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 CU*BASE Application Processing and Managed Hosting 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

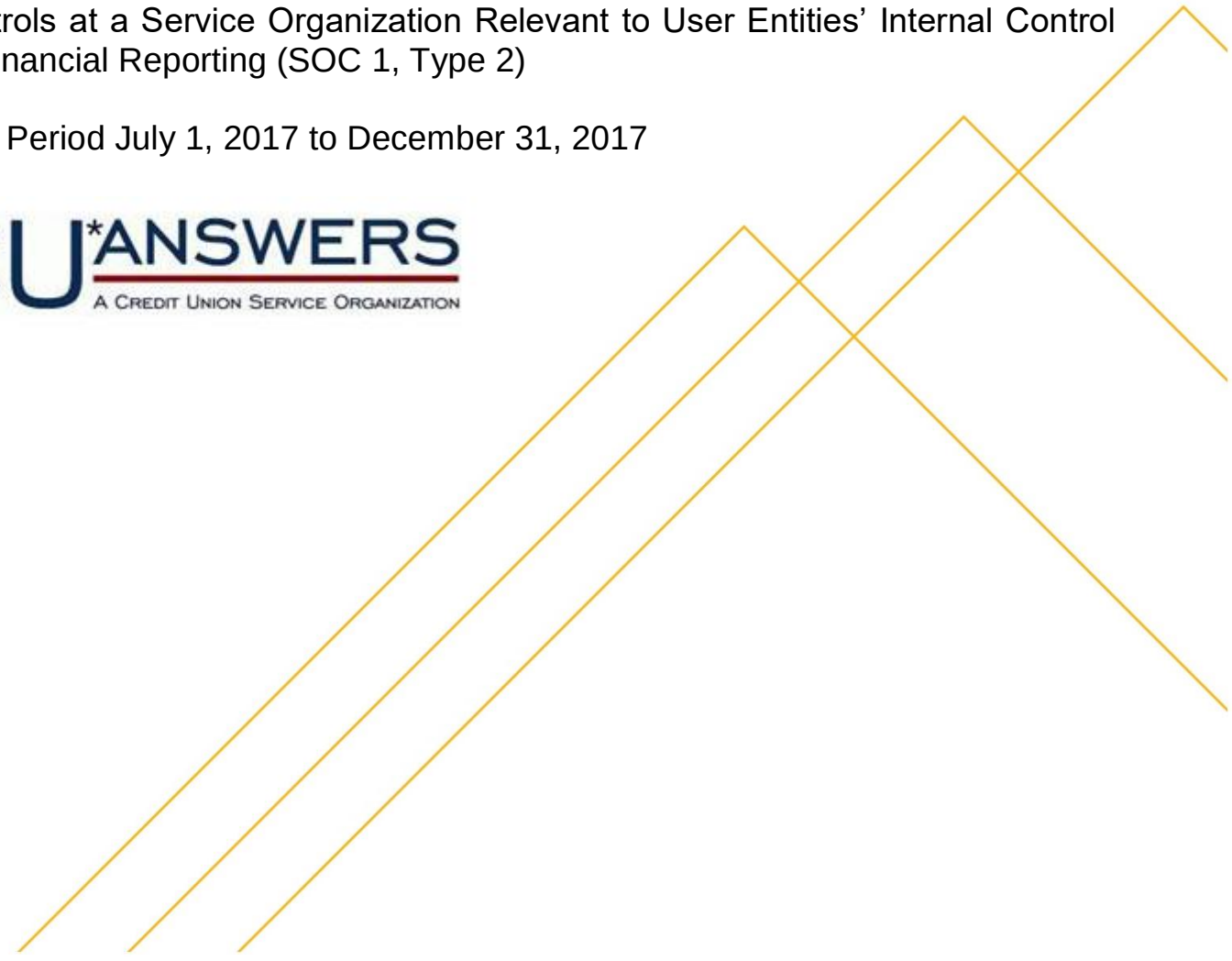


Table of Contents

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 CU*BASE Application Processing and Managed Hosting Services system entitled "CU*Answers' Description of Its CU*BASE Application Processing and Managed Hosting 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 CU*BASE Application Processing and Managed Hosting Services system that are not likely to be relevant to user entities' internal control over financial reporting.

