



**REPORT ON CONTROLS
PLACED IN OPERATION AND
TESTS OF OPERATING EFFECTIVENESS
FOR CU*BASE DEVELOPMENT**

For the Period

July 1, 2008 through December 31, 2008



South Bend, Indiana 46601
<http://www.crowehorwath.com>



**REPORT ON CONTROLS
PLACED IN OPERATION AND
TESTS OF OPERATING EFFECTIVENESS**

**For the Period
July 1, 2008 through December 31, 2008**

Table of Contents

REPORT OF INDEPENDENT ACCOUNTANTS	1
DESCRIPTION OF CONTROLS PLACED IN OPERATION	
<i>Provided By CU*Answers, Inc.</i>	
OVERVIEW OF OPERATIONS	3
GENERAL CONTROLS	5
Organization and Administration	5
Backup and Recovery Procedures	6
Application Development, Maintenance, and Documentation.....	7
On-line Security	14
Physical Security	15
e-Business Policies and Procedures.....	16
APPENDICES	
Appendix A - Tests of Operating Effectiveness.....	17
Appendix B - User Control Considerations	31
Appendix C - Organizational Chart.....	34



REPORT OF INDEPENDENT ACCOUNTANTS

CU*Answers, Inc.
Grand Rapids, Michigan

We have examined the accompanying "Description of Controls Placed in Operation" related to the development of the CU*BASE application of CU*Answers, Inc. (CU*Answers). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of CU*Answers' controls related to the CU*BASE application that may be relevant to a user organization's internal control as it relates to an audit of financial statements, (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of CU*BASE controls and (3) such controls had been placed in operation as of December 31, 2008. The control objectives were specified by CU*Answers. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned application presents fairly, in all material respects, the relevant aspects of CU*Answers' controls related to the development of the CU*BASE application that had been placed in operation as of December 31, 2008. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of CU*Answers' controls related to the CU*BASE application.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in Appendix A, to obtain evidence about their effectiveness in meeting the control objectives, described in Appendix A, during the period from July 1, 2008 to December 31, 2008. The specific controls and the nature, timing, extent, and results of the tests are listed in Appendix A. This information has been provided to user organizations of the CU*BASE application at CU*Answers and to their auditors to be taken into consideration, along with information about the internal control at user organizations, when making assessments of control risk for user organizations. In our opinion, the controls that were tested, as described in Appendix A, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Appendix A were achieved during the period from July 1, 2008 to December 31, 2008. However, the scope of our engagement did not include tests to determine whether control objectives not listed in Appendix A were achieved; accordingly, we express no opinion on the achievement of control objectives not included in Appendix A.

The relative effectiveness and significance of specific controls for the CU*BASE application at CU*Answers and their effect on assessments of control risk at user organizations are dependent on their interaction with the controls and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of controls at individual user organizations.

The description of controls for the development of the CU*BASE application at CU*Answers is as of December 31, 2008, and information about tests of the operating effectiveness of specified controls covers the period from July 1, 2008 to December 31, 2008. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specified controls for the development of the CU*BASE application at CU*Answers is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes may alter the validity of such conclusions.

This report is intended solely for the use of management of CU*Answers, its customers, qualified prospects, and the independent auditors of its customers.

A handwritten signature in black ink that reads "Crowe Horwath LLP". The signature is written in a cursive, flowing style.

Crowe Horwath LLP

South Bend, Indiana
March 13, 2009

**DESCRIPTION OF CONTROLS PLACED IN OPERATION
PROVIDED BY CU*ANSWERS, INC.**

OVERVIEW OF OPERATIONS

CU*Answers, Inc., formerly West Michigan Computer CO-OP, Inc. (WESCO) is a data processing service organization chartered as both a Credit Union Service Organization (CUSO) and a cooperative. The organization is currently owned by 77 credit unions. Each credit union represents only one leadership vote, and has the right to be represented by its 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. This style of direction creates a client-focused organization with an emphasis on services that are consultative, credit union industry focused, and dedicated to a "think tank" approach to data processing services and their application.

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 currently servicing 114 credit unions representing approximately 935,000 members. CU*BASE services are delivered through both on-line processing (105 credit unions) from CU*Answers' Kentwood, Michigan processing center or directly to in-house (self-processing) credit union sites (9 credit unions) located in 15 different states. The CU*BASE software features accommodate full credit union staff operations from the receptionist (interoffice communications) to the teller, member services including lending, and the CEO. 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 and Home Banking options. The CU*BASE software package is designed to run on the IBM iSeries 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 for its production iSeries computer. Data is replicated in real-time from the production system at the Kentwood data center to an identical high availability system at the Grand Rapids data center over a private fiber high speed connection. Roll-over testing is preformed quarterly where full client volumes are processed on the high availability system for at least one full processing day.

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, Direct Deposit and Check 21 services through its Kentwood, Kalamazoo and Saginaw, Michigan offices to 108 Michigan-based credit unions.

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

**DESCRIPTION OF CONTROLS PLACED IN OPERATION
PROVIDED BY CU*ANSWERS, INC.**

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.

