Service Criteria and Related Controls

The Company's applicable trust services criteria, and the related controls designed to provide reasonable assurance that the service organization's service commitments and system requirements 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 applicable trust services criteria 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.

H. Complementary User Entity Controls

Management of CU*Answers assumed, in the design of CU*Answers' CU*BASE System and Network Management Services 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' service commitments and system requirements would be achieved. These complementary user entity controls and the related trust services criteria 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. (PI1.2)
- Balance system generated general ledger entries to reconcile the general ledger interface against the member trial balance. (PI1.3)
- Balance application totals to the independently posted general ledger to verify the overall accuracy of the daily processing results. (PI1.4)

I. 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:

- 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.
- 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.
- Manage employee access to system features, as well as all key parameter configurations. Credit unions are responsible for removing access for employees.
- 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.
- 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.
- Test program changes after general release to verify results areas published.
- Make privacy policies available to members which outline the rights and responsibilities with regard to personal data and review and update such policies periodically.
- Communicate choices regarding the collection of personal information, obtain explicit consent where applicable, and track member opt-in/opt-out with respect to the use of their data.
- Manage changes in member data through tools provided within CU*BASE. Depending on the credit union's configuration, members may be able to update their own information through online banking.
- Review changes made to member information, and whom has been accessing or modifying this information through tools provided within CU*BASE.
- Track and manage member complaints, including responding to requests for personal information help, periodically monitoring compliance with privacy requirements, as well as making decisions regarding notifications and services desired by the membership through the tracker system provided within CU*BASE.
- CU*Answers Network Management Services customers are responsible for authorizing employees that are allowed physical access to the CU*Answers Network Services facility and responsible for communicating this list to CU*Answers Network Services.
- CU*Answers Network Management Services customers are responsible for reporting to CU*Answers Network Services any changes in key contacts for communication purposes or terminations of employees who have been granted access to the facility.
- CU*Answers Network Management Services customers are responsible for establishing communications to the data center facility systems and for ensuring that redundant lines for backup communications exist.
- CU*Answers Network Management Services customers are responsible for ensuring that their network infrastructure deployed at CU*Answers Network Services provides an appropriate level of resiliency and redundancy.
- CU*Answers Network Management Services customers are responsible for designing their applications and systems to ensure they can be adequately supported given the Service Delivery Intervals outlined in the Description of Controls section of this document.

SECTION 4. TRUST SERVICES CRITERIA AND 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 applicable trust services categories and criteria specified by the management of CU*Answers.
- The controls established and specified by CU*Answers to achieve the specified service commitments and system requirements based on the applicable trust services criteria.

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 service commitments and system requirements based on the applicable trust services criteria were achieved based on the applicable trust services criteria. 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.

