



# CU\*Answers, Inc.

## SOC 1 Type 2 Report

---

Report on the Network Management Services System throughout the period October 1, 2022 to September 30, 2023

---

# Contents

<b>Section 1.</b>	<b>Independent Service Auditor's Report</b>	2
<b>Section 2.</b>	<b>CU*Answers, Inc. Management's Assertion</b>	5
<b>Section 3.</b>	<b>CU*Answers, Inc.'s Description of its Network Management Services System</b>	
	A. Company Overview	7
	B. Scope of Report	8
	C. Entity Level Management Processes	8
	D. Components of the System	10
	E. Control Objectives and Related Controls	13
	F. User Entity Responsibilities	13
<b>Section 4.</b>	<b>Control Objectives, CU*Answers, Inc.'s Description of Related Controls and Service Auditor's Description of Tests of Controls and Results</b>	15
<b>Section 5.</b>	<b>Other Information Provided by Management of CU*Answers, Inc.</b>	27

## Independent Service Auditor's Report

To Management  
CU\*Answers, Inc.

### Scope

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

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

### Service Organization's Responsibilities

In Section 2 of this report, CU\*Answers' management has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. CU\*Answers' management is responsible for preparing the description and the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; selecting the criteria stated in the assertion; and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

### Service Auditor's Responsibilities

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

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period October 1, 2022 to September 30, 2023. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

To Management  
CU\*Answers, Inc.

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

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

#### ***Service Auditor's Independence and Quality Control***

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

#### ***Inherent Limitations***

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

#### ***Description of Tests of Controls***

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

#### ***Opinion***

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

- The description fairly presents the information technology general control system for the Network Management Services System that was designed and implemented throughout the period October 1, 2022 to September 30, 2023.
- The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2022 to September 30, 2023.
- The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2022 to September 30, 2023.

To Management  
CU\*Answers, Inc.

***Restricted Use***

This report, including the description of tests of controls and results thereof in Section 4 of this report, is intended solely for the information and use of management of CU\*Answers; user entities of the information technology general control system for the Network Management Services System throughout the period October 1, 2022 to September 30, 2023; and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risk of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than those specified parties.

*Plante & Moran, PLLC*

May 10, 2024



May 10, 2024

Plante & Moran, PLLC

To Service Auditors:

We have prepared the description of CU\*Answers, Inc.'s (CU\*Answers) information technology general control system entitled, "CU\*Answers, Inc.'s Description of its Network Management Services System" throughout the period October 1, 2022 to September 30, 2023 (description), and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves when assessing the risks of material misstatement of user entities' financial statements.

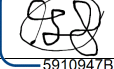
We confirm, to the best of our knowledge and belief, that:

- a. The description fairly presents the information technology general control system made available to user entities of the system for user entities of the system during some or all of the period October 1, 2022 to September 30, 2023 as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:
  - i. Presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable
    - 1) the types of services provided, including as appropriate, the classes of transactions processed; the types of services provided;
    - 2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system;
    - 3) how the system captures and addresses significant events and conditions other than transactions;
    - 4) the process used to prepare reports and other information for user entities;
    - 5) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them;
    - 6) the specified control objectives and controls designed to achieve those objectives and control objectives that are specified by law, regulation, or another party; and
    - 7) other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring activities that are relevant to the services provided to user entities of the system.
  - ii. includes relevant details of changes to the service organization's system during the period covered by the description.
  - iii. does not omit or distort information relevant to the system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the information technology

general control system that each individual user entity of the system and its auditor may consider important in its own particular environment.

- b. The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period October 1, 2022 to September 30, 2023 to achieve those control objectives. The criteria we used in making this assertion were that:
- i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the management of the service organization.
  - ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved
  - iii. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Very truly yours,

  
5910947BA06F416...

Geoff Johnson, Chief Executive Officer

---

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

### A. Company Overview

---

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

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

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

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

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

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

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

**Principle 6: Cooperation Among Cooperatives** - CU\*Answers serves members most effectively and strengthens 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

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 24x7 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 covers the CU\*Answers Network Management Services System as it relates to the network connectivity of clients to their hosted resources, as well as monitoring of client networks in accordance with contracts between the clients and CU\*Answers.