CU*Answers is able to allocate significant resources to client service and education because of a Board directive to control growth to a maximum of ten to fifteen new client conversions annually. The motto, "CU*Answers will never sacrifice service to its current clients for the potential of tomorrow's sale" is a driving force behind CU*Answers' operational strategies. Both the CU*Answers management team and its Board of Directors view each new client as a potential partner, not just a new client relationship.

A professional staff with a comprehensive blend of credit union industry and technical experience supports CU*Answers' services. The organization is divided into two major divisions: the *Client Services Division* which focuses on direct client contact and solution development and the *Technical Services Division* which focuses on the technical disciplines required to run an effective business entity.

Key Client Services Division leaders were added to the organization based on their direct credit union experience with the CU*BASE product line and daily credit union operations. These leaders are encouraged to lead other staff members by using their visions of how they wish past data processing vendors would have provided service.

The Technical Services Division focuses on providing services 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. The Technical Division also includes accounting, marketing, and administration specialists that focus on their interest in 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.

Identification of Control Objectives and Tests of Operating Effectiveness related to the descriptions provided within this section are listed in Appendix A.

User Control Considerations which complement the internal controls of CU*Answers are listed in Appendix B.

**DESCRIPTION OF CONTROLS PLACED IN OPERATION
PROVIDED BY CU*ANSWERS, INC.**

GENERAL CONTROLS

General Controls are those policies, procedures, and safeguards which relate to all Information Systems (IS) activities. They include Organization and Administration, Application Development, Maintenance and Documentation, On-Line Security, Physical Security, and e-Business Policies and Procedures.

Application Software Maintenance is described by the Software Development Life Cycle (SDLC) which includes: Development Standards and Procedures, Programming Standards and Guidelines, Testing, and Quality Control.

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

The company is organized into eight functional groups: Administration/Human Resources Marketing, Technical Resources (Programming, Internal Networks & Software Design), Client Service, Item Processing (CU*CHECK), Finance (Business Development and Accounting), Product Team (Documentation, Quality Control, Compliance), and Operations. For reference purposes, *Appendix C: Organizational Chart* is included. Either an Officer, Vice President or Department Manager controls each group, with each Vice President or Manager reporting directly to the Senior Management Team.

Currently, CU*Answers has 77 current credit union owners and has been organized as a credit union owned CUSO since 1970. A seven-member Board of Directors meets regularly to review company status. Each June, 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 has been conducted for more than ten years, and is also held in June. Additionally, interactive client Focus Group 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.

**DESCRIPTION OF CONTROLS PLACED IN OPERATION
PROVIDED BY CU*ANSWERS, INC.**

Planning activities are on going 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.

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 which include discussions concerning employee training, benefits, audit issues, goals and strategic plans, as well as other corporate issues.

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.

Backup and Recovery Procedures

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. Complete policy and procedures for Production and Development system backups are documented and maintained in the "SOP - Operations Media Retention and Management. 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 CIO and CFO. Upon approval, the SOP is updated and the change is logged in the change history which is included as a part of the SOP document.

Daily backups are performed for all Intel-based servers including facilities management clients. Backups are written to high speed disk drives using Network Attached Storage (NAS) devices and maintained for up to 10 days. Daily backups of the NAS devices are made to tape. Tapes are maintained offsite for 14 days then returned to the originating facility for reuse.

DESCRIPTION OF CONTROLS PLACED IN OPERATION PROVIDED BY CU*ANSWERS, INC.

Application Development, Maintenance, and Documentation

Software development and maintenance at CU*Answers is geared toward providing all credit unions with three releases each year: one in the spring, fall, and end of year. Each release is comprised of software corrections, regulatory changes, and application enhancements. Software corrections are also released several times during the year in the form of “program temporary fix” (PTF) releases. PTFs are made part of the on-line credit union’s PTF library as they are completed. The contents of the PTF library are then moved to the base CU*BASE library once per year. In-house credit unions also receive PTFs throughout the year. Their PTF library is moved to their CU*BASE library only once during the year. Throughout the year, individual programs may also be provided to those credit unions that request custom enhancements.

Organizational Support

Functional units within CU*Answers involved in software development and maintenance includes:

- Client Service - Personnel who provide direct user support.
- Programming - Analysts and programmers responsible for the development and maintenance of software modules.
- Quality Control - Personnel responsible for the testing and quality of software modules.
- Product Development Team and Technical Writers - Personnel who develop and maintain user documentation.

Project Tracking

Projects are categorized into four main areas: Conversions, Program Modifications, Design Change/Enhancement Requests, and Special Job Requests. For each project, a project-tracking sheet is used to document key information such as the originating credit union, submission date, client service contact, system/program involved, type of problem, and description of the problem or change request. All changes are automatically assigned a project number and are assigned to different categories, depending on the type of change (i.e., software corrections, enhancements, custom requests). Clients are able to view the status of specific requests via a network link to Project Monitor.

CU*Answers personnel enter both reported problems and requested enhancements into a central database. The database is used to categorize the reports, provide a means of communication with the group, and to help in analyzing similar issues. In addition, codes are assigned which indicate a report’s current stage in the process.

