Crowe

Smart decisions. Lasting value.™

Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls

Related to the Network Management Services

Under the AICPA, Statement on Standards for Attestation Engagements No. 18 (SSAE No. 18) Related to Subject Matter AT-C 320 – Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting (SOC 1, Type 2)

For the Period July 1, 2017 to December 31, 2017

CU*ANSWERS
A Credit Union Service Organization

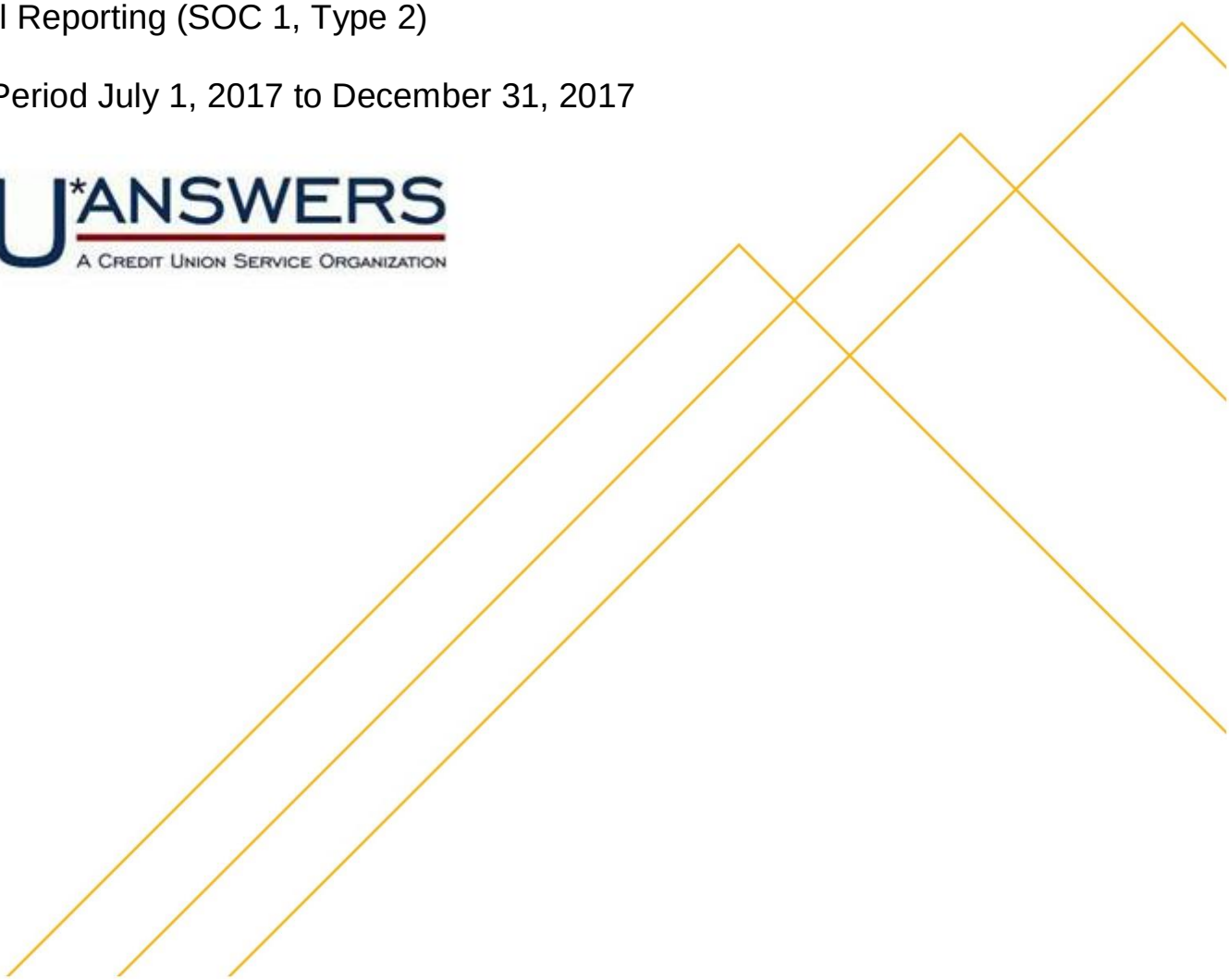


Table of Contents

SECTION I: Independent Service Auditor’s Report

INDEPENDENT SERVICE AUDITOR'S REPORT

To: CU*Answers, Inc.
Grand Rapids, Michigan

Scope

We have examined CU*Answers, Inc.'s (CU*Answers) description of its Network Management Services system entitled "CU*Answers' Description of Its Network Management Services" for processing user entities' transactions throughout the period July 1, 2017 to December 31, 2017 (description) and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "CU*Answers' Assertion" (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 Network Management Services system that are not likely to be relevant to user entities' internal control over financial reporting.

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

The information included in Section VI, "Other Information Provided by CU*Answers" is presented by management of CU*Answers to provide additional information and is not a part of CU*Answers' description of its Network Management Services system made available to user entities during the period July 1, 2017 to December 31, 2017. Information about CU*Answers' organizational model has not been subjected to the procedures applied in the examination of the description of 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 Network Management Services system.

Service Organization's Responsibilities

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

Service 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 July 1, 2017 to December 31, 2017. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

Inherent Limitations

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

Description of Tests of Controls

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

Opinion

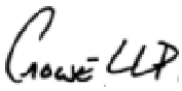
In our opinion, in all material respects, based on the criteria described in CU*Answers' assertion:

a. the description fairly presents the Network Management Services system that was designed and implemented throughout the period July 1, 2017 to December 31, 2017.
b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period July 1, 2017 to December 31, 2017 and user entities applied the complementary controls assumed in the design of CU*Answers' controls throughout the period July 1, 2017 to December 31, 2017.

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period July 1, 2017 to December 31, 2017 if complementary user entity controls assumed in the design of CU*Answers' controls operated effectively throughout the period July 1, 2017 to December 31, 2017.

Restricted Use

This report, including the description of tests of controls and results thereof in Section V, is intended solely for the information and use of management of CU*Answers, user entities of CU*Answers' Network Management Services system during some or all of the period July 1, 2017 to December 31, 2017, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than the specified parties.