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

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

## Significant Changes in the System and Controls

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

## Subsequent Events

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

## C. Entity Level Management Processes

---

### Control Environment

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

### Organizational Structure

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

### Human Resources Policies and Practices

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

---

## Risk Assessment

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

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

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

## Information and Communication

### Policy, Standards, Procedures, and Guidelines

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

### Communication

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

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

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

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

---

## Training

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

## Monitoring

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

## Internal Audit

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

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

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

## D. Components of the System

---

### Infrastructure

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 Network Management Services System:

Application	Description
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

### People

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

- Board of Directors - The Board of Directors is comprised of members independent from management and are responsible for the development and performance of internal controls.
- Human Resources - Responsible for the organizational strategic planning, employee development, and the development and tracking of client interaction standards and expectations.
- Internal Audit - Responsible for providing assurance to management to ensure assets are safeguarded, internal controls are operating effectively, and compliance is maintained with prescribed laws and company policies.
- Network Services - Responsible for the performance of internal controls relating to the network, hardware, capacity, and patching. Also, provides external support of hardware, network configurations, and communications issues that arise from the performance of the in-scope applications.
- Programming Team - Responsible for the development and support of the in-scope applications.

### Data

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

---

## Procedures

### Organization and Administration

Upon hire and periodically upon update of the Employee Handbook and Policy Manual, employees are required to sign an Employee Acknowledgment Form acknowledging receipt and agreement to abide by the rules and conditions outlined in the Employee Handbook and Policy Manual.

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

### Communication with Clients

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

Client requests are tracked within a ticketing system and an authorized client contact is notified.

### Vendor Management

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

### Backup and Recovery Procedures

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

Client firewall configurations are backed up on a daily basis.

The service organization maintains current cyber insurance policies.

### Logical Access

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

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

The following password parameters are in place for the internal network:

- Minimum Length: 7 Characters
- Complexity: Enabled
- Max Age: 30 days
- History: 24 Passwords
- Lockout Threshold: 3 Attempts
- Inactivity Timeout: 10 minutes

Logical access to data is restricted to authorized administrators.

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

---

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

## Network Monitoring

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.

Windows patches for client production systems are monitored and installed by Network Services as outlined in the internal daily checklists.

Network Services monitors the health and security of managed client systems by performing daily checks using runsheets. Issues are tracked to resolution within the ticketing system.

Antivirus software is installed on CU\*Answers production servers and client servers managed by CU\*Answers. All systems are configured such that real-time scanning is performed and tamper protection is enabled. Daily, Network Services monitors that antivirus definitions are up-to-date and real time scanning is active.

The system is configured to provide monitoring reports to the client via email. Reports are automatically generated and delivered by our firewall management reporting servers, on a daily, weekly and/or monthly basis. Procedures are in place to verify that reports have been generated.

## Physical Security

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

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

Data centers are equipped with the following environmental controls:

- Heat and smoke detectors connected to a monitored alarm system
- Fire suppression/fire extinguishers
- Dedicated air conditioning units
- Uninterruptible Power Supply (UPS)
- Server Racks
- Temperature/Humidity Monitoring

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

## E. Control Objectives and Related Controls

---

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

## F. 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:

- CU\*Answers Network Management Services CU 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 securing ongoing maintenance and support contracts for all non-CU\*Answers Network Services-owned software and hardware.
  - 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 should have a business continuity plan in place to ensure that their system can be restored in the event of an unplanned disruption.
  - If CU\*Answers Network Services is not authorized to perform backups, controls should be established for the creation of backup tapes to ensure that important business data would be available to recover after a disaster.
  - 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 reviewing activity reports and security findings reports that are provided by CU\*Answers Network Services.
  - 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.
  - CU\*Answers Network Management Services customers are responsible for accompanying the "guests" that they bring into the CU\*Answers Network Services data center facility. These guests are also required to sign the visitors log and receive a badge to identify themselves.