The 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 CU*BASE Application Processing and Managed Hosting 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 CU*BASE Application Processing and Managed Hosting Services system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the CU*BASE Application Processing and Managed Hosting 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

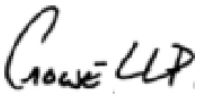
In our opinion, in all material respects, based on the criteria described in CU*Answers' assertion:

a. the description fairly presents the CU*BASE Application Processing and Managed Hosting 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' CU*BASE Application Processing and Managed Hosting 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 CU*BASE Application Processing and Managed Hosting Services:

We have prepared the description of CU*Answers' application processing and managed hosting system entitled, "CU*Answers' Description of Its Application Processing and Managed Hosting 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 Application Processing and Managed Hosting 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 Application Processing and Managed Hosting 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.

Robert Frizzle
Chief Financial Officer
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.

Data Processing and Ancillary Services

CU*Answers has been providing core and peripheral data processing services to its client credit unions since 1970. CU*Answers' product line is anchored by its core solution CU*BASE. CU*BASE is a copyrighted software package which is the exclusive property of CU*Answers. CU*BASE is used by credit unions across the country to serve over two million members. CU*BASE services are delivered through both on-line processing from the Kentwood, Michigan processing center, the Highly Available system in the Yankton, South Dakota secure HA processing center, or directly to in-house (self-processing) credit union sites.

The CU*BASE software features support credit union staff operations from the receptionist (interoffice communications) to the teller, member services including lending, and the executive team. CU*BASE also coordinates all major third-party credit union business interfaces with multiple direct on-line interfaces as well as on-line member contacts through both Audio Response, Online Banking and Mobile Banking options. The CU*BASE software package is designed to run on the IBM Power Systems platform and utilizes microprocessor (PC) terminal networks.

As an example of its dedication to safe, reliable and state of the art processing, CU*Answers employs a high availability infrastructure. Data is replicated in real-time from the production system at the Michigan processing center to an identical High Availability system at the South Dakota processing center over a private fiber high speed connection. Roll-over testing is performed each year where full client volumes are processed on the High Availability system for at least one full processing day. Disaster recovery tests are performed each year and are directed by a dedicated Disaster Recovery/ Business Resumption Manager. CU*Answers' versatility is also demonstrated by its coordination of an internal CU*BASE shared branching operation for its on-line clients, multiple corporation processing for partnered credit union operations, and multiple (service center) credit union license relationships for shared self-processing operations. CU*Answers also provides both Check Clearing and Check 21 services through its Kentwood, Michigan offices.

Network Services

CU*Answers, through its CU*Answers Network Services division, also provides a complete offering of network hosting services. 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.

Education

CU*Answers promotes its competitive advantage of being an educator on how to apply data processing techniques in credit union operations. Its central education product is CU*Answers University. To ensure that all clients have an opportunity to take advantage of CU*Answers University, CU*Answers continually adds new education venues. The offerings currently include classroom training, regional training events, workshops, individual training, Web Conferences, focus groups, online learning and even consumer education for the clients' members. An Education Catalog is developed each year outlining schedules for the different venues. In addition to the scheduled courses, throughout the year additional courses are added based on client request and need. CU*Answers University sessions are provided as a free of charge enhancement to CU*Answers' base services.

Ancillary Services

CU*Answers core data processing services are supported by a professional staff with a comprehensive blend of credit union industry and technical experience. The cooperative provides client services dedicated to assisting users with the CU*BASE product line and daily credit union operations.

There are also technical services provided to CU*Answers' client base. Programming and Software Design members are added to the staff based on the combination of both their general technical skills and their understanding of the financial services industry. CU*Answers also provides accounting, marketing, and administration specialists that focus on the credit union industry and their unique disciplines to ensure that CU*Answers clients receive services that are in line with the best the market has to offer.

Control Objectives and Related Controls

The control objectives specified by CU*Answers and the controls that achieve those control objectives are listed in Section V: Independent Service Auditor’s Description of Tests of Controls and Results section.

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 CU*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, Backup and Recovery Planning, Computer Operations, On-Line Security, Physical Security, and e-Business Policies and Procedures.

Computer Operations includes individual areas such as: Standard Operating Procedures, Run Sheet Maintenance and Review, and Job Processing 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 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.