Crowe LLP

South Bend, Indiana
June 22, 2018

SECTION II: CU*Answers, Inc.’s Management Assertion

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

June 22, 2018

To the Users of CU*Answers Network Management Services:

We have prepared the description of CU*Answers' network management services system entitled, "CU*Answers' Description of Its Network Management Services System," for processing user entities' transactions throughout the period July 1, 2017 to December 31, 2017 (description) for user entities of the system during some or all of the period July 1, 2017 to December 31, 2017, 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, when assessing the risks of material misstatement of user entities' financial statements.

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

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

a. the description fairly presents the Network Management Services system made available to user entities of the system during some or all of the period July 1, 2017 to December 31, 2017 for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description

   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.
      (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) the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
      (4) how the system captures and addresses significant events and conditions other than transactions.
      (5) the process used to prepare reports and other information for user entities.
      (6) the specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls.
      (7) other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

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

   iii. does not omit or distort information relevant to the service organization's system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the Network Management Services system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period July 1, 2017 to December 31, 2017 to achieve those control objectives if user entities applied the complementary controls assumed in the design of CU*Answers' controls throughout the period July 1, 2017 to December 31, 2017. The criteria we used in making this assertion were that:

   i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.
   ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.
   iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Sincerely:

Randy Karnes
Chief Executive Officer
CU*Answers, Inc.

Dave Wordhouse
VP Network Technologies
CU*Answers, Inc.

SECTION III: Description of Systems Provided by CU*Answers, Inc.

Overview of Operations

Ownership and Governance

CU*Answers, Inc., is a data processing service organization incorporated under Michigan law and chartered as a Credit Union Service Organization (CUSO), organized as a profit 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 over 120 credit unions, with more than 50 new owners since 2010. Each credit union owner owns 200 shares, no more nor less, and has one shareholder vote. There is no other private equity in CU*Answers. Each credit owner has 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.

Each year a Leadership Conference is held which provides clients a comprehensive project status review and highlights planning direction for CU*Answers in the coming year. The Annual Stockholder Meeting is held concurrently. Additionally, interactive client sessions and general meetings are scheduled periodically covering current topics of interest including data security. These meetings help assist CU*Answers' management in addressing the needs of the users.

Planning activities are ongoing and reviewed as a standard part of management meetings. Each department head provides input for CU*Answers management team's discussion topics. Examples of meeting topics discussed include client service review, conversion planning information, systems and operations topics, programming enhancements and modifications, and upcoming software release timing and education.

Cooperative Principles

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

Principle 1: Voluntary and Open Membership. Our organization is open to all entities able to use our services and willing to accept the responsibilities of membership.

Principle 2: Democratic Member Control. CU*Answers has democratic member control. Our members actively participate in setting our policies and making decisions. Our 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 our 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 our members. Our 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 our members, elected representatives, managers and employees so they can contribute effectively to the development of our 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 recognizes that we serve our 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 their communities through policies approved by our members.

CU*Answers 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 solutions provider specializing in:

- 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; and
- Web site engineering, server, storage, network, PC hardware sales and support services.

In addition to financial cooperatives, CU*Answers Network Services 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 has a nationwide network of clients with 24×7 real-time monitoring, including management of thousands of devices and hundreds of networks across the U.S.

CU*Answers Network Services also provides compliance expertise with policy development, implementation, and consulting services for highly regulated industries. It has expertise in implementation of proven high availability solutions for critical applications whether hosted at CU*Answers Network Services' state-of-the-art data center facilities or on-premise.

From network design to security consulting to a complete outsourcing of entire networks, CU*Answers Network Services has a solution for both credit unions and companies outside the credit union market. CU*Answers Network Services also provides an entire suite of products for web-based applications and hosting services.

Managed Hosting

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, and
- 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.

Technical Security

Maintaining system integrity and security is a top priority at CU*Answers Network Services. Significant effort is made in establishing and maintaining a secure facilities infrastructure. Therefore, CU*Answers Network Services implements security in a layered approach that includes at least the following:

- Secure network architecture designed by security experts.
- Systems segregated by task.
- Controlled physical access to data centers and systems.
- Controlled network access to all systems by enterprise-grade firewall and router systems.
- Technical filters control all outgoing and incoming network traffic to help prevent unauthorized use.
- Securing of the underlying operating system against known or possible attack by using the manufacturer's best practice recommendations.
- Disabling or removing unnecessary applications and services.
- Security review of applications for known vulnerabilities and configuration errors.
- Host-based intrusion detection: all access to the host system is logged and reviewed daily. As a method of verifying file integrity clients can opt to be sent daily emails that chronicle file level changes on the system to compare with work they did.
- Systems are patched monthly and kept up to date with the latest software updates.
- Network-based intrusion detection alerts administrators to attacks.
- Network-based intrusion prevention thwarts certain known attacks.
- Anti-virus systems scan network, host, and PC traffic and content in real time for virus activity. Pattern files are updated hourly.
- A proactively trained and alert staff on the latest security vulnerabilities and responses.

An additional security layer for all managed hosting customers is a dedicated CU*Answers Network Services managed firewall with a customized rule-set for the environment. Redundant highly-available firewalls are also available.

Physical Security

CU*Answers Network Services employs multi-level building access controls including:

- All guests must sign-in, wear visitor badges and be escorted at all times.
- Employees must use electronic security keys to enter main building, and various secure areas throughout the center.
- Access point activities are centrally logged and monitored.

- Video surveillance to DVR is used throughout the facilities to monitor activity.
- Access to computer room is controlled through key code panels or electronic security keys.
- Operators staff the production datacenter 24x7 and monitor secondary access.
- Only authorized employees are permitted access
- Employees who do not work in the datacenter are required to sign in and wear I.D. badges while in the facility

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 is regularly trained on the latest security techniques and procedures and social engineering tactics and defenses.

Network Backups

CU*Answers Network Services utilizes online network data backups, industry-standard data encryption, granular data recovery capabilities, nightly secure offsite backups to one of CU*Answers' data centers, data de-duplication and compression technology, and on-network virtualization technology.