A. Common Criteria

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
1.0	**Common Criteria related to Control Environment**		
1.1	The entity demonstrates a commitment to integrity and ethical values.		
	1. 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. The Employee Handbook and Policy Manual were designed to be reviewed and approved outside the reporting period. Therefore, there were no circumstances that warranted the performance of the control.	Inspected the Employee Handbook and Policy Manual to determine that internal control policies and procedures are described.	No deviations noted.
		The Employee Handbook and Policy Manual were designed to be reviewed and approved outside the reporting period. Accordingly, no testing to determine review and approval occurred during the reporting period was performed by us. Inspected the Employee Handbook and Policy Manual to determine that while it was performed outside of the reporting period, they were reviewed and approved within the last two years.	Not applicable.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	2. 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 reporting period. Therefore, there were no circumstances that warranted re-acknowledgement by all employees.	Inspected signoff forms for a sample of new employees during the reporting period to determine the employee handbook and policy manual was acknowledged upon hire.	No deviations noted.
		There were no major updates to the Employee Handbook and Policy Manual during the reporting period. Accordingly, no testing of re-acknowledgement by all employees was performed by us. Inspected the Employee Handbook and Policy Manual and Board Meeting Minutes to determine there were no major updates during the reporting period.	Not applicable.
	3. Employee Annual Planning (EAP) is completed for employees by managers on an annual basis. EAP includes performance goals and adherence to company policies.	Inspected EAP completion for a sample of employees to determine it was completed by managers within the reporting period.	No deviations noted.
1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
	1. The Board of Directors is comprised of members independent from management. The Board meets no less than quarterly to monitor the development and performance of internal controls.	Inspected Board of Director meeting minutes to determine the current Board of Directors members are independent from management.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
		Inspected Board of Director meeting minutes for a sample of quarters to determine the Board of Directors is responsible for the development and performance of internal controls.	No deviations noted.
1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
	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 the Board of Directors and executive management.	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 and executive management during the reporting 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.
1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
	1. New employee qualifications are evaluated by HR or the hiring manager prior to hire.	Inspected interview notes for a sample of new employees to determine they were evaluated prior to hire.	No deviations noted.
	2. 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 the background screening was completed prior to hire.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	3. Employees complete security awareness training within seven business days of orientation and annually thereafter.	Inspected security awareness training completion for a sample of new hires to determine it was completed within seven business days of orientation.	No deviations noted.
		Inspected security awareness training completion for a sample of employees to determine it was completed within the reporting period.	No deviations noted.
	4. Employee Annual Planning (EAP) is completed for employees by managers on an annual basis. EAP includes performance goals and adherence to company policies.	Inspected EAP completion for a sample of employees to determine it was completed by managers within the reporting period.	No deviations noted.
1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
	1. Employee Annual Planning (EAP) is completed for employees by managers on an annual basis. EAP includes performance goals and adherence to company policies.	Inspected EAP completion for a sample of employees to determine it was completed by managers within the reporting period.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
2.0	**Common Criteria related to Communication and Information**		
2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
	1. A risk assessment is performed annually by the Internal Audit Team. The risk assessment is reviewed annually and as-needed by the Board of Directors. The risk assessment documents the following items: •Action plans to mitigate deficiencies identified for internal controls •Resource allocation, timing, and the desired outcomes •Likelihood •Impact •Mitigating controls, including preventative, detective, automatic, and manual controls •Risk ratings •Business owners •Risks related to Fraud •Changes affecting internal controls •Risk of using inaccurate or incomplete data	Inspected the risk assessment and risk assessment review to determine it is performed annually by the Internal Audit Team and reviewed by the Board of Directors within the reporting period.	No deviations noted.
		Inspected the risk assessment to determine the items stated in the control description are documented.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
	1. 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 reporting period. Therefore, there were no circumstances that warranted re-acknowledgement by all employees.	Inspected signoff forms for a sample of new employees during the reporting period to determine the employee handbook and policy manual was acknowledged upon hire.	No deviations noted.
		There were no major updates to the Employee Handbook and Policy Manual during the reporting period. Accordingly, no testing of re-acknowledgement by all employees was performed by us. Inspected the Employee Handbook and Policy Manual and Board Meeting Minutes to determine there were no major updates during the reporting period.	Not applicable.
	2. Employees complete security awareness training within seven business days of orientation and annually thereafter.	Inspected security awareness training completion for a sample of new hires to determine it was completed within seven business days of orientation.	No deviations noted.
		Inspected security awareness training completion for a sample of employees to determine it was completed within the reporting period.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	3. 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. The security policy was designed to be reviewed and approved outside the reporting period. Therefore, there were no circumstances that warranted the performance of the control.	Inspected the security policy and company website to determine 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.
		The security policy was designed to be reviewed and approved outside the reporting period. Accordingly, no testing to determine review and approval occurred during the reporting period was performed by us. Inspected the security policy and inquired with the Internal Auditor to determine that while it was performed outside of the reporting period, it was reviewed and approved within the last two years.	Not applicable.
2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.		
	1. Product descriptions and information concerning product functionality and boundaries are listed in the online user help manuals which provide internal and external personnel specific guidance to carry out those responsibilities.	Inspected online user help manuals to determine documentation regarding products and services are available to users.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	2. Commitments are communicated to new clients via formal contracts, including security, confidentiality, availability, processing integrity, and privacy commitments and user responsibilities.	Inspected customer contracts for a sample of new clients during the reporting period to determine responsibilities listed in the control description are communicated.	No deviations noted.
	3. The system is configured to provide monitoring reports to the managed services clients via email. Reports are automatically generated and delivered by the firewall management reporting servers, on a daily, weekly, and/or monthly basis. Procedures are in place to verify that reports have been generated.	Inspected network services checklists for a sample of managed services clients and days to determine client firewall reports were successfully generated and confirmed to be available to clients.	No deviations noted.
3.0	**Common Criteria related to Risk Assessment**		
3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
	1. Management has a formal Business Plan, including a Strategic Technology Plan, to define the company's overall objectives and how it plans to meet such goals. The plan is reviewed and approved by the Board of Directors annually.	Inspected the Business Plan to determine that the plan included a defined Strategic Technology Plan.	No deviations noted.
		Inspected the Business Plan to determine that the plan had been reviewed and approved by the Board of Directors within the reporting period.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
	1. A risk assessment is performed annually by the Internal Audit Team. The risk assessment is reviewed annually and as-needed by the Board of Directors. The risk assessment documents the following items: •Action plans to mitigate deficiencies identified for internal controls •Resource allocation, timing, and the desired outcomes •Likelihood •Impact •Mitigating controls, including preventative, detective, automatic, and manual controls •Risk ratings •Business owners •Risks related to Fraud •Changes affecting internal controls •Risk of using inaccurate or incomplete data	Inspected the risk assessment and risk assessment review to determine it is performed annually by the Internal Audit Team and reviewed by the Board of Directors within the reporting period.	No deviations noted.
		Inspected the risk assessment to determine the items stated in the control description are documented.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
	1. A risk assessment is performed annually by the Internal Audit Team. The risk assessment is reviewed annually and as-needed by the Board of Directors. The risk assessment documents the following items: •Action plans to mitigate deficiencies identified for internal controls •Resource allocation, timing, and the desired outcomes •Likelihood •Impact •Mitigating controls, including preventative, detective, automatic, and manual controls •Risk ratings •Business owners •Risks related to Fraud •Changes affecting internal controls •Risk of using inaccurate or incomplete data	Inspected the risk assessment and risk assessment review to determine it is performed annually by the Internal Audit Team and reviewed by the Board of Directors within the reporting period.	No deviations noted.
		Inspected the risk assessment to determine the items stated in the control description are documented.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.		
	1. A risk assessment is performed annually by the Internal Audit Team. The risk assessment is reviewed annually and as-needed by the Board of Directors. The risk assessment documents the following items: •Action plans to mitigate deficiencies identified for internal controls •Resource allocation, timing, and the desired outcomes •Likelihood •Impact •Mitigating controls, including preventative, detective, automatic, and manual controls •Risk ratings •Business owners •Risks related to Fraud •Changes affecting internal controls •Risk of using inaccurate or incomplete data	Inspected the risk assessment and risk assessment review to determine it is performed annually by the Internal Audit Team and reviewed by the Board of Directors within the reporting period.	No deviations noted.