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.

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

The relationship between CU*Answers and user organizations is contractual in nature. Operations, programming, and network administrators do not initiate or authorize transactions.

Controls provide reasonable assurance that data processing activities are independently reviewed and tested.

The Internal Auditing department staff has experience in accounting, law, network infrastructure, client support, and system auditing. CU*Answers approaches all audits with candid and transparent accountability to allow our owners and clients to feel confident that our solutions and capabilities are built with the intent of being a leader in our industry and an operator of the utmost quality. Internal Audit assists the 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, so risks may be identified, and internal controls are designed at the beginning of a project. CU*Answers undergoes regular regulatory examinations by state and federal authorities and conducts its own thorough internal audits.

Strategic 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.

Backup and Recovery Procedures

Controls provide reasonable assurance that backup procedures and current off-site storage of important files exist, as well as a formal disaster recovery plan.

CU*Answers provides a Disaster Recovery and Contingency Plan manual for its clients, as well as its employees. The first section of the manual documents a recommended course of action for clients in preparing for a credit union disaster. The second section documents the CU*Answers Disaster Recovery Plan. It explains the process of recovering from a disaster at the Grand Rapids, Kentwood and Muskegon locations, as well as the protection of valuable credit union data. CU*Answers employs a full-time Disaster Recovery/ Business Resumption Manager who has responsibility for creating scenarios and providing strategies for responding to and recovering from a disaster at either CU*Answers or a client site. These sections of the Disaster Recovery and Contingency Plan include handling various scenarios such as disaster preparation, organization of recovery teams, recovery of the center, testing of backup sites, recovery work flow summaries, and policies for reducing risk. Appendices, which are attached to the plan for ease of update, include emergency notification lists, recovery team members, vendor contact listings, distribution of the plan manual, hardware configurations and equipment inventory, operations schedules, CU*Answers staff, and Board member and client listings.

Credit unions clients are provided with a manual designed to walk the credit union through a thought process in a disaster. When this is completed, it will form the backbone of the credit union's own disaster recovery plan. This plan handles both short-term disasters as well as major catastrophes. Various optional recovery and restoration tools are available to on-line and self-processing clients.

Numerous backup tapes are created for the purposes of restoration of data for testing and research, for application backups, and for disaster recovery. Backups are performed daily on the Production system and the Development system. All member data is encrypted when backups are created. All critical systems and applications on Intel (server) network are backed up daily. A file retention schedule and a schedule for off premise rotation of system and/or application have been established.

Significant files and programs are replicated in real time using iTera disk to disk replication. Management completes the iTera HA Daily Tasks List to monitor replication status. Complete policy and procedures for Production and Development system backups are documented and maintained in the "SOP - Operations Media Retention and Management" repository. The SOP includes naming conventions, a process description, content summary, media type, retention cycle, a backup process summary and the program that is called for the process. All substantive changes are submitted for approval to the appropriate executive manager. Upon approval, the SOP is updated and the change is logged in the change history that is included as a part of the SOP document. Operations and Network Services also provide backup services for clients.

Controls provide reasonable assurance that insurance coverage exists relative to loss of equipment, records, and data processing capability.

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.

Computer Operations

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

CU*Answers operates a variety of IBM Midrange and Intel-based computers in the Kentwood, Muskegon, and Grand Rapids facilities. Primary hardware consists of three IBM servers: one in the Kentwood data center (Production) and two in the Grand Rapids data center (Development/ Quality Control and High Availability systems). Operating systems are standard OS/400 Releases and are upgraded as needed. CU*Answers utilizes third party security monitoring tools to complement their security program.

CU*Answers employs a high availability infrastructure for its production System-i computer. Data is replicated in real-time from the Production system at the Kentwood data center to an identical High Availability system at the data center in Yankton, South Dakota. Data replication is facilitated by iTera software. Network Services provides managed high availability services for client System-i servers utilizing the same tool sets.

Intel-based computers use a variety of operating systems including Microsoft Windows Server and Linux. Intel-based computers are housed in both CU*Answers' data centers and share the same fire protection and power continuance systems as the IBM computers. Intel-based computers host ancillary products to CU*BASE such as online banking as well as being used to provide managed hosting services.