The CU*Answers Network Services team also focuses on providing services to its client base. Network Solutions and Software Design members are added to the staff based on the combination of both their general technical skills and their understanding of the managed services industry. CU*Answers Network Services are also supported by accounting, marketing, and administration specialists that focus on their interest in the managed services industries and their unique disciplines to ensure that CU*Answers Network Services clients receive services that are in line with the best the market has to offer.

Complementary User Entity Controls

Certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of Answers' controls are suitably designed and operating effectively, along with related controls at the service organization. In Section IV, Complementary User Entity Controls are specific user controls, or issues each CU*Answers client should implement in order to achieve certain control objectives identified in this report. These considerations are not necessarily a comprehensive list of all internal accounting controls that should be employed by the customer, nor do they represent procedures that may be necessary in all circumstances.

General Controls

General Controls are those policies, procedures, and safeguards that relate to all Information Systems (IS) activities. They include Organization and Administration, Physical Security, Managed Hosting Services, Complete Care Management, Firewall Management Service and e-Business Policies and Procedures.

General Controls seek to ensure the continued, consistent, and proper functioning of information systems by controlling and protecting the maintenance of application software and the performance of computer operations. Because General Controls affect all IS activities, their adequacy is considered basic to the effectiveness of specific application controls. Furthermore, any weaknesses in General Controls can often have pervasive effects. It is important to understand the General Controls in evaluating controls over specific applications.

Organization and Administration

Controls provide reasonable assurance that CU*Answers Network Services and user functions are segregated.

CU*Answers Network Services is physically separate from and operates independently of the user institutions for which it provides Co-location and network management services. User organizations have contracts with CU*Answers Network Services that outline the responsibilities of both CU*Answers Network Services and the user organization. User personnel are only allowed in the computer room when accompanied by CU*Answers Network Services network personnel.

Controls provide reasonable assurance that policies and procedures exist to provide internal segregation of duties.

CU*Answers is organized into several functional groups including: Leadership, General Administration, Invention, Production, Capture Market Share, Client Interaction and Support, cuasterisk.com, Management Configuration, and Executive Council's Direct Reports. These functional groups provide internal segregation of duties.

All employees are provided with a variety of manuals that include procedures for the departments in which they work. An Employee Handbook is distributed to all new employees and all documentation is also provided to the employees via a CU*Answers hosted intranet. Further, the CEO of the company conducts several meetings during the year that include discussions concerning employee training, benefits, audit issues, goals and strategic plans, as well as other corporate issues. CU*BASE computer operators, network administrators, programmers, and customer service personnel have at least five consecutive days away from job functions each year or receive exemptions from the Executive Council.

CU*Answers maintains an insurance package that includes IS equipment, media, extra expense, general liability, building and contents casualty coverage, workmen's compensation, umbrella liability coverage, employee dishonesty coverage, and errors and omissions coverage.

Management has a Vendor Management Program in place to ensure appropriate oversight is performed over third party vendors. The Vendor Management Program provides procedures for determining the criticality of specific relationships or vendors. Vendor Management evaluates control of reputation risk, financial risk, and compliance risk for the organization. When assessing the risk of each vendor, CU*Answers reviews key risk information:

- extent to which the vendor has access to non-public member information and/or stores non-public member information;
- extent to which the vendor has access to the organization's physical location;

- extent to which the vendor has access to the organization's IT infrastructure;
- extent to which the service provided by the vendor is intolerant (disaster recovery/business resumption) to the disruption of member services; and
- extent to which the service provided is vital to the organization and financially woven into the strategies of the organization.

Each vendor reviewed is evaluated in accordance with the above variables and based upon this evaluation was assigned a tier level appropriate for the ongoing monitoring and continued due diligence of the vendor.

Physical Security

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

The CU*Answers Kentwood Center is located on the main floor of a one-floor office building. The center is staffed 24-hours per day, seven days per week. The entrances are locked at all times. Visitors can only gain entrance into the building when authorized by CU*Answers personnel. All visitors must sign in at the receptionist desk and wear a badge at all times while in the building. The security alarm is set at a specified time each evening securing the perimeter of the facility. Key employees are issued electronic building keys that allow access to the building on a five or seven-day system. A log is maintained of all keys and their numbers.

The CU*Answers Grand Rapids Center is located on the lower level of a three-floor office building. The center is staffed 10-hours per day, five days per week. Visitors can only gain entrance into the building when authorized by CU*Answers personnel. All visitors must sign in at the receptionist desk and wear a badge at all times while in the building. The security alarm is set at a specified time each evening securing the interior and perimeter of the facility. Employees are issued electronic building keys that allow access to the building on a five or seven-day system. A log is maintained of all keys and their numbers.

The CU*Answers Muskegon Center is located on the fifth level of a seven-story office building. The entrance is locked at all times. Visitors can only gain entrance into the building when authorized and escorted by CU*Answers personnel. The security alarm is set at all times unless occupied by CU*Answers support staff. Authorized employees are issued electronic building keys that allow access to the building on a seven-day system. A log is maintained of all keys and their numbers.

Access to the computer rooms may be gained only by authorized employees using electronic building keys on the computer room door. Smoking, eating and drinking are prohibited in the computer room. Any non-operations staff must sign in at the computer room reception area.

Computer rooms are protected by a FM-200 fire suppression system. Additionally, all the buildings are directly linked to a local monitoring company via an alarm system. Sensors positioned throughout the building, including storage areas, detect heat, smoke, motion and immediately notify the local monitoring company who in turn notifies the fire department and building security. The buildings are monitored 24-hours per day, seven days per week.

The buildings are also protected against fire by hand held extinguishers. These extinguishers are inspected each year and may be used on fires involving electrical devices, liquids, and other combustible materials. Sensors are installed in the computer rooms to ensure that changes in heat or moisture will be detected and alarms sent directly to staff who can respond immediately to a problem.

Emergency battery powered lighting, activated when the power is cut off, is located throughout all facilities. Signs posted above certain doors mark emergency exits. An Uninterrupted Power Supply (UPS) has been installed in each facility to provide power for the systems for up to 40 minutes in the event of a power failure.