**DESCRIPTION OF CONTROLS PLACED IN OPERATION
PROVIDED BY CU*ANSWERS, INC.**

After being logged into the database, Special Job Requests are given directly to the CIO or Programming Manager. In the event that custom programming is required, the CIO or Programming Manager, along with the Product Development Team, will establish estimated time frames as well as cost to the client. The requests are categorized for department responsibility and assigned. Once approved by the CIO or Programming Manager and the credit union, the request is forwarded to Quality Control for monitoring and testing in accordance with established guidelines.

Program Modifications and Design/Enhancement Requests are given to either the CEO or the Product Team Manager for evaluation. Each item is evaluated to determine which of three courses of action is appropriate: further investigation required, no action to be taken, or action recommended.

Results of the evaluation are logged into the database and the report is routed to the appropriate person with a recommended action: research, refused, priority fix, tabled fix, priority development, tabled development or education required. The recommendation is then carried out and the client is made aware of the determination.

A project control database has been designed to accommodate project information as well as to produce management reports for tracking project time lines and workload projections. All projects will be entered into this database. A weekly report will be produced to show each programmer's assigned projects, the number of hours worked during the past week, the target date, the total hours estimated, and the percent complete.

Procedures Unique to Specific Types of Changes

Software Corrections

Credit Unions typically communicate requests for software corrections to Client Service personnel. Upon receipt, each problem is evaluated to determine the necessity of documenting the problem on a project-tracking sheet. If it is determined that the problem requires a software correction, Client Service will transfer the project to the Product Team or CEO to perform initial analysis of each requested software correction by attempting to verify that the issue was indeed due to the software, and not due to hardware or operating procedure problems.

Once it has been determined that the issue requires a software correction, the project tracking sheet is assigned for programming. Based on the initial analysis of the software correction, the CEO, CIO or Product Team Manager will indicate the priority of the software correction on the problem-tracking sheet, and then it may be reported to Client Service for client contact. Priorities for these corrections are considered during the review of outstanding projects. The Programming Manager maintains a calendar of outstanding projects for each programmer.

**DESCRIPTION OF CONTROLS PLACED IN OPERATION
PROVIDED BY CU*ANSWERS, INC.**

Software corrections are assigned to programmers for correction and testing by Quality Control. Once completed, the programmer will create a Software Modification/Completion form, which is then reviewed by Quality Control. This review details the files that have been modified and moved to the beta or project library for further testing.

Once approved by Quality Control, the program change will be included with the next software release. However, in the event the correction encompasses a limited PTF change or Special Job Request, the change will be released immediately. If the correction is considered critical to operations and an acceptable alternative method to work around the problem cannot be found, the CIO or Programming Manager may send software corrections electronically before Quality Control tests the corrections. In these cases, Quality Control will still test the corrections after they have been sent to the credit union.

Custom Changes

Requests for custom changes can be communicated by phone call or correspondence from credit unions to Client Service personnel. Client Service personnel fill out a project tracking sheet and forward it to the CIO or Programming Manager for determination of cost, timing, and feasibility for the custom change. Once approved by the CIO or Programming Manager and approved by the client, the project-tracking sheet is then assigned to a programmer. Projects are closed out after the expired bid date if the credit union does not send its approval.

The CIO and Programming Manager are in charge of custom changes and are responsible for assigning a programmer to these approved projects. Programmers perform modifications, conduct limited testing and develop program documentation. Due to the unique nature and often-limited applicability of custom modifications, program documentation may consist of only the analyst's notes and the program itself. Upon completion by the programmer and testing by Quality Control, the custom change is released to the credit union for testing. Once the credit union is satisfied with the change, the project-tracking sheet is returned to Quality Control Department to prepare the billing paperwork which will be submitted to Accounting. After this procedure is completed, the project is closed.

Enhancements

Suggestions for enhancements are typically received from user group meetings, electronic Idea forms to the CEO, phone calls to Client Service, or staff suggestions. As each request is received, an Enhancement/Design Change form is created and reviewed by the CEO and the Product Team Manager. Enhancements may also be discussed at the user group meetings where further recommendations may be considered. All approved enhancements are also prioritized. The project tracking sheets associated with the enhancements that were accepted are assigned and distributed to the writing team to provide specifications as necessary. Those that were rejected are assigned to the originator of the request for client notification.

**DESCRIPTION OF CONTROLS PLACED IN OPERATION
PROVIDED BY CU*ANSWERS, INC.**

Once a project is approved and specifications are complete, it is then forwarded to the CIO or Programming Manager who then assigns the project to a programmer. The programmer may work with one or more credit unions requesting the enhancement to complete the project. The programmer is responsible for completing the change, doing the preliminary testing, and updating any internal programming documentation as necessary. Once these steps are complete, the programmer creates a project modification/completion form, which includes instructions for testing the change, and any documentation he or she feels would be useful to the technical writer in updating the user documentation. The problem tracking sheets automatically go to Quality Control to test the change and to the technical writer to update documentation. Enhancements are tested by Quality Control and are distributed to the credit unions in the next software release.

Standards and Procedures

Software development and maintenance documentation includes:

- Software Development Life Cycle (SDLC)
- Testing and Quality Control Procedures
- Programming Standards and Guidelines
- Data Security Policy

The above listed documentation contains all the material required for the orderly and consistent renovation of the CU*BASE product. These documents are also designed to provide guidance to the programming staff in the standardization of one program to the next. The other reference tools describe procedures to be followed by the documentation and quality control teams.