CU*Answers additionally provides network and computer managed hosting services for a variety of clients from its data centers using segregated network segments that share the same fire protection and power continuance systems as other devices. Hardware malfunctions are reported immediately to IBM using a secure VPN. Hardware issues are logged by operations personnel and reported to the appropriate vendor.

CU*Answers Network Services have processes and processing directions ("run sheets") for modifications to system software and are engaged in ongoing monitoring to ensure the quality and effectiveness of these updates.

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

Computer operators monitor the system for messages using Client Access sessions on microcomputers, run specified daily jobs using processing directions ("run sheets"), and restore libraries to the production system as requested by client service and programming personnel.

Network operations staff monitor network and systems health, inclusive of managed hosting services, using a variety of 24x7 tools including centralized network and service monitoring and alerting systems, centralized log file aggregation and analysis systems, centralized historical performance tracking and analysis systems, and centralized security monitoring and alerting systems.

The operations management team maintains all operations documentation. Examples of documentation include:

- Production Run Sheets
- Standard Operating Procedures pertaining to Operations
- Backup restore requests
- FEDLINE procedures

Processing is performed for on-line clients. Reports and statements are available to clients online from a dedicated server. CU*Answers produces archival materials for its clients. Users can request that reports and statements be archived. Likewise, member statements are electronically stored, encrypted and password protected.

Standard operating procedures and run sheets have been created to conduct daily operation of both the CU*BASE system and all Intel-based servers, including managed hosting assets. The procedures describe the purpose, times, and reasoning for computer operator duties, while the run sheets contain all the tasks an operator would need for processing the daily work. Operators initial completed jobs on these run sheets and record the start and end time of processes as required. The first page of each section of the run sheets includes documenting outstanding issues, requests for run sheet modifications for changed or outdated information, and a section to communicate pertinent information to the management team and following shift personnel. Run sheets are reviewed on a daily basis for completeness and accuracy, to follow up on any outstanding problems or incidents, and for any modifications in content. The run sheets are retained for six months.

On-line Security

Controls provide reasonable assurance that on-line security measures should provide the ability to restrict users to the data files and menu functions to which they are authorized.

There are two levels of security used by client credit unions: terminal access security and CU*BASE application security.

As users enter a user identification name and password to access the system, the on-line communications network reviews a predefined list of users and establishes communications with authorized terminals. The Service Center's system requires terminal access passwords to be changed every 30 days. If the terminal is authorized, and the user is valid, the transaction is processed. When any of these criteria fail, the transaction is denied and rejected. Communication links are secured through MPLS or VPN. In addition, an automatic time-out feature is set to prevent users from leaving terminals unattended and logged into CU*BASE for extended periods.

CU*BASE application security provides a comprehensive method of controlling user access to individual CU*BASE commands and features. The length and expiration settings for these passwords can be customized by each credit union.

CU*Answers maintains terminal access security for both internal users and credit unions. A feature of CU*BASE allows credit unions to re-enable user profiles for their own employees that disable their profiles due to three invalid sign-on attempts. CU*Answers conversion coordinators set up the initial CU*BASE application security within the credit union, at the direction of the credit union. Credit unions are responsible for maintaining CU*BASE application security after it has been originally established. Security logs are monitored using a third-party security tool.

Upon employment, and annually thereafter, employees complete an "Employee/ Client Account Disclosure Form" showing employee accounts at client credit unions. These disclosures are sent annually to each credit union.

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.

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, Inc. (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.

Input Controls

1. Verify and balance all incoming third party files, such as ATM, ACH, and share drafts.
2. Balance system generated general ledger entries to reconcile the general ledger interface against the member trial balance.
3. Monitor daily exception reports and application suspense accounts.
4. Develop internal data security and employee access to system features, as well as all key parameter configurations.

Processing Controls

1. Assign a Data Processing Coordinator to be responsible for coordinating, communicating, and monitoring any processing changes made by CU*Answers that may affect the user, and to attend User Group meetings.
2. Test program changes after general release to verify that results are as published.
3. Periodically consolidate and revise as necessary the manuals and any supplementary notes which comprise the documentation of each user department's data processing procedures to help ensure the user's proper understanding of the system and to facilitate future training of new employees.
4. Review operations logs on a daily basis.
5. Review standard forms generated by the system for regulatory compliance.