		Inspected the risk assessment to determine the items stated in the control description are documented.	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 to determine the plan was updated, reviewed by executive management, and approved by the Board of Directors within the reporting period.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
4.0	**Common Criteria related to Monitoring Activities**		
4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
	1. A risk assessment is performed annually by the Internal Audit Team. The risk assessment is reviewed annually and as-needed by the Board of Directors. The risk assessment documents the following items: •Action plans to mitigate deficiencies identified for internal controls •Resource allocation, timing, and the desired outcomes •Likelihood •Impact •Mitigating controls, including preventative, detective, automatic, and manual controls •Risk ratings •Business owners •Risks related to Fraud •Changes affecting internal controls •Risk of using inaccurate or incomplete data	Inspected the risk assessment and risk assessment review to determine it is performed annually by the Internal Audit Team and reviewed by the Board of Directors within the reporting period.	No deviations noted.
		Inspected the risk assessment to determine the items stated in the control description are documented.	No deviations noted.
	2. 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 for a sample of quarters to determine internal control testing occurred and results were presented to management and the Board of Directors and tracked until remediation.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	3. 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 documented within Internal Audit's report and reported to the Board of Directors.	Inspected iSeries reports for a sample of days to determine the reports were reviewed by Internal Audit and any issues identified were escalated and documented within Internal Audit's report to the Board of Directors.	No deviations noted.
	4. A third-party vendor performs an external penetration test of the company's external network security infrastructure on an annual basis. Management reviews the results of testing and determines a plan for remediation. Results of testing and the remediation plan are monitored by the Board of Directors.	Inspected the external penetration test to determine it was performed within the reporting period.	No deviations noted.
		Inspected the Internal Audit close out report to determine management and the Board of Directors reviewed the penetration test and addressed plans for remediation.	No deviations noted.
	5. Internal vulnerability scans are completed on a quarterly basis. Findings are tracked within ConnectWise and remediated by the Network Services Team.	Inspected the vulnerability scan schedule to determine that internal vulnerability scans are performed quarterly.	No deviations noted.
		Performed an observation of the vulnerability remediation process with the Network Services Team to determine that tickets are tracked within ConnectWise and remediated by the Network Services Team.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.		
	1. A risk assessment is performed annually by the Internal Audit Team. The risk assessment is reviewed annually and as-needed by the Board of Directors. The risk assessment documents the following items: •Action plans to mitigate deficiencies identified for internal controls •Resource allocation, timing, and the desired outcomes •Likelihood •Impact •Mitigating controls, including preventative, detective, automatic, and manual controls •Risk ratings •Business owners •Risks related to Fraud •Changes affecting internal controls •Risk of using inaccurate or incomplete data	Inspected the risk assessment and risk assessment review to determine it is performed annually by the Internal Audit Team and reviewed by the Board of Directors within the reporting period.	No deviations noted.
		Inspected the risk assessment to determine the items stated in the control description are documented.	No deviations noted.
	2. 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 for a sample of quarters to determine internal control testing occurred and results were presented to management and the Board of Directors and tracked until remediation.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	3. A third-party vendor performs an external penetration test of the company's external network security infrastructure on an annual basis. Management reviews the results of testing and determines a plan for remediation. Results of testing and the remediation plan are monitored by the Board of Directors.	Inspected the external penetration test to determine it was performed within the reporting period.	No deviations noted.
		Inspected the Internal Audit close out report to determine management and the Board of Directors reviewed the penetration test and addressed plans for remediation.	No deviations noted.
	4. Internal vulnerability scans are completed on a quarterly basis. Findings are tracked within ConnectWise and remediated by the Network Services Team.	Inspected the vulnerability scan schedule to determine that internal vulnerability scans are performed quarterly.	No deviations noted.
		Performed an observation of the vulnerability remediation process with the Network Services Team to determine that tickets are tracked within ConnectWise and remediated by the Network Services Team.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
5.0	**Common Criteria related to Control Activities**		
5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
	1. A risk assessment is performed annually by the Internal Audit Team. The risk assessment is reviewed annually and as-needed by the Board of Directors. The risk assessment documents the following items: •Action plans to mitigate deficiencies identified for internal controls •Resource allocation, timing, and the desired outcomes •Likelihood •Impact •Mitigating controls, including preventative, detective, automatic, and manual controls •Risk ratings •Business owners •Risks related to Fraud •Changes affecting internal controls •Risk of using inaccurate or incomplete data	Inspected the risk assessment and risk assessment review to determine it is performed annually by the Internal Audit Team and reviewed by the Board of Directors within the reporting period.	No deviations noted.
		Inspected the risk assessment to determine the items stated in the control description are documented.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.		
	1. A risk assessment is performed annually by the Internal Audit Team. The risk assessment is reviewed annually and as-needed by the Board of Directors. The risk assessment documents the following items: •Action plans to mitigate deficiencies identified for internal controls •Resource allocation, timing, and the desired outcomes •Likelihood •Impact •Mitigating controls, including preventative, detective, automatic, and manual controls •Risk ratings •Business owners •Risks related to Fraud •Changes affecting internal controls •Risk of using inaccurate or incomplete data	Inspected the risk assessment and risk assessment review to determine it is performed annually by the Internal Audit Team and reviewed by the Board of Directors within the reporting period.	No deviations noted.
		Inspected the risk assessment to determine the items stated in the control description are documented.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
	1. 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. The security policy was designed to be reviewed and approved outside the reporting period. Therefore, there were no circumstances that warranted the performance of the control.	Inspected the security policy and company website to determine 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.
		The security policy was designed to be reviewed and approved outside the reporting period. Accordingly, no testing to determine review and approval occurred during the reporting period was performed by us. Inspected the security policy and inquired with the Internal Auditor to determine that while it was performed outside of the reporting period, it was reviewed and approved within the last two years.	Not applicable.
6.0	**Common Criteria related to Logical and Physical Access Controls**		
6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
	1. An asset inventory is manually maintained by the Network Services Team. Newly provisioned and decommissioned devices are tracked in real time within the asset inventory.	Performed an observation with the VP of Network Infrastructure to determine that the asset inventory is maintained by the Network Services Team and updated in real time.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	2. Administrative access to iSeries and Active Directory is restricted to IT personnel based on job responsibilities.	Inspected the listing of Active Directory and iSeries administrators to determine access is restricted based on job responsibilities.	No deviations noted.
	3. The following password parameters are in place for Active Directory: -Minimum Length: 12 Characters -Complexity: Enabled -Max Age: 365 days -History: 24 Passwords -Lockout Threshold: 10 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.
	4. The following password parameters are in place to authenticate into the CU*BASE application: -Minimum Length: 8 Characters -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.
	5. An individual data library exists for each credit union. External users are restricted to their organization's specific data library. Credit unions have the ability to define sensitive access restrictions based on security profile configurations for the users.	Inspected system configuration settings to determine security profiles are utilized to restrict user access within the system.	No deviations noted.
		Inspected data libraries for a sample of new clients to determine individual data libraries are in place for each credit union.	No deviations noted.
	6. Firewall administrators are restricted to IT personnel based on their job responsibilities.	Inspected the firewall administrator listing for the internal and external firewalls to determine that access was restricted to IT personnel.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	7. 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 reporting period.	No deviations noted.
6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
	1. An individual data library exists for each credit union. External users are restricted to their organization's specific data library. Credit unions have the ability to define sensitive access restrictions based on security profile configurations for the users.	Inspected system configuration settings to determine security profiles are utilized to restrict user access within the system.	No deviations noted.
		Inspected data libraries for a sample of new clients to determine individual data libraries are in place for each credit union.	No deviations noted.
	2. An access request process exists for Active Directory that is used to document management authorization and approval of new user accounts. The requests are approved by HR or employee's manager and are submitted through an access form to the IT staff.	Inspected access request forms for a sample of new Active Directory user accounts added during the reporting period to determine the access request process is documented and approved by HR or the employee's manager.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	3. An access request process exists for iSeries that are used to document management authorization and approval of new user accounts. Internal users are approved by CU*Answers management and external users are approved by client management. 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 reporting period to determine the access request process is documented and approved.	No deviations noted.