Natural gas powered electric generators are in place in Muskegon, Kentwood and Grand Rapids to supply continuous power to all critical systems for an unlimited amount of time. There are specific test procedures for the UPS and generator systems that are detailed in the Disaster Recovery Manual.

Managed Hosting Services (aka Facilities Management)

Controls provide reasonable assurance that controls are in place for managing server backups and ensuring appropriate network segmentation is in place.

CU*Answers Network Services utilizes online network data backups, industry-standard data encryption, granular data recovery capabilities, nightly secure offsite backups to one of CU*Answers' data centers, data de-duplication and compression technology, and on-network virtualization technology.

Network Security Domains

CU*Answers Network Services segregates client networks by security domain using routing application-aware stateful inspection firewalls. These security domains are used to control ingress/ egress traffic and are constructed based on role. For example, web servers will typically be grouped into a security domain and file and database servers into another. Each security domain consists of a subnet of network addresses as predetermined by network administrators and as tracked in the IP Address Allocation Schedule spreadsheet.

The typical deployment of a managed hosting network is to place a security appliance on an existing network segment (such as a web security zone) behind the core firewalls. The security appliance then would have LAN and DMZ security domains, as appropriate, based on the required role(s). The dedicated client security appliance would then be used primarily to:

- Provide controls for traffic leaving the hosted client security domain for the purpose of preventing unauthorized traffic to adjoining security domains behind the core firewall.
- Provide a VPN end point for client networks that connect to the hosted network.
- Provide controls for traffic taking place between LAN and DMZ security domains of the security appliance (i.e. between a web server and a database server.)
- Provide an auditing point for traffic traversing security domains.

Management Tools

CU*Answers Network Services uses a variety of tools to manage its network. Clients generally do not have access to these tools though it is permissible to allow the network monitoring system to send availability email alerts to clients and to provide historical graphing information with appropriate approval. CU*Answers Network Services has deployed Latitude, a web-based Management Portal for online client access to reports and help desk systems.

Daily Operational Procedures

The following procedures must be executed every week day on all client Intel systems. The purpose of these procedures is to maintain the safe, secure, and ongoing operating environment for all network assets under our management. Anomalies must be investigated and errors reported, escalated, and remediated on a daily basis. Errors allowed to continue may create an unstable environment and may cause failures.

- Follow run sheets for each system.
- Respond to network monitoring system alerts as appropriate.
- Run backups following established procedures and review network backup system logs.

- Review Intrusion Detection System logs.

Monthly Operational Procedures

Monthly run sheets have been developed to document the following:

- Systems will be patched according to predetermined schedule.
- Patches will be downloaded automatically and installed manually by Administrator unless other arrangements are made.
- Administrators will verify patch installation by checking application and system logs for relevant entries and will occasionally run security verification against the system for further verification.
- All critical patches will be installed. Optional patches will be installed at the discretion of the administrator depending on the severity and applicability of the update.
- Drivers must not be installed unless approved by the hardware vendor.
- Unsuccessful patches will be worked until successful unless determined non-critical by the administrator.

Client Change Requests

It is not often that request for system or network changes are submitted by managed hosting clients, as most manage their own applications and will install/ remove software at their own discretion. They are also administrators on their systems and can make configuration changes at will and handle their own password resets.

The majority of client requests will be for assistance troubleshooting a problem and prompt responses by CU*Answers Network Services administrators is expected. Client request are submitted via the Latitude Help Desk Portal and are tracked to completion.

Unscheduled Maintenance

Unscheduled maintenance that would affect system availability or interfere with contractual obligations will be communicated to the client at least 24 hours in advance, though at least a week's notice is preferred. Care is taken not to perform maintenance on client systems during known critical production cycles.

Firewall Management Service

Controls provide reasonable assurance that intrusion prevention, anti-virus and anti-spyware monitoring have been implemented on the firewall and/or gateway equipment. Content Filtering has been configured and implemented.

CU*Answers Network Services Firewall management is an on-premise managed security service which provides 24x7x365 proactive monitoring and administration for firewall infrastructure. The service includes the following service and deliverables:

- Provides a comprehensive, integrated network security solution against advanced threats by employing High-bandwidth stateful packet inspection.
- Deep Packet Inspection Technology
- Intrusion Prevention/ Detection
- Gateway Anti-Virus
- Gateway Anti-Spyware
- Policy based application filtering

- Firewall policy design and Technical Assistance
- 24x7x365 Monitoring with Secure Offsite Log Storage
- 10x5 Support Standards, with 24x7 support optional
- VPN/Remote User Management
- Complete Hardware Warranty and Replacement
- Firmware Upgrades
- Automatic Configuration Control and Backup
- Comprehensive Scheduled and On-Demand Reporting
- Real Time Alerting
- Strategic Network Planning

All managed equipment is placed on-premise at the client site and subject to client's physical and environmental security controls. CU*Answers Network Services recommends following industry standard best practices to address physical and environment security.

Infrastructure

CU*Answers Network Services firewall management monitoring and reporting system resides on a secured network segment within the CU*Answers corporate network. The firewall management system consists of a front-end web console server and a backend database server. CU*Answers Network Services is using management software to monitor and manage client firewalls, collect network traffic data, track subscription licensing and provide reporting. Client firewalls transfer log data in real-time via encrypted tunnel. The tunnel connections are terminated at redundant firewalls.

CU*Answers Network Services maintains all Syslog data collected from client firewall systems for a minimum of 30 days.

Operational Procedures

The following procedures are executed according to published schedule for all managed units. The purpose of these procedures is to maintain the safe, secure, and ongoing operating environment for all network assets under CU*Answers Network Services management. Anomalies must be investigated and errors reported, escalated, and remediated on a daily basis. Errors allowed to continue may create an unstable environment and may cause failures. CU*Answers Network Services monitoring and management infrastructure is configured to open trouble tickets and/or issue alerts when certain thresholds are met on managed systems.

- Review report distribution, make client contact for any down units.
- Process all client change requests.
- Installation/upgrade of any firmware or software available.
- Resolution of any trouble tickets generated from server monitoring system.
- Review firewall management system logs.
- Conduct a quarterly audit of firewall settings, to ensure licenses and services are synchronized and available and review firmware version. Results are recorded and available for client review.