Output Controls

1. Review and document on a checklist the reports generated by the system each day to determine that all reports have been received.
2. Control the distribution of reports to user personnel to ensure that reports are distributed to only authorized personnel.
3. Balance application totals to the independently posted general ledger to verify the overall accuracy of the daily processing results.
4. Balance debit and credit entry totals per the daily application subsidiary reports to the entry run and any other on-line entry function to verify the source of all application entries.
5. Physically segregate unposted transaction to establish control for research, correction, and re-entry.
6. Independently verify master file change listing to help ensure the accuracy and propriety of file maintenance posting.
7. Review each application's exception report to help identify any unusual application activity.
8. Annually review the schedule of all reports that are available for each application and determine their actual utilization at the credit union to help ensure that user personnel are receiving and properly utilizing the information available from each application.
9. Establish report retention procedures to provide backup of printed or microfiche output.

10. Shred old and unneeded reports to provide security over account and user information.
11. Independently monitor usage of interest and accounts payable checks printed by the data processing department to safeguard and maintain accountability for such items.
12. Review ACH reports and ACH errors daily to identify batch errors and exceptions. Any items previously sent as ACH organizations that have been returned by the ACH operator must be corrected and retransmitted. Any incoming ACH items that have been rejected need to be manually posted and corrective action needs to be taken to prevent errors in the future.

On-Line Controls

1. Assign an On-Line Security Coordinator to identify one officer who is responsible for defining and monitoring the user's on-line security assignments.
2. Assign each on-line terminal operator a unique sign-on code/ password to positively identify the operator and provide accountability for on-line activity.
3. Assign each backroom user/ operator a system sign-on and password code to positively identify the operator and provide accountability for system and operations activity.
4. Restrict backroom users/ operators to specific menus to limit the activity of these users to authorized transactions.
5. Assign each teller override levels to prevent a teller from performing certain transactions.
6. Periodically change sign-on codes to maintain the confidentiality of each operator's sign-on code.
7. Perform an annual review and approval of all security authorizations to verify that security levels are appropriate for each operator, and to identify any potential conflict of duties.
8. Assign employee numbers to restrict employees from accessing their own or other family members' accounts.
9. Maintain a log of CU*Answers' access.
10. Review on a monthly basis the Member File Maintenance, General Transaction Register, General Journal Report and the Employee Activity Audit for changes made by CU* Answers employees.

Managed Hosting

1. CU*Answers Network Services customers are responsible for reporting to CU*Answers Network services any changes in key contacts for communication purposes.
2. CU*Answers Network Services customers are responsible for their own user account management inclusive of disabling or deleting accounts of terminated employees, unless other arrangements have been made. CU*Answers Network Services customers are responsible for establishing communications to WescoNet facility systems and for ensuring that there exist redundant lines for backup communications.
3. CU*Answers Network Services customers should have a business continuity plan in place and are encouraged to share this plan with CU*Answers Network Services to ensure that their operations can be restored in the event of an unplanned disruption.
4. CU*Answers Network Services customers should have appropriate recovery capabilities in place in the event that they are not able to operate from CU*Answers Network Services data centers.
5. CU*Answers Network Services customers that manage their own systems should establish procedures to monitor their systems activity.
6. CU*Answers Network Services customers are responsible for establishing procedures s to ensure that application and/or other content on servers are appropriate.

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 policies and procedures exist to provide internal segregation of duties.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
1.1	CU*Answers is organized in separate functional areas to provide adequate segregation of duties.	Inspected the organization model for completion, accuracy, and appropriateness to the situation.	No exceptions noted.
1.2	Job descriptions have been prepared for personnel.	Inspected employee job descriptions and verified for completeness.	No exceptions noted.
1.3	Computer operators and network administrators do not perform programming functions.	Inspected the organization model and noted the degree to which operations, network administration and programming functions are segregated.	No exceptions noted.
1.4	CU*BASE programming personnel do not perform network administration or operations duties.	Inspected the organization model and noted the degree to which operations, network administration, and programming functions are segregated.	No exceptions noted.
1.5	CU*Answers 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.
		Reperformed the application of the control by selecting a sample of new employees and verifying that a signed handbook acknowledgement form was maintained in their personnel file.	No exceptions noted.
		Reperformed the application of the control by selecting a sample of employees to determine that they took the mandatory vacation days.	No exceptions noted.