---

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

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

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

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

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

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



# 1. Organization and Administration

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

**Description of Controls**

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

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
<p>5. Upon hire and periodically upon update of the Employee Handbook and Policy Manual, employees are required to sign an Employee Acknowledgment Form acknowledging receipt and agreement to abide by the rules and conditions outlined in the Employee Handbook and Policy Manual.</p> <p>There were no major updates to the Employee Handbook and Policy Manual during the period. Therefore, there were no circumstances that warranted the performance of the control.</p>	<p>Inspected signoff forms for a sample of new employees during the period to determine if the employee handbook and policy manual was acknowledged upon hire.</p> <hr/> <p>There were no instances of this control during the period. Therefore, there were no circumstances that warranted the performance of the control.</p> <p>Inspected the Employee Handbook and Policy Manual and Board Meeting Minutes to determine there were no major updates during the period.</p>	<p>No deviations noted.</p> <hr/> <p>Not applicable.</p>
<p>6. 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.</p>	<p>Inspected the security policy to determine if it addresses key elements pertaining to the protection of non-public personal information and is provided to both internal and external users.</p> <hr/> <p>Inspected meeting minutes to determine the security policy was reviewed and approved by executive management and the Board of Directors within the period.</p>	<p>No deviations noted.</p> <hr/> <p>No deviations noted.</p>

## 2. Communication with Clients

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

**Description of Controls**

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
1. Commitments are communicated to new clients via formal contracts, including confidentiality and privacy commitments and user responsibilities.	Inspected a sample of customer contracts for new clients during the period to determine if responsibilities, including confidentiality and privacy practices, are communicated.	No deviations noted.
2. Client requests are tracked within a ticketing system and an authorized client contact is notified.	Inspected a sample of client requests to determine if the request details were tracked within a ticketing system and closure notification was configured for sending to an authorized client contact.	No deviations noted.

### 3. Vendor Management

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

**Description of Controls**

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

## 4. Backup and Recovery Procedures

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

### Description of Controls

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
1. The service organization maintains current cyber insurance policies.	Inspected cyber insurance policy to determine it is in place and covers the period.	No deviations noted.
2. CU*Answers has a formal written contingency plan that addresses risks related to potential business disruptions. The plan is tested and documented by management at least annually.	Inspected the business continuity plan and documented testing results to determine if the plan addresses risks related to business disruptions.	No deviations noted.
	Inspected the results of the most recent business continuity plan test to determine testing is conducted annually.	No deviations noted.
3. Client firewall configurations are backed up on a daily basis.	Inspected a sample of client firewall configurations to determine if the configurations were backed up on a daily basis.	No deviations noted.

## 5. Logical Access

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

### Description of Controls

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
1. Logical access to data is restricted to authorized administrators.	Inspected the listing of Active Directory administrators to determine logical access to data is restricted to personnel requiring access based on their job responsibilities.	No deviations noted.
2. The following password parameters are in place for the internal network: -Minimum Length: 7 Characters -Complexity: Enabled -Max Age: 30 days -History: 24 Passwords -Lockout Threshold: 3 Attempts -Inactivity Timeout: 10 minutes	Inspected password parameters for Active Directory to determine it contains the items noted within the control description.	No deviations noted.
3. An access request process exists for AD that is used to document management authorization and approval of new user accounts. The requests are approved by HR or employee's manager and is submitted through an access form to the IT staff.	Inspected access request forms for a sample of new AD user accounts added during the period to determine the access request process is documented and approved by HR or the employee's manager.	No deviations noted.
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.	Deviations noted. CU*Answers could not demonstrate Active Directory access was disabled within one business day of termination for two out of 10 sampled terminated employees. CU*Answers provided evidence access was terminated after one business day of termination.