	4. 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.	No deviations noted.
		Inspected user listings for a sample of terminated employees to determine the account was removed or disabled.	No deviations noted.
	5. The ability to access iSeries 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 the ability to access iSeries was removed within one business day of termination.	No deviations noted.
		Inspected iSeries configurations settings to determine iSeries accounts are automatically disabled after 92 days of inactivity.	No deviations noted.
	6. User access reviews to ensure terminated employees' access to the network has been disabled are performed by Internal Audit and reported to the Board of Directors on a quarterly basis.	Inspected Internal Audit report results for a sample of quarters to determine a review of terminated employees' access was performed and reported to the Board of Directors.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	7. 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 documented within Internal Audit's report and reported to the Board of Directors.	Inspected iSeries reports for a sample of days to determine the reports were reviewed by Internal Audit and any issues identified were escalated and documented within Internal Audit's report to the Board of Directors.	No deviations noted.
6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
	1. An individual data library exists for each credit union. External users are restricted to their organization's specific data library. Credit unions have the ability to define sensitive access restrictions based on security profile configurations for the users.	Inspected system configuration settings to determine security profiles are utilized to restrict user access within the system.	No deviations noted.
		Inspected data libraries for a sample of new clients to determine individual data libraries are in place for each credit union.	No deviations noted.
	2. An access request process exists for Active Directory that is used to document management authorization and approval of new user accounts. The requests are approved by HR or employee's manager and are submitted through an access form to the IT staff.	Inspected access request forms for a sample of new Active Directory user accounts added during the reporting period to determine the access request process is documented and approved by HR or the employee's manager.	No deviations noted.
	3. An access request process exists for iSeries that are used to document management authorization and approval of new user accounts. Internal users are approved by CU*Answers management and external users are approved by client management. 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 reporting period to determine the access request process is documented and approved.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	4. 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.	No deviations noted.
		Inspected user listings for a sample of terminated employees to determine the account was removed or disabled.	No deviations noted.
	5. The ability to access iSeries 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 the ability to access iSeries was removed within one business day of termination.	No deviations noted.
		Inspected iSeries configurations settings to determine iSeries accounts are automatically disabled after 92 days of inactivity.	No deviations noted.
	6. User access reviews to ensure terminated employees' access to the network has been disabled are performed by Internal Audit and reported to the Board of Directors on a quarterly basis.	Inspected Internal Audit report results for a sample of quarters to determine a review of terminated employees' access was performed and reported to the Board of Directors.	No deviations noted.
	7. 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 documented within Internal Audit's report and reported to the Board of Directors.	Inspected iSeries reports for a sample of days to determine the reports were reviewed by Internal Audit and any issues identified were escalated and documented within Internal Audit's report to the Board of Directors.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
	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 job titles for a sample 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. Security cameras are in place at all in-scope facilities to monitor facility entrances, data centers, and network closets. Camera footage is retained for at least 90 days.	Performed an observation of the security cameras at all in-scope facilities to determine cameras are in place.	No deviations noted.
		Inspected security camera settings to determine footage is retained for at least 90 days.	No deviations noted.
	4. 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.
	5. Physical access is approved by HR and documented within the onboarding checklist.	Inspected the onboarding checklist for a sample of new employees to determine physical access was approved.	No deviations noted.
	6. Physical access is removed within one business day and is documented within the offboarding checklist.	Inspected the offboarding checklist for a sample of terminated employees to determine physical access was removed within one business day.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	7. Internal Audit reports document quarterly physical access reviews.	Inspected Internal Audit reports for a sample of quarters to determine quarterly physical access reviews are documented.	No deviations noted.
	8. 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.
6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.		
	1. File retention procedures have been established and documented in the Policy Manual and Business Continuity Plan. Internal Audit tests compliance of the retention procedures as part of the annual audit.	Inspected the Policy Manual and Business Continuity Plan to determine that file retention procedures have been established and are documented.	No deviations noted.
		Inspected Internal Audit close out report to determine that Internal Audit tests compliance of the retention procedures as part of the annual audit.	No deviations noted.
	2. A checklist for decommissioning equipment is required to be completed by the Network Services Team, in accordance with policies and procedures, prior to the discontinuation of logical or physical protections of organizational assets. Electronic devices are destroyed and/or data is erased prior to disposal.	Inspected the checklist for a sample of decommissioned devices to determine they were destroyed and/or data was erased prior to disposal.	No deviations noted.
	3. The Client Interaction and Support Area Team maintains a log for electronic data removals. The log details the client data libraries that are deleted due to mergers or deconversions.	Inspected the deconversion log and performed an inquiry with the VP of Client Interactions to determine the log is in place and documents the deletion of client data libraries.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
	1. 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.
	2. The firewall logs suspicious and unauthorized access attempts. The Network Services Team reviews these logs on a daily basis.	Inspected network services checklists for a sample of days to determine the firewall logs and critical events were reviewed.	No deviations noted.
	3. Arctic Wolf monitors the internal network and sends alerts to the Operations Support Specialist 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 Operations Support Specialist 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.
	4. Production system logs are configured to record specified system events. The logs are reviewed by the Network Services Team as part of the daily checklist.	Inspected network services checklists for a sample of days to determine system logs were reviewed for specified system events by the Network Services Team.	No deviations noted.
	5. The Network Services Team monitors the health and security of internal network systems by performing daily checks using runsheets. Issues are tracked to resolution within the ticketing system.	Inspected network services checklists for a sample of days to determine internal network systems were monitored and noted issues were resolved by the Network Services Team.	No deviations noted.
	6. Stateful firewalls have been implemented to monitor and segregate client networks from each other and control traffic between networks. Each security domain is documented and consists of a subnet of addresses as determined by network administrators.	Inspected firewall configurations for a sample of managed client firewalls to determine network security zones were implemented and rules are in place to segregate client networks and control traffic.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	7. The Network Services Team monitors the health and security of managed services clients' systems by performing daily checks using runsheets. Issues are tracked to resolution within the ticketing system.	Inspected ticket history of network services daily checklists for a sample of managed services clients and days and inspected exception response procedures to determine client system health and security monitoring was performed.	No deviations noted.
	8. Firewall administrators are restricted to IT personnel based on their job responsibilities.	Inspected the firewall administrator listing for the internal and external firewalls to determine that access was restricted to IT personnel.	No deviations noted.
6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		
	1. Data communication lines are internet dedicated lines and are secured using VPN tunnels.	Inspected network diagrams within the Business Continuity Plan to determine they document VPN 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.
	2. Data is transmitted securely between the host and client application.	Inspected the encryption certificate chain for connections to the host to determine data is transmitted securely.	No deviations noted.
	3. Laptops are encrypted via BitLocker.	Inspected encryption screenshots for a sample of laptops to determine laptops are encrypted via BitLocker.	No deviations noted.
	4. Backup tapes are encrypted via AES-256.	Inspected encryption settings to determine that backup tapes are encrypted.	No deviations noted.
	5. Removable media use is restricted for all devices. Exceptions are manually reviewed by the HR and updated by the Network Services Team via exception request form.	Inspected antivirus configuration settings to determine that use of removable media is restricted.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
		Performed an observation of the removable media exception process with the Sr. Internal Auditor to determine exceptions are reviewed by the HR and implemented by the Network Services Team.	No deviations noted.
6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
	1. Antivirus software is installed on production servers and client servers managed by the Network Services Team. All systems are configured such that real-time scanning is performed and tamper protection is enabled. Daily, the Network Services Team monitors that antivirus definitions are up-to-date and real time scanning is active.	Inspected global anti-virus configurations to determine systems are configured for real-time scanning and has tamper protections in place.	No deviations noted.
		Inspected ticket history of network services daily checklists for a sample of managed services clients and days to determine antivirus monitoring was completed.	No deviations noted.
	2. Windows patches for client production systems are monitored daily by the Network Services Team and patches are installed as necessary.	Inspected ticket history of Network Services daily checklists for a sample of days and inspected patch monitoring procedures to determine server patch monitoring and installation was completed.	No deviations noted.
7.0	**Common Criteria related to System Operations**		
7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		