Control Objective 1: 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**
1.6	CU*BASE computer operators, network administrators, programmers, and customer service personnel have at least five consecutive days away from job functions each year.	Reperformed the application of the control by selecting a sample of current employees and verified that attendance records indicate computer operators, network administrators, programmers, and customer service personnel have spent five consecutive days away from the company.	No exceptions noted.
1.7	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.
1.8	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 2: Organization and Administration

Control Objective 2: Controls provide reasonable assurance that CU*Answers and user functions are segregated.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
2.1	The relationship between CU*Answers and user organizations is contractual in nature.	Re-performed the application of the control by selecting a sample of user organizations processed by CU*Answers and verifying that a current signed contract is maintained on file.	No exceptions noted.
2.2	Operations, programming, and network administrators do not initiate or authorize transactions.	Inspected CU*Answers policies and procedures of the service organization and made inquiries of management regarding standards for initiating or authorizing transactions.	No exceptions noted.

Control Objective 3: Organization and Administration

Control Objective 3: Controls provide reasonable assurance that data processing activities are independently reviewed and tested.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
3.1	CU*Answers monitors and audits activities including program moves, DFUs, user activity, terminal security, and off-site and on-site tape backup libraries.	Inspected internal audit reports and verified program moves, DFUs, User activity, terminal security, and off-site and on-site tape backup libraries are included in the reviews.	No exceptions noted.
3.2	CU*Answers provides the results of the Internal audit and regulatory reports to the Board for review.	Inspected Board Meeting minutes and verified that audit reports are presented to the Board for oversight.	No exceptions noted.
3.3	CU*Answers 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 example logs and verified they are reviewed on a daily basis.	No exceptions noted.
3.4	On an annual basis, management reviews and develops strategic plans for the upcoming year. In addition, prior year's major accomplishments are analyzed and compared to the strategic plan.	Inspected the Business Plan for the current year and verified completeness.	No exceptions noted.

Control Objective 4: Backup and Recovery Procedures

Control Objective 4: Controls provide reasonable assurance that backup procedures and current off-site storage of important files exist, as well as a formal disaster recovery plan.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
4.1	Significant files and programs are backed up daily. A file retention schedule and a schedule for off premise rotation of master files and programs have been established.	Reperformed the application of the control and verified the off-site presence and timeliness of the following backups: • Masterfiles • Program Source Code • Program Object Code • Operating System Code	No exceptions noted.
4.2	A formal written disaster plan has been prepared and testing has been performed.	Inspected the disaster recovery plan and verified completeness.	No exceptions noted.
		Inspected disaster recovery test results and verified that recovery procedures were adequately tested.	No exceptions noted.
4.3	CU*Answers has a hot-site agreement to provide equipment and facilities backup should the service organization site be destroyed or rendered inoperable.	Inspected the hot-site agreement and verified it is current and provides equipment and facilities if a disaster were to occur.	No exceptions noted.
4.4	All critical systems and applications on Intel (server) network are backed up daily. A file retention schedule and a schedule for off premise rotation of system and/or application have been established.	Reperformed the control by selecting a sample of days and verifying network daily checklist were completed and logs of network server backups were present.	No exceptions noted.
4.5	Significant files and programs are replicated in real time using iTera disk to disk replication. Management completes the iTera HA Daily Tasks List to monitor replication status.	Reperformed the control by selecting a sample of days and verified that iTera Daily Tasks Lists were present, and completed.	No exceptions noted.

Control Objective 5: Backup and Recovery Procedures

Control Objective 5: Controls provide reasonable assurance that insurance coverage exists relative to loss of equipment, records, and data processing capability.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
5.1	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 copies of IS insurance policies and noted that effective dates and related coverage were current.	No exceptions noted.
		Confirmed coverage with third party carrier and verified that coverage noted in the confirmation agreed to the policies reviewed.	No exceptions noted.