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
	Inspected user listings for a sample of terminated employees to determine access to Active Directory was removed by IT staff.	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 on a quarterly basis.	Inspected Internal Audit report results and selected a sample of quarters to determine a review of terminated employees access was performed and reported to the Board.	No deviations noted.
6. The firewall logs suspicious and unauthorized access attempts. Network Services personnel review these logs on a daily basis.	Inspected Network Services checklists for a sample of days to determine if firewall logs and critical events were reviewed.	No deviations noted.
7. 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.
8. ArcticWolf monitors the internal network and sends alerts to the Network Services Team related to intrusion prevention and malware. Critical events that require additional investigation are communicated via phone or email to the Network Services Team and are monitored and tracked to resolution.	Inspected the Arctic Wolf escalation procedures and performed an observation with the Network Services Team to determine Arctic Wolf monitors the internal network and the Network Services Team monitors and tracks the received security events until resolution.	No deviations noted.
9. Data is transmitted securely between the host and client application.	Inspected the encryption certificate chain for connections to the host to determine if data is transmitted securely.	No deviations noted.
10. Data communication lines are either internet or MPLS dedicated lines and secured using VPN tunnels.	Inspected network diagrams within the BCP to determine they document VPN or MPLS dedicated line utilization for client network connections.	No deviations noted.
	Inspected configurations for a sample of routers to determine VPN tunnels were established.	No deviations noted.

## 6. Physical Security

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

**Description of Controls**

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
1. Access to the facilities is restricted via key fob.	Performed an observation of the key fob system at all in-scope facilities to determine facility access is restricted via key fob.	No deviations noted.
2. Access to the data centers and network closets is restricted via the key fob system and is limited to personnel requiring access based on job responsibilities.	Performed an observation of in-scope data centers and network closets to determine access is restricted via key fob.	No deviations noted.
	Inspected a listing of users with access to in-scope data centers and network closets to determine access is restricted based on the individual's job responsibilities.	No deviations noted.
3. Data centers are equipped with the following environmental controls: <ul style="list-style-type: none"> <li>•Heat and smoke detectors connected to a monitored alarm system</li> <li>•Fire suppression/fire extinguishers</li> <li>•Dedicated air conditioning units</li> <li>•Uninterruptible Power Supply (UPS)</li> <li>•Server Racks</li> <li>•Temperature/Humidity Monitoring</li> </ul>	Performed an observation of the in-scope data centers to determine they are equipped with the items noted within the control description.	No deviations noted.
	Inspected the contract for the alarm vendor to determine the fire and smoke detection system is monitored.	No deviations noted.



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

## 7. Network Monitoring

**Control Objective:** Controls provide reasonable assurance that the risks of unauthorized access to the network are monitored and mitigated.