	1. Production system logs are configured to record specified system events. The logs are reviewed by the Network Services Team as part of the daily checklist.	Inspected network services checklists for a sample of days to determine system logs were reviewed for specified system events by the Network Services Team.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	2. The Network Services Team monitors the health and security of internal network systems by performing daily checks using runsheets. Issues are tracked to resolution within the ticketing system.	Inspected network services checklists for a sample of days to determine internal network systems were monitored and noted issues were resolved by the Network Services Team.	No deviations noted.
	3. The Network Services Team monitors the health and security of managed services clients' systems by performing daily checks using runsheets. Issues are tracked to resolution within the ticketing system.	Inspected ticket history of network services daily checklists for a sample of managed services clients and days and inspected exception response procedures to determine client system health and security monitoring was performed.	No deviations noted.
	4. A server and workstation baseline configuration checklist is in place to provision new servers and workstations. The checklist is utilized by the Network Services Team and manually updated as needed.	Inspected the baseline configuration checklists and performed an inquiry with the VP of Network Infrastructure to determine configurations are in place and utilized by the Network Services Team.	No deviations noted.
	5. A third-party vendor performs an external penetration test of the company's external network security infrastructure on an annual basis. Management reviews the results of testing and determines a plan for remediation. Results of testing and the remediation plan are monitored by the Board of Directors.	Inspected the external penetration test to determine it was performed within the reporting period.	No deviations noted.
		Inspected the Internal Audit close out report to determine management and the Board of Directors reviewed the penetration test and addressed plans for remediation.	No deviations noted.
	6. Internal vulnerability scans are completed on a quarterly basis. Findings are tracked within ConnectWise and remediated by the Network Services Team.	Inspected the vulnerability scan schedule to determine that internal vulnerability scans are performed quarterly.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
		Performed an observation of the vulnerability remediation process with the Network Services Team to determine that tickets are tracked within ConnectWise and remediated by the Network Services Team.	No deviations noted.
7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
	1. The firewall logs suspicious and unauthorized access attempts. The Network Services Team reviews these logs on a daily basis.	Inspected network services checklists for a sample of days to determine the firewall logs and critical events were reviewed.	No deviations noted.
	2. Arctic Wolf monitors the internal network and sends alerts to the Operations Support Specialist 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 Operations Support Specialist 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.
	3. Production system logs are configured to record specified system events. The logs are reviewed by the Network Services Team as part of the daily checklist.	Inspected network services checklists for a sample of days to determine system logs were reviewed for specified system events by the Network Services Team.	No deviations noted.
	4. The Network Services Team monitors the health and security of internal network systems by performing daily checks using runsheets. Issues are tracked to resolution within the ticketing system.	Inspected network services checklists for a sample of days to determine internal network systems were monitored and noted issues were resolved by the Network Services Team.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	5. The Network Services Team monitors the health and security of managed services clients' systems by performing daily checks using runsheets. Issues are tracked to resolution within the ticketing system.	Inspected ticket history of network services daily checklists for a sample of managed services clients and days and inspected exception response procedures to determine client system health and security monitoring was performed.	No deviations noted.
	6. A third-party vendor performs an external penetration test of the company's external network security infrastructure on an annual basis. Management reviews the results of testing and determines a plan for remediation. Results of testing and the remediation plan are monitored by the Board of Directors.	Inspected the external penetration test to determine it was performed within the reporting period.	No deviations noted.
		Inspected the Internal Audit close out report to determine management and the Board of Directors reviewed the penetration test and addressed plans for remediation.	No deviations noted.
	7. Internal vulnerability scans are completed on a quarterly basis. Findings are tracked within ConnectWise and remediated by the Network Services Team.	Inspected the vulnerability scan schedule to determine that internal vulnerability scans are performed quarterly.	No deviations noted.
		Performed an observation of the vulnerability remediation process with the Network Services Team to determine that tickets are tracked within ConnectWise and remediated by the Network Services Team.	No deviations noted.
7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		
	1. An Incident Response Plan is in place within the Policy Manual documenting the process for identifying, investigating, remediating, and recovering from a security incident.	Inspected the Incident Response Plan within the Policy Manual to determine it contains the items noted within the description.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	2. Security events are identified through multiple sources including network monitoring software and daily reviews. Security events are investigated by the Internal Audit Team, documented within the Internal Audit reports, and remediated as necessary.	Inspected Internal Audit reports to determine security events are investigated by the Internal Audit Team, documented, and remediated.	No deviations noted.
7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
	1. An Incident Response Plan is in place within the Policy Manual documenting the process for identifying, investigating, remediating, and recovering from a security incident.	Inspected the Incident Response Plan within the Policy Manual to determine it contains the items noted within the description.	No deviations noted.
	2. Security incidents are investigated by the Internal Audit Team and documented within the Internal Audit reports. A root cause analysis and lessons learned are documented as part of the remediation process.	Selected a sample of security incidents and inspected internal audit reports to determine the event was investigated and documented.	No deviations noted.
7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.		
	1. An Incident Response Plan is in place within the Policy Manual documenting the process for identifying, investigating, remediating, and recovering from a security incident.	Inspected the Incident Response Plan within the Policy Manual to determine it contains the items noted within the description.	No deviations noted.
	2. Security incidents are investigated by the Internal Audit Team and documented within the Internal Audit reports. A root cause analysis and lessons learned are documented as part of the remediation process.	Selected a sample of security incidents and inspected internal audit reports to determine the event was investigated and documented.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
8.0	**Common Criteria related to Change Management**		
8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		
	1. 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 reporting period.	No deviations noted.
	2. 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.
	3. Custom client requests require an acceptance letter from the credit union requesting the change prior to release.	Inspected acceptance letters for a sample of custom client requests to verify approvals were provided by the client prior to release.	No deviations noted.
	4. The Programming 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.	Inspected meeting minutes for a sample of months to determine the Programming Team discussed the status of projects, took actions in response to identified issues, and approved changes for production.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	5. System development and change control policies have been created to formally direct system modifications. The policies are updated, reviewed, and approved by the Programming Team 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 they address system modification and change control processes.	No deviations noted.
		Inspected meeting minutes to determine the Software Development Life Cycle (SDLC) is updated, reviewed, and approved by management and the Board of Directors within the reporting period.	No deviations noted.
	6. New server operating system versions for servers are authorized by Network Services management prior to implementation.	Inspected approvals for a sample of new operating system versions implemented for servers to determine they were authorized by Network Services management prior to implementation.	No deviations noted.
	7. Production, development, and quality control environments are physically segregated within the environment.	Inspected iSeries environments to determine that the production, development, and quality control environments are segregated.	No deviations noted.
	8. Access to source code stored on the production 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 reporting period.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	9. The Programming Team meets quarterly with senior leadership to review the inventory of projects and ensure they are in alignment with the business plan.	Inspected programming meeting minutes for a sample of quarters to determine senior management and the Programming Team discuss project alignment with business goals and documented actions to take in response.	No deviations noted.
	10. 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 documented within Internal Audit's report and reported to the Board of Directors.	Inspected iSeries reports for a sample of days to determine the reports were reviewed by Internal Audit and any issues identified were escalated and documented within Internal Audit's report to the Board of Directors.	No deviations noted.
9.0	**Common Criteria related to Risk Mitigation**		
9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
	1. A cyber insurance policy is in place.	Inspected cyber insurance policy to determine it is in place and covers the reporting period.	No deviations noted.
	2. CU*Answers has a formal written Business Continuity 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 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.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
9.2	The entity assesses and manages risks associated with vendors and business partners.		
	1. A formal vendor management program is in place 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 relating to security, availability, confidentiality, processing integrity, and privacy objectives, 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 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. Executive management performs an annual vendor management review for critical vendors that covers the following: - Access to NPPI - Risk Dimensions - Physical Access - Inherent Risk Level - Tier Level - Residual Risk Level	Inspected the vendor management review for a sample of critical vendors to determine it includes the items as noted in the control description.	No deviations noted.