Documentation

User documentation in the CU*BASE application is maintained by the documentation department. This documentation is communicated through the CU*BASE online and Internet reference library. Other user documentation includes topical procedural booklets that serve in most cases as a temporary document.

Software development and changes are documented both within the program and on the project and design specification sheets. Program narratives and/or revision statements typically exist to describe the overall functionality of each program. Documentation may include: analyst's notes, input/output specifications, testing procedures, and user documentation. Documentation required for each change depends on the nature and complexity of each change.

**DESCRIPTION OF CONTROLS PLACED IN OPERATION
PROVIDED BY CU*ANSWERS, INC.**

A technical writer reviews the project tracking sheet for user documentation issues noted by the programmer. These notes are refined and formatted to be included in the appropriate user manual. If user documentation is not addressed in the project tracking sheet, a technical writer will review the program related notes to determine whether user documentation requires updating, and will then update the appropriate user manual.

Quality Control

Quality control of the CU*BASE product is maintained from the inception of the project tracking sheet to the implementation of the final product. Quality Control personnel review the project, before it is assigned to programming, utilizing the procedures outlined in the SDLC. Upon completion of program modification and limited testing by programmers, all changes are sent to Quality Control using the project tracking sheets. Depending on the nature of the change, programmers may perform significant testing on their own prior to submitting the program changes to Quality Control.

The programmer moves the programs into the "BETA" or project library and forwards the Problem Report to Quality Control. Technical Resources then executes a complete rebuild of the CU*BASE database such that all source modules, screens, and other files are included in a test of the entire system. If the program change is anything other than a PTF and passes the Quality Control testing, the program is moved into the upcoming "release" library. If the program change fails the testing, Quality Control notes the rejection on the Quality Control Test Problem Tracking form which also documents the reasons for the failure. The failure is then reported to the programmer. The program is then fixed by the programmer and resubmitted for Quality Control review.

Upon completion of each change, Quality Control must approve the program before it can be added to the appropriate release library. Quality Control reviews weekly any changes with the following status:

- Initial specifications being written
- Specifications completed waiting to be assigned
- Programming
- Quality Control testing
- Beta site testing
- Completed awaiting implementation

Program Release

Programs are placed into a beta library based on the version and the updates required. The project-tracking sheet is routed to the technical writing staff for documentation changes or to Client Service for client notification via regular newsletters.

DESCRIPTION OF CONTROLS PLACED IN OPERATION PROVIDED BY CU*ANSWERS, INC.

Release Preparation

Preparation of each release begins four to five months prior to the expected release date. CU*Answers personnel meet to develop release strategy. Based on the requests approved by the Product Team, reported software corrections, and regulatory changes, management assembles the detailed plans for the release. The key personnel involved include the CEO, CIO, programming manager, technical writing staff, Product Team Manager, and VP of Client Services, as well as the Quality Control leader, programmers, and analysts working on major portions of the release.

All project -tracking sheets are formally reviewed and prioritized as a basis for developing the next release. By their nature, most of the regulatory changes are implemented prior to the regulatory changes becoming effective. Additionally, on a monthly basis, the problem tracking sheet log is reviewed to note any necessary changes in priority. A formal release date is established based on the desired release date, the time frame for analysis, programming, documentation and testing. Release dates may be different for on-line and in-house credit unions.

Beta Site Testing

Beta testing is conducted with the voluntary assistance of a select group of credit unions. These credit unions have all the modules installed so that the beta site testing covers the complete range of modules offered. Typically, it is not the same credit unions that volunteer each time, but rather those who have a particular interest in the changes planned within the next release. Beta test procedures of the planned release are provided to the credit union along with user tools and documentation for the usage and testing of the release. Quality Control and credit union personnel conduct frequent discussions during the beta site testing period to review any problems noted.

Software problems are recorded on a Problem Report and reported to both Quality Control and Programming. The logged problems are subject to the same controls and procedures for handling other software related problems. These problems are given the highest priority. Once the beta site has finished its review of the release, in some cases the credit union fills out a Beta Site User Acceptance Form and submits it to Quality Control for final review.

Announcement of Releases

In the months immediately preceding the release, users are informed of the major planned enhancements through newsletters and user group meetings. Topical documentation is provided several weeks in advance of the release to describe all enhancements, corrections, regulatory changes and configuration changes. A meeting of all Client Service personnel is held prior to the distribution of the release to ensure their ability to provide effective support to users.

**DESCRIPTION OF CONTROLS PLACED IN OPERATION
PROVIDED BY CU*ANSWERS, INC.**

Distribution of Releases

After completion of beta testing, documentation and training of Client Service personnel, the procedures for release distribution begin.

On-Line

For on-line credit unions, Technical Resources implement releases for all credit unions on the designated release date, usually over a weekend. To ensure all programs from the release library are included and all updates are made correctly, the Programming Manager maintains a "checklist" of programs to be included in the update. The checklist is compiled using information provided by programmers as the various projects included in the release were completed.