Weekly run sheets have been developed to document the following:

- Systems will be patched according to a predetermined schedule, daily, as updates are available.
- Patches will be downloaded automatically and installed manually by Administrator unless other arrangements are made.
- Administrators will verify patch installation by checking application and system logs for relevant entries and will occasionally run Microsoft Baseline Security Analyzer against the system for further verification.
- All critical patches will be installed. Optional patches will be installed at the discretion of the administrator depending on the severity and applicability of the update.
- Drivers must not be installed unless approved by the hardware vendor.
- Unsuccessful patches will be worked until successful unless determined non-critical by the administrator.

Complete Care Management

Controls provide reasonable assurance that critical data servers (fileservers, email, database, etc.) are configured and kept up to date as new service packs and critical manufacturer fixes are released. Anti-virus systems are operational.

CU*Answers Network Services Complete Care Management is an on-premise managed security service. The service includes the following service and deliverables:

- 24x7x365 monitoring and alerting for all network connected devices and critical services
- Server and workstation patching (24-hour response for critical and security related patches)
- Weekly Server Security Baseline testing
- Real time Backup Log monitoring and remediation
- Real time Anti-Virus monitoring including virus pattern version and unprotected machines
- Unlimited Group and User Management
- Quarterly Backup File Restore and Virtualization Testing with Report
- Quarterly Third Party Vulnerability Scanning for Public Facing Network Devices
- Third Party Vulnerability Scanning for Internal Network Devices
- Weekly Systems Review
- Weekly Full Finding Report

All managed equipment is placed on-premise at the client site and subject to client's physical and environmental security controls. CU*Answers Network Services recommends following industry standard best practices to address physical and environment security.

Infrastructure

CU*Answers Network Services Complete Care monitoring and reporting system resides on a secured network segment within the CU*Answers corporate network at the Kentwood datacenter. The Complete Care management system consists of a front-end web console server and a backend database server. Client devices transfer log data in real-time via encrypted tunnel. The tunnel connections are terminated at the front-end web server. The management platform resides behind a high availability pair of firewalls.

CU*Answers Network Services maintains all data collected from client systems for a minimum of 90 days.

Operational Procedures

The following procedures are executed according to published schedule for all managed units. The purpose of these procedures is to maintain the safe, secure, and ongoing operating environment for all network assets under our management. Anomalies must be investigated and errors reported, escalated, and remediated on a daily basis. Errors allowed to continue may create an unstable environment negatively affecting the overall security posture of the client site. CU*Answers Network Services' monitoring and management infrastructure is configured to open trouble tickets and/or issue alerts when certain thresholds are met or exceeded on managed systems.

- Review trouble tickets and alerts.
- Process all client change requests.
- Review critical and security related patch availability.
- Daily review of system status, including event logs, backup systems, security baseline report and anti-virus systems.
- Weekly report review and delivery.
- Quarterly backup restore tests.

Controls provide reasonable assurance that system security management is performed per the request of the client.

Client Change Requests

Client change requests are regularly received from Complete Care and firewall management clients. CU*Answers Network Services uses a secure, web-based client management portal to receive these requests. Users with the ability to submit requests for information or configuration changes must have prior authorization from their institution. CU*Answers Network Services technical staff has the ability to open support tickets based on email from authorized clients on behalf of that client. CU*Answers Network Services technical support staff is required to ensure client requests have been logged in Latitude prior to completing the request. Clients have the ability to track the status of their tickets through the portal at any time. All client requests are archived to ensure a clear audit trail. Clients have the ability to review their past request history and can request a custom report on this activity at any time.

The majority of client requests are for assistance troubleshooting a problem or for configuration changes and prompt responses by CU*Answers Network Services administrators is expected.

Infrastructure Backups

The Complete Care and firewall management servers are part of CU*Answers Network Services' high availability backup solution, which uses a continuous data protection strategy, whereby encrypted system snapshots are made to local, high speed network attached storage (NAS) device. Incremental backups are compressed and transferred to an offsite via high-speed encrypted connection. The system offers restore capabilities for multiple file versions. The backup system is monitored 24x7 and a ticket is automatically generated for missed backup or any issue with the backup system.

The local and remote NAS devices also offer backup virtualization capabilities, facilitating a business continuity strategy for critical hardware or environmental failures at the primary site. Data backup integrity, recovery and virtualization are tested on the backup appliances on a quarterly basis.

System Maintenance

All planned maintenance, including hardware, operating system or application upgrades is preceded by an announcement at least 8 hours prior to start. Any system maintenance that will result in downtime is scheduled at least 24 hours and preceded by an announcement. Care is taken not to perform maintenance on client systems during known critical production cycles.

e-Business Policies and Procedures

Controls provide reasonable assurance that policies and procedures to address e-Business risk are documented, communicated, and provided to the staff.

Data security is a top priority at CU*Answers and permeates everything we do. Because security is such a complex issue, no single solution or "silver bullet" can be expected to provide adequate protection. As such, we view security much like an onion: it should have many layers each providing additional levels of protection.

The first layer in any organization is knowledgeable network administrators experienced in applying security best practices to network resources. Our IT staff continuously monitors third-party advisories for the latest security bulletins and alerts. In addition, staff conducts regular research and application of the latest security standards. Additionally, technical staff members are encouraged to seek appropriate external security training.

Additional security layers for managed hosting devices include:

- Border and gateway devices secured to industry best-practices,
- Dual redundant gateway firewalls, network and host-based intrusion detection systems,
- Layered network firewalls in some segments,
- Hosts secured to industry best-practices and kept up to date with critical security fixes,
- Regular log file reviews,
- Centrally managed enterprise-wide anti-virus software,
- Centralized critical event log file aggregation systems,
- Centralized device performance and response monitoring and alerting, and
- Regular internal host configuration security audits.

To independently verify our security, CU*Answers contracts with independent third parties to perform periodic external and internal penetration tests. These assessments identify potential targets, probe those targets to determine their configuration and identify vulnerabilities, and finally attempt to exploit discovered vulnerabilities. CU*Answers management reviews the results of each assessment and evaluating implementation of recommendations.