B. Availability

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
1.0	**Additional Criteria for Availability**		
1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.		
	1. Production iSeries systems are monitored daily by the Network Services Team 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 production iSeries systems were monitored daily by the Network Services Team.	No deviations noted.
1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.		
	1. 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.
	2. 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.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
		Inspected the contract for the alarm vendor to determine the fire and smoke detection system is monitored.	No deviations noted.
	3. CU*Answers has a hot-site agreement to provide equipment and facilities backup should the in-scope facilities be destroyed or rendered inoperable.	Inspected hot-site agreement to determine equipment and backup facility requirements are defined and included for use if a disaster occurs.	No deviations noted.
	4. iSeries hardware is maintained under contract with the vendor.	Inspected the vendor contract to determine it includes iSeries hardware maintenance coverage.	No deviations noted.
	5. Files are backed up daily and replicated to redundant systems at the offsite location. Backups are monitored daily by the Operations Team.	Inspected the backup runsheets for a sample of days to determine daily iSeries file backup and replication tasks were completed.	No deviations noted.
	6. All mission critical database servers are replicated to the secured servers at the offsite facility throughout the day. Backup performance is reviewed daily by the Network Services Team.	Inspected network services checklists for a sample of days to determine daily database server backup tasks were completed.	No deviations noted.
	7. Client firewall configurations are backed up on a daily basis.	Inspected a sample of client firewall configurations to determine the configurations were backed up on a daily basis.	No deviations noted.
1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
	1. CU*Answers has a formal written Business Continuity 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 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.

C. Confidentiality

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
1.0	**Additional Criteria for Confidentiality**		
1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
	1. File retention procedures have been established and documented in the Policy Manual and Business Continuity Plan. Internal Audit tests compliance of the retention procedures as part of the annual audit.	Inspected the Policy Manual and Business Continuity Plan to determine that file retention procedures have been established and are documented.	No deviations noted.
		Inspected Internal Audit close out report to determine that Internal Audit tests compliance of the retention procedures as part of the annual audit.	No deviations noted.
1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
	1. In accordance with policies and procedures, employees are instructed to dispose of confidential records via shred bins located throughout the facility. The shred bins are locked and are only accessible by Facilities Management and a third-party service organization that comes onsite and securely destroys the records on a regular basis. The third-party provides the organization with certification that records have been shredded securely and in accordance with the service agreement.	Inspected Policy Manual to determine that employees are instructed to dispose of confidential records via shred bins.	No deviations noted.
		Observed that shred bins are locked and inspected the agreement with third-party to determine it defines the process to securely destroy contents of the shred bins.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
		Inspected invoices from the third-party service organization providing shredding services for a sample of months to determine that the third-party comes onsite and securely destroys the records on a weekly basis, in accordance with the service agreement.	No deviations noted.
	2. A checklist for decommissioning equipment is required to be completed by the Network Services Team, in accordance with policies and procedures, prior to the discontinuation of logical or physical protections of organizational assets. Electronic devices are destroyed and/or data is erased prior to disposal.	Inspected the checklist for a sample of decommissioned devices to determine they were destroyed and/or data was erased prior to disposal.	No deviations noted.
	3. The Client Interaction and Support Area Team maintains a log for electronic data removals. The log details the client data libraries that are deleted due to mergers or deconversions.	Inspected the deconversion log and performed an inquiry with the VP of Client Interactions to determine the log is in place and documents the deletion of client data libraries.	No deviations noted.