In-House

For in-house processors, Technical Resources creates a standard release package for each credit union from the appropriate release library. Technical Resources ensures that the credit union receives the release (either via tape media or a transmission via their Extended Business Network line), release notes and any release user documentation (if it was not already sent to the credit union) approximately a week prior to implementation.

Technical Resources personnel normally perform software updates on dates mutually agreed upon by CU*Answers and senior credit union management. Technical Resources staff may access the credit union system remotely and load the software updates or the credit union can follow the Release Instructions/Procedures and perform the upgrade themselves. This procedure is based on specific credit union information relating to the current operating system version.

Distribution of Single Programs

Individual programs may be distributed directly to specific credit unions at any time throughout the year to the on-line custom or PTF libraries via either magnetic tape or modem. These program distributions are preceded by a problem tracking sheet. Listed below are examples of when special distribution would be necessary:

- Enhancement/Design Change modules for beta testing based on special credit union requests.
- Custom software or urgent software corrections reported by users.

**DESCRIPTION OF CONTROLS PLACED IN OPERATION
PROVIDED BY CU*ANSWERS, INC.**

For in-house credit unions, the programming transfer takes place via communication links or tape to the user credit union system. To facilitate tracking of single program transmissions, CU*Answers utilizes a "CU*BASE Credit Union Library Control" log. The CIO maintains this log.

On-Line Security

There are two levels of security used by client credit unions: AS/400 terminal access security and CU*BASE application security.

As users enter a user identification name and password to access the Service Center's 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. Most communication links are either through dedicated leased lines or MPLS. Dial-up capability is available and is password controlled. In addition, a thirty minute automatic time-out feature is set to prevent users from leaving terminals unattended and logged into the AS/400 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.

The CU*Answers Security Administrator maintains AS/400 terminal access security for both internal users and credit unions. An Account Maintenance Form is used to notify the Security Administrator of all internal additions, modifications, and deletions to security. 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. Credit unions are responsible for maintaining CU*BASE application security after it has been originally established.

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.

**DESCRIPTION OF CONTROLS PLACED IN OPERATION
PROVIDED BY CU*ANSWERS, INC.**

Physical Security

The CU*Answers Kentwood Service 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 "visitor" 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 building security officer maintains a log of all keys and their numbers.

The CU*Answers Grand Rapids Service 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. 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 "visitor" 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 building security officer maintains a log of all keys and their numbers.

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

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

The buildings are also protected against fire by hand held extinguishers. These extinguishers are inspected in February of each year and may be used on electrical devices, liquids, and other combustible materials.

Emergency battery powered lighting, activated when the power is cut off, is located throughout both of the 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 approximately 40 minutes in the event of a power failure. Two natural gas powered electric generators are in place 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.

**DESCRIPTION OF CONTROLS PLACED IN OPERATION
PROVIDED BY CU*ANSWERS, INC.**

e-Business Policies and Procedures

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 a knowledgeable network administrators experienced in applying security best practices to network resources. Our IT staff continuously monitors CERT and other third party advisories for the latest security bulletins and alerts in addition to 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 iSeries, Intel-based, and facilities management 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 updated hourly, 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 an independent firm to perform periodic external and internal penetration tests. These assessments identify potential targets on Internet accessible devices, 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 implements necessary recommendations as suggested.

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, our 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.”

**APPENDIX A
ORGANIZATION AND ADMINISTRATION**

CONTROL OBJECTIVE -- CU*Answers is organized to provide internal segregation of duties.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>CU*Answers is organized in separate functional areas to provide adequate segregation of duties.</p> <p>Computer operators and network administrators do not perform programming functions.</p> <p>CU*BASE programming personnel do not perform network administration or operations duties.</p> <p>CU*BASE computer operators, network administrators, programmers, and customer service personnel have at least five consecutive days away from job functions each year.</p>	<ol style="list-style-type: none"> 1. Reviewed the organization chart for completion, accuracy, and appropriateness to the situation. 2. Reviewed the organization chart noting the degree to which operations/programming functions are segregated. 3. Interviewed CU*BASE computer operations management to determine adherence to policy. 4. Reviewed the organization chart noting the degree to which operations/programming functions are segregated. 5. Interviewed CU*BASE programming management to determine adherence to policy. 6. Verified that attendance records indicate computer operators, network administrators, programmers, and customer service personnel have spent five consecutive days away from work. 	<p>Inspected documents and reports indicating performance of the control.</p> <p>Inspected documents and reports indicating performance of the control.</p> <p>Made inquiries of appropriate company personnel.</p> <p>Inspected documents and reports indicating performance of the control.</p> <p>Made inquiries of appropriate company personnel.</p> <p>Inspected documents and reports indicating performance of the controls by selecting a sample of current employees and reviewing attendance records for indication of five consecutive days away from the job.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