The final, and most important, security layer in any organization is a security-conscious and trained staff. All the firewalls in the world will not stop an uninformed, careless, or reckless employee from accidentally disclosing important information or succumbing to social engineering attacks. Because CU*Answers recognizes this threat, on-staff security experts have crafted an aggressive security awareness campaign that includes comprehensive courses covering everything from security basics to advanced network defense principles and teaches these to both staff and clients alike. This campaign is an essential ingredient for creating and maintaining an attitude of "security is our way of doing business."

SECTION IV: Complementary User Entity Controls Provided by CU*Answers, Inc.

Complementary User Entity Controls

This section outlines specific complementary user entity controls, or issues each CU*Answers client should implement in order to achieve certain control objectives identified in this report. These considerations are not necessarily a comprehensive list of all internal accounting controls that should be employed by the customer, nor do they represent procedures that may be necessary in all circumstances.

1. CU*Answers Network 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.
2. CU*Answers Network 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.
3. CU*Answers Network Services customers are responsible for accompanying the "guests" that they bring into the CU*Answers Network Services datacenter facility. These guests are also required to sign the visitors log and receive a badge to identify themselves.
4. CU*Answers Network Services customers are responsible for establishing communications to the datacenter facility systems and for ensuring that redundant lines for backup communications exist.
5. CU*Answers Network Services customers should have a business continuity plan in place to ensure that their systems can be restored in the event of an unplanned disruption.
6. CU*Answers Network Services customers are responsible for reviewing activity reports and security findings reports that are provided by CU*Answers Network Services.
7. 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.
8. Facility management and Managed Services customers are responsible for ensuring that their network infrastructure deployed at CU*Answers Network Services provides an appropriate level of resiliency and redundancy.
9. Managed 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.
10. Managed Services customers are responsible for securing ongoing maintenance and support contracts for all non-CU*Answers Network Services-owned software and hardware.

SECTION V: Independent Service Auditor's Description of Tests of Controls and Results

Control Objective 1: Organization and Administration

Control Objective 1: Controls provide reasonable assurance that CU*Answers Network Services and user functions are segregated.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
1.1	CU*Answers Network Services is physically separate from and operates independently of the user institutions for which it provides Co-location and network management services.	Observed application of the control while on-site and inspected a sample contract and verified CU*Answers Network Services is physically separate and operates independently of user institutions.	No exceptions noted.
1.2	User organizations have contracts with CU*Answers Network Services that outline the responsibilities of both CU*Answers Network Services and the user organization.	Inspected a sample of contracts and verified that contract exist between CU*Answers Network Services and user organizations.	No exceptions noted.

Control Objective 2: Organization and Administration

Control Objective 2: Controls provide reasonable assurance that policies and procedures exist to provide internal segregation of duties.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
2.1	An organizational model exists to define the reporting structure of the organization and the lines of segregation between functional areas.	Inspected the organization model for completion, accuracy, and appropriateness to the situation.	No exceptions noted.
2.2	Job descriptions have been prepared for CU*Answers Network Services personnel.	Inspected employee job descriptions and verified completeness.	No exceptions noted.
2.3	CU*Answers Network Services has an employee handbook that describes the company's policies for hiring, termination, salary administration, performance reviews, vacation, employee benefits, building and system security, and discrimination and harassment.	Inspected the Employee Handbook and verified the inclusion of key policies.	No exceptions noted.
2.4	An acknowledgement form is in place that requires employees to sign stating they have read and understand the company's administrative policies as stated in the Employee Handbook.	Reperformed the application of the control by selecting a sample of employees and verified that a signed acknowledgement form is retained in the employee's file.	No exceptions noted.
2.5	The service organization maintains insurance coverage for the building and contents, IS equipment, media reconstruction, extra expense, fidelity coverage, errors and omissions, and umbrella liability coverage.	Inspected IS insurance policies and noted that effective dates and related coverage's were current.	No exceptions noted.
		Confirmed coverage with all appropriate third party insurance companies.	No exceptions noted.
2.6	Management has vendor management procedures in place to ensure appropriate oversight is performed over third party vendors.	Inspected management policies and procedures pertaining to vendor management and made inquiries with management regarding vendor oversight standards.	No exceptions noted.

Control Objective 2: Controls provide reasonable assurance that policies and procedures exist to provide internal segregation of duties.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
2.7	Management have implemented a vendor risk assessment process to review the vendors utilized by the organization.	Inspected vendor risk assessment documentation and made inquiries with management regarding the risk assessment process.	No exceptions noted.

Control Objective 3: Physical Security

Control Objective 3: Controls provide reasonable assurance that safeguards and/or procedures are used to protect the service organization against intrusions, fire and other hazards.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
3.1	All doors to the service organizations main and backup facility are locked and controlled by a security system.	Observed security systems and procedures and inspected the Physical Security Policy and verified doors are secured.	No exceptions noted.
3.2	Authorized personnel have been issued electronic building keys and have been given the code to deactivate the perimeter alarm system at the facilities.	Inspected the Physical Security Policy and inquired with CU*Answers Operations Management and verified only authorized personnel are allowed access to the buildings.	No exceptions noted.
3.3	The computer rooms are locked at all times and visitors must be admitted to the area by operations personnel.	Observed physical security procedures throughout the audit and verified the compliance with service organization policies and procedures.	No exceptions noted.
		Reperformed application of the control by obtaining the listing of users with access to the computer rooms and verified that only authorized personnel are allowed access.	No exceptions noted.
3.4	Heat, smoke, FM200 automated suppression system and intrusion detectors are connected to a monitored alarm system to the computer room facilities. Further, hand held fire extinguishers are located throughout the facilities.	Toured the entire Grand Rapids and Kentwood facilities and computer rooms and noted the presence and location of portable fire extinguishers (recent inspection), fire detection sensors and alarms, FM200 suppression, electrical power shut-off switch, analog phone line in the computer room, emergency lighting, and exit signs.	No exceptions noted.
3.5	A written action plan relating to emergency situations is distributed to employees.	Inspected the emergency action plan and verified that the plan included actions to be taken (e.g., equipment restart and recovery procedures), individuals to phone, and materials to be removed from the computer room.	No exceptions noted.