Control Objective 6: Computer Operations

Control Objective 6: Controls provide reasonable assurance that changes to system software are authorized, tested, and reviewed, prior to implementation.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
6.1	Control features within all network operating systems and managed hosting networks note any hardware errors.	Inspected network operating system and hosting network procedures and verified alerts are in place for any hardware errors.	No exceptions noted.
6.2	New versions of the operating system are implemented by the operations personnel and have the authorization of management prior to implementation.	Inspected the Operations Implementation and the Change Request policy and verified that procedures exist for system software implementation and that management authorization is required prior to implementation into the production environment.	No exceptions noted.
6.3	Operating system revisions are normally accomplished during a period where minimal processing activity is expected.	Inspected the SDLC policy and verified operating systems revisions are installed during a period of minimal processing activity.	No exceptions noted.
6.4	New versions of network and server operating systems are implemented by network administrators and have the authorization of management prior to implementation.	Inspected the SDLC policy and verified operating systems revisions are implemented by the network administrator based on authorization from management.	No exceptions noted.

Control Objective 7: Computer Operations

Control Objective 7: Controls provide reasonable assurance that computer operations and data control procedures are used to help ensure complete, authorized and accurate processing.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
7.1	The operations department utilizes a daily checklist for processing. The checklist are reviewed by the operations manager for completeness.	Reperformed the application of the control by selecting a sample of days during the period and verified a daily processing checklist was present, complete, and reviewed.	No exceptions noted.
7.2	The daily checklist is used by operators to document that necessary files have been backed up.	Inspected a daily processing checklist and verified the operator must document the backup process.	No exceptions noted.
7.3	The Internal Network department utilizes a daily checklist for system and device monitoring.	Reperformed the application of the control by selecting a sample of days and verified a daily processing checklist was present, complete, and reviewed.	No exceptions noted.
7.4	A summary system exception log is reviewed by CU*Answers management on a daily basis.	Reperformed the application of the control by selecting a sample of days and verified a daily processing checklist was present, complete, and reviewed.	No exceptions noted.
7.5	For incoming ACH, totals from FEDLINE are compared to system totals prior to processing.	Inspected the run sheets and inquired with Assistant Operations Manager and verified that the totals from FEDLINE are compared to system totals before processing begins.	No exceptions noted.
7.6	Operations personnel perform preventive maintenance as needed.	Inspected preventative maintenance procedures and inquired with Assistant Operations Manager and verified preventative maintenance is performed as needed.	No exceptions noted.
7.7	Network administrators perform preventative maintenance as needed.	Inspected preventative maintenance procedures and inquired with Network Services Manager and verified preventative maintenance is performed as needed.	No exceptions noted.

Control Objective 7: Controls provide reasonable assurance that computer operations and data control procedures are used to help ensure complete, authorized and accurate processing.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
7.8	Processing is controlled by job streams so that prior processing steps are completed before proceeding with the next processing step.	Inspected the operations job processing procedures and inquired with Assistant Operations Manager and verified prior processing steps must be completed before next steps can begin.	No exceptions noted.
7.9	The tape library is organized and all tapes are properly labeled.	Inspected tape labels within the tape libraries documents and inquired with Assistant Operations Manager and verified the necessary procedures related to tape labeling.	No exceptions noted.
7.10	Output reports and customer statements are downloaded to CD-ROM for use by user financial institutions.	Inspected with Assistant Operations Manager, the necessary procedures related for ensuring that all reports are downloaded to CD-ROM.	No exceptions noted.
7.11	System restart/ rerun procedures are in place and assist in the proper recovery of application processing should a program abnormally terminate.	Inspected the operations job processing procedures and inquired with Assistant Operations Manager and verified that the system restart/ rerun procedures are implemented when program abnormalities have occurred.	No exceptions noted.
7.12	Control features within the operating system software note any hardware errors occurring during processing.	Inspected an example of a robot message and inquired with Assistant Operations Manager and verified any hardware malfunctions that may occur are brought to management's attention.	No exceptions noted.
7.13	The computer hardware is maintained under contract with the hardware vendor.	Inspected the "Server Asset Inventory" and verified computer hardware is maintained under contracts.	No exceptions noted.