**APPENDIX A
ORGANIZATION AND ADMINISTRATION**

CONTROL OBJECTIVE -- CU*Answers and user functions are segregated.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>The relationship between CU*Answers and user organizations is contractual in nature.</p> <p>Operations, programming, and network administrators do not initiate or authorize transactions.</p>	<ol style="list-style-type: none"> 1. Reviewed policies of the service organization and contractual obligations that exist between the service organization and user organization. 2. Verified contracts were signed and had been executed. 3. Reviewed the policies and procedures of the service organization. 	<p>Made inquiries of appropriate company personnel and inspected documents and reports indicating performance of the control.</p> <p>Reperformed the application of the controls by selecting a sample of user organizations processed by CU*Answers and verifying that a current signed contract is maintained on file.</p> <p>Made inquiries of appropriate company personnel and inspected documents and reports indicating performance of the control.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

**APPENDIX A
ORGANIZATION AND ADMINISTRATION**

CONTROL OBJECTIVE -- Data processing activities are independently reviewed and tested.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>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.</p> <p>Job descriptions have been prepared for all personnel.</p> <p>CU*Answers monitors and audits activities including program moves, DFUs, user activity, terminal security, and off-site and on-site tape backup libraries.</p> <p>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.</p>	<ol style="list-style-type: none"> 1. Ascertained that an employee handbook existed and reviewed the manual for inclusion of key policies. 2. Reviewed employee job descriptions. 3. Discussed with Internal Audit the procedures for performing audits and the methods for reporting findings. 4. Reviewed a sample of Internal Audit Checklists and verified they were completed 5. Interviewed management and reviewed policies and procedures regarding the monitoring and auditing of network systems. 	<p>Reperformed the application of the control by selecting a sample of employees and verifying that a signed handbook acknowledgement form was maintained in their personnel file.</p> <p>Inspected documents and reports indicating performance of the control.</p> <p>Made inquiries of appropriate company personnel.</p> <p>Inspected documents and reports indicating performance of the control.</p> <p>Made inquiries of appropriate company personnel and reperformed the application of the control by selecting a sample of days and verified review of network server system logs by appropriate company personnel.</p>	<p>During our review of handbook acknowledgement forms, we found that one employee did not have a signed handbook acknowledgement form in her personnel file.</p> <p><u>Management Response:</u> The signed form has been returned to the appropriate personnel file.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

**APPENDIX A
BACKUP AND RECOVERY PROCEDURES**

CONTROL OBJECTIVE -- Backup procedures and current off-site storage of important files exist.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>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.</p> <p>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.</p>	<ol style="list-style-type: none"> 1. Verified the off-site presence and timeliness of the following backups: <ul style="list-style-type: none"> ➤ Program Source Code ➤ Program Object Code ➤ Operating System Code 2. Observed the physical protection of the off-site backup location. 3. Verified the off-site presence and timeliness of the network server backups. 4. Observed the physical protection of the off-site backup location. 	<p>Reperformed the application of the control by inspecting backup tapes at the off-site facility.</p> <p>Observed application of specific controls.</p> <p>Reperformed the application of the control by inspecting backup tapes at the off-site facility.</p> <p>Observed application of specific controls.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

**APPENDIX A
BACKUP AND RECOVERY PROCEDURES**

CONTROL OBJECTIVE -- Insurance coverage exists relative to loss of equipment, records, and data processing capability.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>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.</p>	<ol style="list-style-type: none"> 1. Obtained copies of IS insurance policies and noted that effective dates and related coverages were current. 2. Confirmed coverages with all appropriate third party insurance companies. 	<p>Made inquiries of appropriate company personnel and inspected documents and reports indicating performance of the control.</p> <p>Confirmed coverages with appropriate insurance carriers.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

APPENDIX A
APPLICATION DEVELOPMENT, MAINTENANCE, AND DOCUMENTATION

CONTROL OBJECTIVE -- All program change requests should require proper authorization, have adequate implementation procedures, and provide an audit trail to facilitate future program changes.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>User-initiated and internally generated requests for program changes are entered into a database.</p> <p>Programming documentation is modified as changes occur which affect such documentation.</p> <p>Programmers determine whether user documentation needs to be updated.</p>	<ol style="list-style-type: none"> 1. Reviewed program change control procedures with management noting detailed procedures for program implementation. 2. Selected a sample of completed program change requests from the support database. 3. Verified that the project number agreed among all applicable forms. 4. Verified that program change documentation was indicated on the project request. 5. Verified that review of documentation was indicated on the request form. 	<p>Made inquiries of appropriate company personnel.</p> <p>Re-performed the application of the control by selecting a sample of completed program change requests and verified all applicable forms were present, project numbers agreed, documentation and testing completed.</p> <p>Reference prior test.</p> <p>Reference prior test.</p> <p>Reference prior test.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