Control Objective 3: Controls provide reasonable assurance that safeguards and/or procedures are used to protect the service organization against intrusions, fire and other hazards.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
3.6	An Uninterruptible Power Supply (UPS) system with power conditioners is installed to protect both computer room facilities from short or long-term power failures.	Toured the service organization's Grand Rapids and Kentwood computer rooms and noted the presence and location of an UPS system.	No exceptions noted.
		Inspected the results of the UPS inspections for each facility and verified UPS systems are being maintained.	No exceptions noted.
3.7	A natural gas generator is installed at each facility to protect the buildings from power failures.	Toured the service organization's Grand Rapids and Kentwood facilities and noted the presence of a natural gas generator and inquired with Internal Network Manager about the weekly testing of the generator.	No exceptions noted.
		Inspected the results of the generator inspections for each facility to ensure generators are being maintained.	No exceptions noted.

Control Objective 4: Managed Host Services (aka Facilities Management)

Control Objective 4: Controls provide reasonable assurance that controls are in place for managing server backups and ensuring appropriate network segmentation is in place.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
4.1	All critical systems and applications on Intel (server) network are backed up daily. A file retention schedule and a schedule for premise rotation of system and/or application have been established.	Inspected the backup settings and scripts and verified systems and applications on Intel network are backed up daily.	No exceptions noted.
4.2	Backup logs are monitored and reviewed on a daily basis. File restore test of backup data are performed on a quarterly basis.	Inspected alerts created for failed and successful backups and inquired with Network Services Manager of Client Support and Operations and verified backups are monitored and reviewed.	No exceptions noted.
		Inspected the Backup Restore Test Log and verified that restores are completed.	No exceptions noted.
4.3	CU*Answers Network Services segregates client networks by security domain using routing application-aware stateful inspection firewalls. These security domains are used to control ingress/ egress traffic and are constructed based on role.	Inspected company network diagrams and firewall settings and inquired with the Manager of Network Services Client Support and Operations and verified that client networks are segregated.	No exceptions noted.
4.4	Each security domain will consist of a subnet of network addresses as predetermined by network administrators and as tracked in the IP Address Allocation Schedule spreadsheet.	Inspected the IP Address Allocation Schedule spreadsheet and inquired with the Network Services Manager Client Support and Operations and verified IP addresses are tracked in the spreadsheet.	No exceptions noted.

Control Objective 5: Firewall Management Service

Control Objective 5: Controls provide reasonable assurance that intrusion prevention, anti-virus and anti-spyware monitoring have been implemented on the firewall and/or gateway equipment. Content Filtering has been configured and implemented.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
5.1	CU*Answers Network Services implemented industry standard firewall systems to monitor and control traffic between all network segments including the production networks, managed hosting networks, and the Internet.	Inspected company network diagrams and inquired with the Manager of Client Services and Operations and verified that firewall systems are in place for production and hosting networks and the Internet.	No exceptions noted.
5.2	Application or hardware systems have been configured to monitor the following items: • Intrusion Prevention Monitoring • Gateway Anti-Virus Monitoring • Gateway Anti-Spyware Monitoring	Inspected firewall configurations and inquired with the Network Services Manager of Client Support and Operations and verified applications and hardware systems have been configured appropriately.	No exceptions noted.
5.3	Firewall and additional security devices (e.g., routers, and authentication servers) have been configured to appropriately restrict access from the Internet, user institutions, and business partners.	Inspected router and firewall configuration settings and inquired with the Network Services Manager of Client Support and Operations and verified access from the Internet, user institutions and business partners is restricted.	No exceptions noted.
5.4	Firewall policy changes, technical assistance and VPN management are authorized and tracked within the Latitude issue tracking system.	Reperformed application of the control by selecting a sample of firewall changes during the period and verified that each change was authorized and appropriately entered into the Latitude issue tracking system.	No exceptions noted.
5.5	The firewall is set up to log suspicious and unauthorized access attempts. Network Administrators review the firewall logs on a daily basis.	Inspected sample firewall alerts and inquired with Network Services Manager of Client Support and Operations and verified firewalls are logged and alert Network Services if any problems are encountered.	No exceptions noted.

Control Objective 5: Controls provide reasonable assurance that intrusion prevention, anti-virus and anti-spyware monitoring have been implemented on the firewall and/or gateway equipment. Content Filtering has been configured and implemented.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
		Reperformed the application of the control by selecting a sample of days and verified review of firewall logs by appropriate company personnel.	No exceptions noted.
5.6	Hardware warranties are in place for firewall systems.	Inspected firewall warranties and inquired with the Network Services Network Engineering Manager and verified warranties are in place for firewall systems.	No exceptions noted.
5.7	Firewalls firmware is updated and backed up on a periodic basis.	Inspected the firewall firmware settings and backup settings and inquired with Network Services Manager of Client Support and Operations and verified firmware is updated and backed up.	No exceptions noted.

Control Objective 6: Complete Care Management

Control Objective 6: Controls provide reasonable assurance that critical data servers (fileservers, email, database, etc.) are configured and kept up to day as new service packs and critical manufacturer fixes are released. Anti-virus systems are operational.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
6.1	Servers are patched with latest critical and security updates within 24 hours of the patch being released.	Inspected a sample contract and inquired with CU*Answers Network Services Manager of Client Support and Operations and verified contract terms state that servers must be patched within 24 hours for critical and security updates.	No exceptions noted.
6.2	Server hardware and critical services are automatically inspected every 5 minutes. Security tests are executed against the servers on a weekly basis.	Inspected sample monitoring reports produced for clients and verified that hardware and critical services are being monitored. Further, inspected scan settings for the security tests and verified they are executed on a weekly basis.	No exceptions noted.
6.3	System and device logs are configured to record specified system events and the logs are retained both on the system and on a central log file aggregation device.	Inspected sample device configuration logs and inquired with CU*Answers Network Services Manager of Client Support and Operations and verified network administrators procedures for configuring system logs.	No exceptions noted.
6.4	CU*Answers Network Services 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.	Inspected procedures for reviewing the network systems performance and security logs and verified contract terms identify events and changes that are monitored by CU*Answers Network Services.	No exceptions noted.
		Reperformed the control by selecting a sample of days and verified review of network server system logs by appropriate company personnel.	No exceptions noted.