D. Processing Integrity

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
1.0	**Additional Criteria related to Processing Integrity**		
1.1	The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.		
	1. Product descriptions and information concerning product functionality and boundaries are listed in the online user help manuals which provide internal and external personnel specific guidance to carry out those responsibilities.	Inspected online user help manuals to determine documentation regarding products and services are available to users.	No deviations noted.
	2. Commitments are communicated to new clients via formal contracts, including security, confidentiality, availability, processing integrity, and privacy commitments and user responsibilities.	Inspected customer contracts for a sample of new clients during the reporting period to determine responsibilities listed in the control description are communicated.	No deviations noted.
	3. Procedures are documented in the runsheet for job processing streams with sequential processing required so that prior processing steps are completed before proceeding with the next processing step.	Inspected runsheets for a sample of days to determine processing steps are outlined and executed sequentially.	No deviations noted.
1.2	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.		
	1. The Operations Team 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 an Operations supervisor acknowledged completeness of each day's runsheet.	No deviations noted.
	2. For incoming ACH transactions, totals from FEDLINE are compared to system totals prior to processing by Operations. The comparison is documented within the runsheet.	Inspected runsheets for a sample of days to determine ACH totals from FEDLINE were compared with system totals prior to processing.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
1.3	The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.		
	1. Procedures are documented in the runsheet for job processing streams with sequential processing required so that prior processing steps are completed before proceeding with the next processing step.	Inspected runsheets for a sample of days to determine processing steps are outlined and executed sequentially.	No deviations noted.
	2. 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 the Network Services Team.	Inspected network services checklists for a sample of days to determine hardware errors during processing are monitored, investigated and resolved by the Network Services Team.	No deviations noted.
	3. Processing exceptions are documented within the runsheets. The Operations supervisors review and resolve identified issues on a daily basis.	Inspected runsheets for a sample of days to determine an Operations supervisor reviewed the processing exceptions log and noted issues were resolved.	No deviations noted.
	4. 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 runsheets for a sample of days to determine restart/rerun procedures were followed and issues resolved if an abnormal termination occurred by Operations.	No deviations noted.
1.4	The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.		
	1. 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 runsheets for a sample of days to determine the daily report import process successfully executed and identified issues were resolved by the Imaging Solutions Team.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
1.5	The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.		
	1. Files are backed up daily and replicated to redundant systems at the offsite location. Backups are monitored daily by the Operations Team.	Inspected the backup runsheets for a sample of days to determine daily iSeries file backup and replication tasks were completed.	No deviations noted.

E. Privacy

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
1.0	**Privacy Criteria related to Notice and Communication**		
1.1	The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.		
	Not applicable. CU*Answers does not collect personal information directly from or communicate directly with data subjects; this is the responsibility of the credit unions.		
2.0	**Privacy Criteria related to Choice and Consent**		
2.1	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.		
	Not applicable. CU*Answers does not collect personal information directly from or communicate directly with data subjects; this is the responsibility of the credit unions.		
3.0	**Privacy Criteria related to Collection**		
3.1	Personal information is collected consistent with the entity's objectives related to privacy.		
	1. Commitments are communicated to new clients via formal contracts, including security, confidentiality, availability, processing integrity, and privacy commitments and user responsibilities.	Inspected customer contracts for a sample of new clients during the reporting period to determine responsibilities listed in the control description are communicated.	No deviations noted.
	2. CU*Answers maintains a security policy 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 that it contains the elements noted within the control description.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
3.2	For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.		
	Not applicable. CU*Answers does not collect personal information directly from or obtain explicit consent from data subjects; this is the responsibility of the credit unions.		
4.0	**Privacy Criteria related to Use, Retention, Disposal**		
4.1	The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.		
	1. Commitments are communicated to new clients via formal contracts, including security, confidentiality, availability, processing integrity, and privacy commitments and user responsibilities.	Inspected customer contracts for a sample of new clients during the reporting period to determine responsibilities listed in the control description are communicated.	No deviations noted.
	2. CU*Answers maintains a security policy 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 that it contains the elements noted within the control description.	No deviations noted.
4.2	The entity retains personal information consistent with the entity's objectives related to privacy.		
	1. An access request process exists for Active Directory that is used to document management authorization and approval of new user accounts. The requests are approved by HR or employee's manager and are submitted through an access form to the IT staff.	Inspected access request forms for a sample of new Active Directory user accounts added during the reporting period to determine the access request process is documented and approved by HR or the employee's manager.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	2. An access request process exists for iSeries that are used to document management authorization and approval of new user accounts. Internal users are approved by CU*Answers management and external users are approved by client management. 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 reporting period to determine the access request process is documented and approved.	No deviations noted.
	3. 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.	No deviations noted.
		Inspected user listings for a sample of terminated employees to determine the account was removed or disabled.	No deviations noted.
	4. The ability to access iSeries 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 the ability to access iSeries was removed within one business day of termination.	No deviations noted.
		Inspected iSeries configurations settings to determine iSeries accounts are automatically disabled after 92 days of inactivity.	No deviations noted.
	5. User access reviews to ensure terminated employees' access to the network has been disabled are performed by Internal Audit and reported to the Board of Directors on a quarterly basis.	Inspected Internal Audit report results for a sample of quarters to determine a review of terminated employees' access was performed and reported to the Board of Directors.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	6. 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 documented within Internal Audit's report and reported to the Board of Directors.	Inspected iSeries reports for a sample of days to determine the reports were reviewed by Internal Audit and any issues identified were escalated and documented within Internal Audit's report to the Board of Directors.	No deviations noted.
	7. File retention procedures have been established and documented in the Policy Manual and Business Continuity Plan. Internal Audit tests compliance of the retention procedures as part of the annual audit.	Inspected the Policy Manual and Business Continuity Plan to determine that file retention procedures have been established and are documented.	No deviations noted.
		Inspected Internal Audit close out report to determine that Internal Audit tests compliance of the retention procedures as part of the annual audit.	No deviations noted.
4.3	The entity securely disposes of personal information to meet the entity's objectives related to privacy.		
	1. In accordance with policies and procedures, employees are instructed to dispose of confidential records via shred bins located throughout the facility. The shred bins are locked and are only accessible by Facilities Management and a third-party service organization that comes onsite and securely destroys the records on a regular basis. The third-party provides the organization with certification that records have been shredded securely and in accordance with the service agreement.	Inspected Policy Manual to determine that employees are instructed to dispose of confidential records via shred bins.	No deviations noted.
		Observed that shred bins are locked and inspected the agreement with third-party to determine it defines the process to securely destroy contents of the shred bins.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
		Inspected invoices from the third-party service organization providing shredding services for a sample of months to determine that the third-party comes onsite and securely destroys the records on a weekly basis, in accordance with the service agreement.	No deviations noted.
	2. A checklist for decommissioning equipment is required to be completed by the Network Services Team, in accordance with policies and procedures, prior to the discontinuation of logical or physical protections of organizational assets. Electronic devices are destroyed and/or data is erased prior to disposal.	Inspected the checklist for a sample of decommissioned devices to determine they were destroyed and/or data was erased prior to disposal.	No deviations noted.
5.0	**Privacy Criteria related to Access**		
5.1	The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.		
	Not applicable. Credit unions are responsible for providing the data subjects with access to their information and notifying CU*Answers of any data changes.		
5.2	The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.		
	Not applicable. Credit unions are responsible for providing the data subjects with access to their information and notifying CU*Answers of any data changes.		