APPENDIX A
APPLICATION DEVELOPMENT, MAINTENANCE, AND DOCUMENTATION

CONTROL OBJECTIVE -- All program change requests should require proper authorization, have adequate implementation procedures, and provide an audit trail to facilitate future program changes.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>Quality Control performs system testing on each program change prior to being released. For custom requests, acceptance letters are received from the credit union requesting the change.</p>	<p>6. Verified that each program change affected by the project request was tested by Quality Control and for custom requests verified that an acceptance letter was received from the credit union.</p>	<p>Reference prior test.</p>	<p>No relevant exceptions noted.</p>
<p>Programmers document a brief history of the changes performed within the source code.</p>	<p>7. Reviewed that the source code contained a brief summary of the change.</p>	<p>Inspected documents and reports indicating performance of the control.</p>	<p>No relevant exceptions noted.</p>
<p>Source code is reviewed for a sample of accepted program changes.</p>	<p>8. Reviewed source code review procedures.</p>	<p>Made inquiries of appropriate company personnel and inspected documents and reports indicating performance of the control.</p>	<p>No relevant exceptions noted.</p>
<p>Quality Control personnel move the program source into the production libraries.</p>	<p>9. Reviewed program change implementation procedures.</p>	<p>Made inquiries of appropriate company personnel and inspected documents and reports indicating performance of the control.</p>	<p>No relevant exceptions noted.</p>
<p>A new version of a revised program replaces the previous version and only one version of each program is maintained in the production library.</p>	<p>10. Reviewed program change implementation procedures.</p>	<p>Made inquiries of appropriate company personnel and inspected documents and reports indicating performance of the control.</p>	<p>No relevant exceptions noted.</p>
<p>Each major release is tested at several beta sites prior to full distribution to all users.</p>	<p>11. Discussed beta site procedures with management.</p>	<p>Made inquiries of appropriate company personnel.</p>	<p>No relevant exceptions noted.</p>

APPENDIX A
APPLICATION DEVELOPMENT, MAINTENANCE, AND DOCUMENTATION

CONTROL OBJECTIVE -- All program change requests should require proper authorization, have adequate implementation procedures, and provide an audit trail to facilitate future program changes.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>Programs in the release directories are supported by a Project Completion/Modification Notice form.</p> <p>Documentation of application systems includes system overviews, program narratives, operating instructions, data file descriptions, and user instruction manuals.</p> <p>Changes to programming and operations documentation are completed by the programmers during program modifications and updates. A checklist of documentation to be updated for each change is utilized.</p>	<p>12. Verified that source modules, which were changed, were supported by a Project Completion/Modification Notice form.</p> <p>13. Discussed documentation procedures with management.</p> <p>14. Verified the existence of an off-site copy of CU*Answers specific documentation, including operations, standards and procedures, and disaster recovery manuals.</p> <p>15. Reviewed program change procedures with management.</p>	<p>Inspected documents and reports indicating performance of the controls by selecting a sample of program source modules that were modified from the production library and traced the last modified date on these modules to the last modified date on the last accepted Project Completion Modification Notice form.</p> <p>Made inquiry of appropriate company personnel.</p> <p>Reperformed the application of the control by inspecting that there was documentation at the off-site facility.</p> <p>Made inquiries of appropriate company personnel.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

**APPENDIX A
ON-LINE SECURITY**

CONTROL OBJECTIVE -- On-line security measures should provide the ability to restrict users to the data files and menu functions to which they are authorized.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>Data communication lines are either dedicated lines or dial-up lines that are both being monitored.</p> <p>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.</p> <p>The on-line applications require valid passwords to identify the user financial institution employees.</p>	<ol style="list-style-type: none"> 1. Discussed with management security concerning data communications. 2. Discussed with management the capabilities within the system operating software to check terminal addresses for validity and to identify that each terminal corresponds to the appropriate user financial institution. 3. Verified that user identifications are restricted to only the access required and the related user identification password has an expiration interval assigned. 4. Verified that users are restricted to only the data necessary for their job responsibilities. 5. Verified that only authorized users have access to system commands. 	<p>Made inquiries of appropriate company personnel.</p> <p>Made inquiries of appropriate company personnel.</p> <p>Inspected documents and reports indicating performance of the control by selecting all users from the production system and reviewing their security profiles.</p> <p>Reference prior test.</p> <p>Reference prior test.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

**APPENDIX A
ON-LINE SECURITY**

CONTROL OBJECTIVE -- On-line security measures should provide the ability to restrict users to the data files and menu functions to which they are authorized.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>User organizations have access to only the information for their institution and cannot access data of other institutions.</p> <p>The on-line processing system provides the ability to restrict user organization employees to menus and functions to which they are authorized.</p> <p>The on-line applications require valid passwords to identify CU*Answers employees.</p> <p>Program source code is not installed on the CU*BASE computer operation's production system.</p> <p>A third party audit tool is used to monitor sensitive system activity.</p>	<p>6. Reviewed the procedures for assigning profiles provided to individual user organizations such that those users can access only their organization's information.</p> <p>7. Reviewed security set-up within the software applications.</p> <p>8. Verified that user identifications are restricted to only the access required and the related user identification password has an expiration interval assigned.</p> <p>9. Interviewed operation's management to determine if release installations include source code.</p> <p>10. Discussed with management procedures for reviewing reports produced by the third party audit tool.</p>	<p>Made inquiries of appropriate company personnel.</p> <p>Made inquiries of appropriate company personnel.</p> <p>Inspected documents and reports indicating performance of the control by selecting all users from the production and development systems and reviewing their security profiles.</p> <p>Inspected documents and reports indicating performance of the control.</p> <p>Inspected documents and reports indicating performance of the control.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