Control Objective 6: Controls provide reasonable assurance that critical data servers (fileservers, email, database, etc.) are configured and kept up to day as new service packs and critical manufacturer fixes are released. Anti-virus systems are operational.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
6.5	Anti-virus configurations are reviewed and updated weekly; a scan of all network devices is performed weekly to determine virus pattern, scan engine version and locate any unprotected workstations.	Observed the anti-virus software and inspected screenshots of the console and reports produced from the system.	No exceptions noted.
6.6	Various monitoring reports are supplied to the client on a periodic basis. Reports are automatically generated and delivered by our firewall management reporting servers, on a daily, weekly and/or monthly basis via email. Procedures are in place to verify that reports have been generated.	Discussed with management procedures to monitor report generation and inspected the reporting configuration settings and verified that the following reports are created: • Patch Management • Server Backup Results • Vulnerability Scans • Server Activity Results	No exceptions noted.

Control Objective 7: Complete Care Management

Control Objective 7: Controls provide reasonable assurance that system security management is performed per the request of the client.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
7.1	Client change requests are regularly received from Complete Care and firewall management clients. CU*Answers Network Services uses a secure, web based client management portal, Latitude, to receive these requests.	Observed application of the control and inquired with Network Services Client Support and Operations Manager and verified procedures for documenting client change request in the Latitude issue tracking system.	No exceptions noted.
7.2	Users with the ability to submit requests for information or configuration changes must have prior authorization from their institution. CU*Answers Network Services technical staff has the ability to open support tickets based on email from authorized clients on behalf of that client.	Inspected a Latitude firewall ticket and verified that the contact that opened the request is recorded on the ticket.	No exceptions noted.
		Observed CU*Answers Network Services personnel open a ticket and inquired with CU*Answers Network Services Client Support and Operations Manager and verified tickets are only opened when authorized by a client.	No exceptions noted.
7.3	The Latitude issue report is available to clients on demand. Clients can logon and access issue reports at any time.	Observed the Latitude system and verified that the issue report is available for clients.	No exceptions noted.
7.4	Client requests are archived to ensure a clear audit trail exist. Clients have the ability to review their past request history and can request a custom report on this activity at any time.	Observed the Latitude system and verified that the past request history is a report that is available for clients.	No exceptions noted.

Control Objective 8: e-Business Policies and Procedures

Control Objective 8: Controls provide reasonable assurance that policies and procedures to address e-Business risk are documented, communicated, and provided to the staff.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
8.1	Policies and procedures for e-Business activities are documented, reviewed by management, and provided to CU*Answers staff.	Inspected e-Business policy documents and inquired with Manager of Network Engineering and Implementation to verify procedures are documented.	No exceptions noted.
8.2	CU*Answers implemented an industry standard firewall systems to monitor and control traffic between all network segments including the production networks, managed hosting networks, and the Internet.	Inspected the firewall documentation and inquired with Manager of Network Engineering and Implementations about the configuration of the firewall and monitoring controls.	No exceptions noted.
8.3	The firewall is set up to log suspicious and unauthorized access attempts. Network Administrators review the firewall logs on a daily basis.	Reperformed the application of the control by selecting a sample of days and verified review of firewall logs by appropriate company personnel.	No exceptions noted.
8.4	A firewall and additional security devices (e.g., routers, and authentication servers) have been configured to appropriately restrict access from the Internet, user institutions, and business partners.	Inspected the firewall, Network Diagrams, settings, reports and inquired about security configurations with Manager of Network Engineering and Implementations and confirm that the security devices have been configured to appropriately restrict access from the Internet, user institutions, and business partners.	No exceptions noted.
8.5	System and device logs are configured to record specified system events and the logs are retained both on the system and on a central log file aggregation device.	Inspected configuration of the firewall logs with Manager of Network Engineering and Implementations and verified that specified system events are recorded and are retained.	No exceptions noted.

SECTION VI: Other Information Provided by CU*Answers, Inc. (Unaudited)

Other Information

The Organizational Model (OM) is a tool that combines day-to-day administration with team concepts. This web tool is a management chessboard that allows us to redefine teams, move people around, and get a big-picture idea of where people are wearing multiple hats.

We believe you first create the intent of a team, the reason for its existence, well ahead of actually having independent people to lead the team or standalone departments to take on the challenge. The OM allows us to think about who we wish to be, what roles are needed, and how we might extend ourselves through new people when that financial investment is warranted.

The OM is a succession planning resource that documents the digital intelligence about how CU*Answers is organized and how its people are deployed across multiple functional teams. It also reflects our philosophy that every employee can be a leader, as they interact with other teams across multiple disciplines.

Areas of our Organization:

- Leadership
- General Administration Invention
- Production
- Capture Market Share
- Client Interaction and Support cuasterisk.com
- Management Configuration Executive Council's Direct Reports

Leadership Area Teams
CU*Answers is organized in a way that ensures key leaders will work with the board on a regular basis to represent our most important corporate concepts:

1. Vision & Coordination: The teams under the leadership of the CEO, who pulls everything together
2. Financial Leadership: The teams under the leadership of the CFO
3. Client Leadership: The teams under the leadership of the COO
4. Market Leadership: The teams under the leadership of the EVP of National Sales & Marketplace Relationships
5. Network Technology Leadership: The teams under the leadership of the EVP of Technology
6. Software Development Leadership: The teams under the leadership of the EVP of Software Development

These positions make up the senior management team referred to as the Executive Council, or EC team. CU*Answers uses various retention strategies to secure and maintain the officers of the EC as a long-term leadership asset, including key-man insurance and a Supplemental Employee Retirement Plans (SERP). The CEO, COO and CFO are under contract, and the Board Handbook Committee periodically reviews the procedures for negotiating these contracts and documents their procedures as a standard part of the handbook.