Control Objective 8: On-Line Security

Control Objective 8: Controls provide reasonable assurance that on-line security measures should provide the ability to restrict users to the data files and menu functions to which they are authorized.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
8.1	Data communication lines are either dedicated lines or dial-up lines that are both being monitored.	Inspected network documentation and inquired with Manager of Network Engineering and Implementations and verified security concerning data communications.	No exceptions noted.
8.2	Each terminal device is identified with a unique hardware address that must be recognized and validated by the security system before any incoming transaction is processed.	Inspected i-Series security reports and inquired with i-Series Administrator about the capabilities within the operating system software and verified terminal addresses for validity and that each terminal corresponds to appropriate user.	No exceptions noted.
8.3	The on-line applications require valid passwords to identify the user financial institution employees.	Inspected the User Profile Listing and verified that access to sensitive functions within operating systems is restricted to only authorized personnel and require valid passwords	No exceptions noted.
8.4	Access to sensitive functions within operating system is restricted to authorize users.	Inspected the User Profile Listing and verified that only authorized users have access to system commands.	No exceptions noted.
8.5	User organizations have access to only the information for their institution and cannot access data of other institutions.	Reperformed the control by selecting a sample of client organizations data libraries and verified that access is to the client organization data libraries are appropriately restricted.	No exceptions noted.
8.6	The on-line processing system provides the ability to restrict user organization employees to menus and functions to which they are authorized.	Inspected security set-up within software application to confirm that employees are restricted by menus available to them based on their requested access.	No exceptions noted.
8.7	The on-line applications require valid passwords to identify CU*Answers employees.	Inspected the User Profile Listing and verified that user identifications are restricted to only the required access.	No exceptions noted.
8.8	Access for terminated employee is removed from the system in a timely manner.	Reperformed the control by selecting a sample of terminated employees and verified they do not have access to the system.	No exceptions noted.

Control Objective 8: Controls provide reasonable assurance that on-line security measures should provide the ability to restrict users to the data files and menu functions to which they are authorized.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
8.9	Program source code is not installed on the CU*BASE computer operation's production system.	Inspected procedures that prohibit testing in production environment.	No exceptions noted.
8.10	Access to source code stored on the development i-Series is restricted to appropriate individuals.	Reperformed the control by inspecting the user profile listing and verified that only authorized users have access to source code.	No exceptions noted.
8.11	A third party audit tool is used to monitor sensitive system activity.	Inspected reports generated by the third party audit tool, iSecurity to confirm that a third party audit tool is used to monitor system activity.	No exceptions noted.

Control Objective 9: Physical Security

Control Objective 9: 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**
9.1	All doors to the service organizations main and backup facility are locked and controlled by a security system.	Observed security systems and inspected the Physical Security Policy and verified doors are secured.	No exceptions noted.
9.2	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.
9.3	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.
9.4	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 CU*Answers, Kentwood and Muskegon 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.
9.5	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 9: 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**
9.6	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 CU*Answers, Kentwood and Muskegon computer rooms and noted the presence and location of an UPS system.	No exceptions noted.
		Inspected the results of the last UPS inspections for each facility and verified both UPS systems are being maintained.	No exceptions noted.
9.7	A natural gas generator is installed at each facility to protect the buildings from power failures.	Toured the service organization's CU*Answers, Kentwood and Muskegon facilities 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 last generator inspections for each facility and verified both generators are being maintained.	No exceptions noted.

Control Objective 10: e-Business Policies and Procedures

Control Objective 10: 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**
10.1	Policies and procedures for e-Business activities are documented, reviewed by management, and provided to CU*Answers staff.	Inspected the e-Business policy documents and inquired with Manager of Network Engineering and Implementations to verify procedures are documented.	No exceptions noted.
10.2	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 the monitoring controls.	No exceptions noted.
10.3	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 control by selecting a sample of days and verified that firewall activity was logged and reviewed.	No exceptions noted.
10.4	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.
10.5	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.
10.6	CU*Answers security administrators review the network server systems and devices on a daily basis to detect inappropriate or unauthorized activity on the system.	Reperformed the control by selecting a sample of days and verified the review of network server systems logs was performed.	No exceptions noted.

Control Objective 10: 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**
10.7	CU*Answers follows a change control procedure for firewall rule base changes and all policy changes are approved by management.	Reperformed the control by selecting a sample of firewall changes and verified firewall rule change review was performed.	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.