**APPENDIX A
PHYSICAL SECURITY**

CONTROL OBJECTIVE -- Safeguards and/or procedures are used to protect the service organization against intrusions, fire and other hazards.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>All doors to the service organizations main and backup facility are locked and controlled by a security system.</p> <p>Authorized personnel have been issued electronic building keys and have been given the code to deactivate the perimeter alarm system at the facilities.</p> <p>The computer rooms are locked at all times and visitors must be admitted to the area by operations personnel.</p> <p>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.</p>	<ol style="list-style-type: none"> 1. Interviewed management, reviewed policies relating to physical security procedures and devices, and schedules of operation, and observed security systems and procedures. 2. Discussed with management that only appropriate personnel have access to the buildings. 3. Observed physical security procedures throughout the audit and verified the compliance with service organization policies and procedures. 4. Toured the entire CU*Answers 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. 	<p>Made inquiries of appropriate company personnel and observed application of specific controls.</p> <p>Made inquiries of appropriate company personnel.</p> <p>Made inquiries of appropriate company personnel and observed application of specific controls.</p> <p>Observed application of specific controls.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

**APPENDIX A
PHYSICAL SECURITY**

CONTROL OBJECTIVE -- Safeguards and/or procedures are used to protect the service organization against intrusions, fire and other hazards.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
A written action plan relating to emergency situations is distributed to employees.	5. Reviewed the emergency action plan for adequacy and content. Determined 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.	Inspected documents and reports indicating performance of the control and made inquiries of appropriate company personnel.	No relevant exceptions noted.
An Uninterruptible Power Supply (UPS) system with power conditioners is installed to protect both computer room facilities from short or long-term power failures.	6. Toured the service organization and computer room and noted the presence and location of an UPS system.	Observed application of specific controls.	No relevant exceptions noted.
A natural gas generator is installed at each facility to protect the buildings from power failures.	7. Toured the service organization and noted the presence of a natural gas generator and discussed with management the weekly testing of the generator.	Observed application of specific controls and made inquiries of appropriate company personnel.	No relevant exceptions noted.

APPENDIX A
e-BUSINESS POLICIES AND PROCEDURES

CONTROL OBJECTIVE - Policies and procedures to address e-Business risk are documented, communicated, and provided to the staff.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>Policies and procedures for e-Business activities are documented, reviewed by management, and provided to CU*Answers staff.</p> <p>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.</p> <p>The firewall is set up to log suspicious and unauthorized access attempts. Network Administrators review the firewall logs on a daily basis.</p> <p>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.</p>	<ol style="list-style-type: none"> 1. Reviewed e-Business Policies and Procedure documents. 2. Discussed with management the configuration of the firewall and the monitoring controls. 3. Discussed with management policies and procedures for reviewing the firewall logs. 4. Verified procedures for reviewing the firewall logs. 5. Discussed security configurations with management and reviewed the annual Penetration Study Report. 	<p>Made inquiries of appropriate company personnel and inspected documents and reports indicating the performance of the controls.</p> <p>Made inquiries of appropriate company personnel and inspected documents and reports indicating the performance of the controls.</p> <p>Made inquiries of appropriate company personnel.</p> <p>Reperformed the application of the control by selecting a sample of days and verified review of firewall logs by appropriate company personnel.</p> <p>Made inquiries of appropriate company personnel and inspected documents and reports indicating the performance of the controls.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

APPENDIX A
e-BUSINESS POLICIES AND PROCEDURES

CONTROL OBJECTIVE - Policies and procedures to address e-Business risk are documented, communicated, and provided to the staff.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>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.</p> <p>CU*Answers security administrators review the network server systems and devices on a daily basis to detect inappropriate or unauthorized activity on the system.</p> <p>CU*Answers follows a change control procedure for firewall rule base changes and all policy changes are approved by management.</p>	<p>6. Interviewed management to determine policies and procedures regarding configuration of system logs.</p> <p>7. Interviewed management to determine policies and procedures regarding review of the system logs.</p> <p>8. Verified procedures for reviewing the network server system logs.</p> <p>9. Interviewed management and reviewed firewall policy change logs to determine policies and procedures regarding change control procedures for firewall rule base changes.</p>	<p>Made inquiries of appropriate company personnel and inspected documents and reports indicating the configuration of the system logs.</p> <p>Made inquiries of appropriate company personnel and inspected documents and reports indicating the performance of the controls.</p> <p>Reperformed the application of the control by selecting a sample of days and verified review of network server system logs by appropriate company personnel.</p> <p>Made inquiries of appropriate company personnel and inspected documents and reports indicating the configuration of the firewall.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

APPENDIX B - USER CONTROL CONSIDERATIONS

This section outlines specific User Control Considerations that may be appropriate at each user financial institution, along with the objective of the control. These considerations should not be regarded as a comprehensive list of all internal accounting controls that should be employed by users, or as representing procedures that are 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 G/L 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. Test program changes after general release to verify that results are as published.
2. 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.
3. Review operations logs on a daily basis.
4. 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.

APPENDIX B - USER CONTROL CONSIDERATIONS

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.

On-Line Security 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.

APPENDIX B - USER CONTROL CONSIDERATIONS

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 the Member File Maintenance General Transaction and Print General Ledger History reports for changes made by employee identification number 89. This identification number signifies the change was made by a CU*Answers employee.

APPENDIX C - ORGANIZATIONAL CHART