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
6.0	**Privacy Criteria related to Disclosure and Notification**		
6.1	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.		
	Partially not applicable. CU*Answers does not collect personal information directly from or obtain explicit consent from data subjects; this is the responsibility of the credit unions.		
	1. For vendors with access to personal information, a contract that includes privacy service commitments is signed and in place.	Inspected contracts in place for a sample of new vendors with access to personal information to determine they are signed and define privacy service commitments.	No deviations noted.
6.2	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.		
	1. Executive management performs an annual vendor management review for critical vendors that covers the following: - Access to NPPI - Risk Dimensions - Physical Access - Inherent Risk Level - Tier Level - Residual Risk Level	Inspected the vendor management review for a sample of critical vendors to determine it includes the items as noted in the control description.	No deviations noted.
	2. For vendors with access to personal information, a contract that includes privacy service commitments is signed and in place.	Inspected contracts in place for a sample of new vendors with access to personal information to determine they are signed and define privacy service commitments.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
6.3	The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.		
	1. Unauthorized disclosures are investigated by the Internal Audit Team and documented within the Internal Audit reports. There were no unauthorized disclosures during the reporting period. Therefore, there were no circumstances that warranted the performance of the control.	There were no circumstances that warranted the performance of the control. Accordingly, no testing was performed by us. Inspected the Internal Audit reports and performed an inquiry with the Internal Auditor to determine there were no unauthorized disclosures during the reporting period.	Not applicable.
6.4	The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.		
	1. A formal vendor management program is in place 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 relating to security, availability, confidentiality, processing integrity, and privacy objectives, 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 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.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
6.5	The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.		
	1. An Incident Response Plan is in place within the Policy Manual documenting the process for identifying, investigating, remediating, and recovering from a security incident.	Inspected the Incident Response Plan within the Policy Manual to determine it contains the items noted within the description.	No deviations noted.
	2. A formal vendor management program is in place 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 relating to security, availability, confidentiality, processing integrity, and privacy objectives, 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 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.
6.6	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.		
	1. An Incident Response Plan is in place within the Policy Manual documenting the process for identifying, investigating, remediating, and recovering from a security incident.	Inspected the Incident Response Plan within the Policy Manual to determine it contains the items noted within the description.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	2. Unauthorized disclosures are investigated by the Internal Audit Team and documented within the Internal Audit reports. There were no unauthorized disclosures during the reporting period. Therefore, there were no circumstances that warranted the performance of the control.	There were no circumstances that warranted the performance of the control. Accordingly, no testing was performed by us. Inspected the Internal Audit reports and performed an inquiry with the Internal Auditor to determine there were no unauthorized disclosures during the reporting period.	Not applicable.
6.7	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objective related to privacy.		
	Not applicable. CU*Answers is not responsible for providing an account to data subjects of personal information held and disclosed; this is the responsibility of the credit unions.		
7.0	**Privacy Criteria related to Quality**		
7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.		
	Partially not applicable. CU*Answers does not collect personal information directly from or communicate directly with data subjects; this is the responsibility of the credit unions.		
	1. An access request process exists for Active Directory that is used to document management authorization and approval of new user accounts. The requests are approved by HR or employee's manager and are submitted through an access form to the IT staff.	Inspected access request forms for a sample of new Active Directory user accounts added during the reporting period to determine the access request process is documented and approved by HR or the employee's manager.	No deviations noted.
	2. An access request process exists for iSeries that are used to document management authorization and approval of new user accounts. Internal users are approved by CU*Answers management and external users are approved by client management. 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 reporting period to determine the access request process is documented and approved.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	3. 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.	No deviations noted.
		Inspected user listings for a sample of terminated employees to determine the account was removed or disabled.	No deviations noted.
	4. The ability to access iSeries 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 the ability to access iSeries was removed within one business day of termination.	No deviations noted.
		Inspected iSeries configurations settings to determine iSeries accounts are automatically disabled after 92 days of inactivity.	No deviations noted.
	5. User access reviews to ensure terminated employees' access to the network has been disabled are performed by Internal Audit and reported to the Board of Directors on a quarterly basis.	Inspected Internal Audit report results for a sample of quarters to determine a review of terminated employees' access was performed and reported to the Board of Directors.	No deviations noted.
	6. 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 documented within Internal Audit's report and reported to the Board of Directors.	Inspected iSeries reports for a sample of days to determine the reports were reviewed by Internal Audit and any issues identified were escalated and documented within Internal Audit's report to the Board of Directors.	No deviations noted.

Criteria	Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
8.0	**Privacy Criteria related to Monitoring and Enforcement**		
8.1	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.		
	Partially not applicable. Communication with data subjects is the responsibility of the credit unions. Receiving, addressing, resolving, and communicating to others is the responsibility of CU*Answers.		
	1. 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 for a sample of quarters to determine internal control testing occurred and results were presented to management and the Board of Directors and tracked until remediation.	No deviations noted.
	2. Inquiries, complaints, and disputes are responded to by the General Counsel and Director of Internal Audit. Those that are identified will be documented to resolution within the Internal Audit reports. There were no inquiries, complaints, and disputes identified during the reporting period. Therefore, there were no circumstances that warranted documentation of resolution.	Performed an observation of the process for responding to inquiries, complaints, and disputes to determine they are responded to by the General Counsel and Director of Internal Audit and documented within the Internal Audit reports.	No deviations noted.
		There were no inquiries, complaints, and disputes identified during the period. Accordingly, no testing of documentation of resolution was performed by us. Inspected the Internal Audit reports and performed an inquiry with the Internal Auditor to determine there were no inquiries, complaints, and disputes during the reporting period.	Not applicable.

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

For more information regarding the report, contact:

Patrick Sickels | General Counsel and Director of Internal Audit
CU*Answers, Inc.
616.285.5711 x335
psickels@cuanswers.com

For more information on Plante Moran, contact:

Sarah Pavelek | Partner
Plante Moran
248.223.3891
sarah.pavelek@plantemoran.com