### Description of Controls

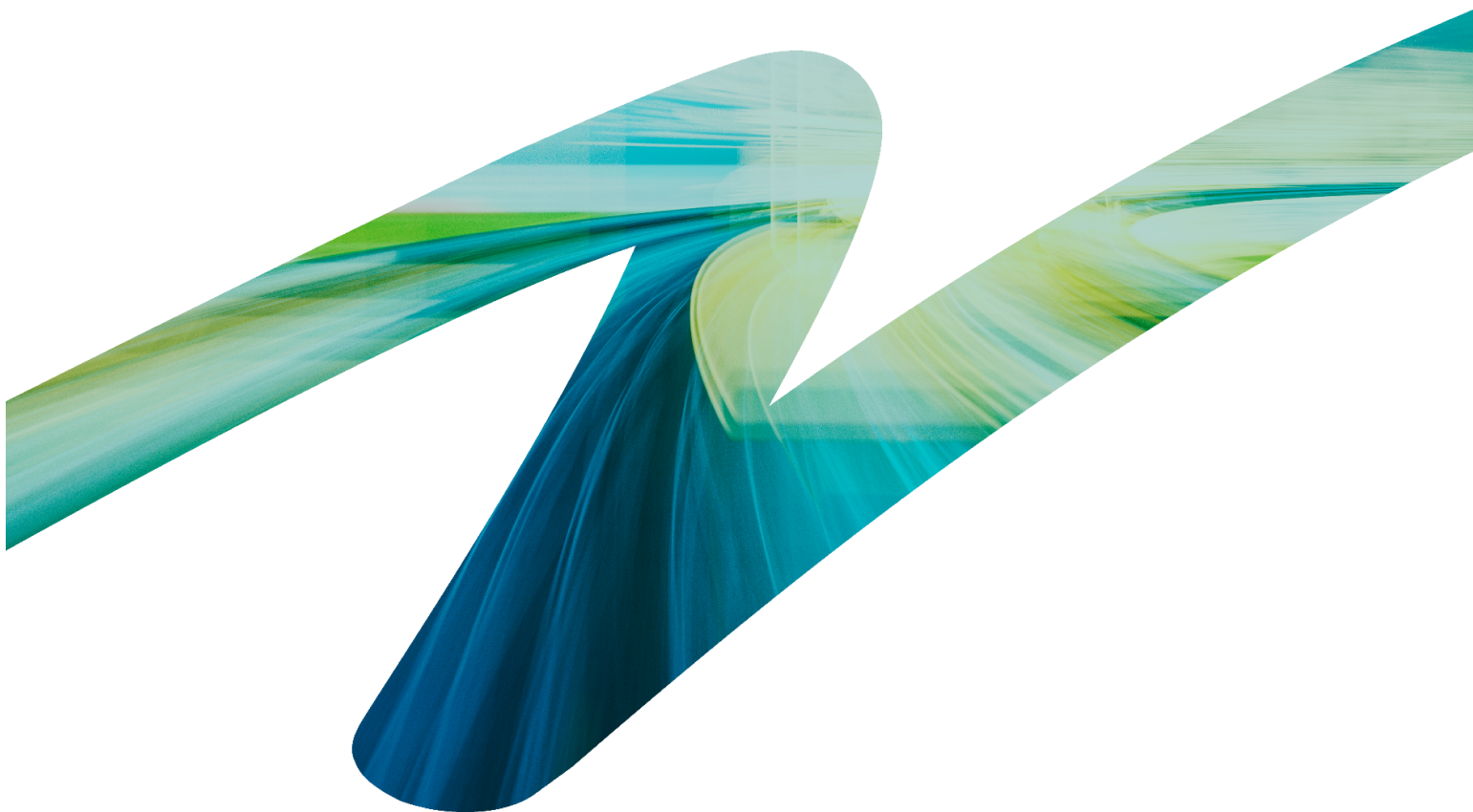
Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
<p>1. Stateful firewalls have been implemented to monitor and segregate client networks from each other and control traffic between networks. Each security domain is documented and consists of a subnet of addresses as determined by network administrators.</p>	<p>Inspected a sample of firewall configurations to determine if network security zones were implemented and rules are in place to segregate client networks and control traffic.</p>	<p>No deviations noted.</p>
<p>2. Windows patches for client production systems are monitored and installed by Network Services as outlined in the internal daily checklists.</p>	<p>Inspected ticket history of Network Services daily checklists for a sample of days and inspected patch monitoring procedures to determine if server patch monitoring and installation was completed.</p>	<p>No deviations noted.</p>
<p>3. Network Services monitors the health and security of managed client systems by performing daily checks using runsheets. Issues are tracked to resolution within the ticketing system.</p>	<p>Inspected ticket history of Network Services daily checklists for a sample of clients and days and inspected exception response procedures to determine if client system health and security monitoring was performed.</p>	<p>No deviations noted.</p>
<p>4. Antivirus software is installed on CU*Answers production servers and client servers managed by CU*Answers. All systems are configured such that real-time scanning is performed and tamper protection is enabled. Daily, Network Services monitors that antivirus definitions are up-to-date and real time scanning is active.</p>	<p>Inspected global anti-virus configurations to determine if systems are configured for real-time scanning and has tamper protections in place.</p>	<p>No deviations noted.</p>
	<p>Inspected ticket history of Network Services daily checklists for a sample of clients and days to determine if antivirus monitoring was completed.</p>	<p>No deviations noted.</p>

Controls Specified by CU*Answers	Testing Performed by Service Auditor	Results of Tests
<p>5. The system is configured to provide monitoring reports to the client via email. Reports are automatically generated and delivered by our firewall management reporting servers, on a daily, weekly and/or monthly basis. Procedures are in place to verify that reports have been generated.</p>	<p>Inspected Network Services checklists for a sample of clients and days to determine if client firewall reports were successfully generated and confirmed to be available to clients.</p>	<p>No deviations noted.</p>

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

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

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



**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