Crowe Horwath.

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 Development

Under the AICPA, Statement on Standards for Attestation Engagements No. 16 (SSAE No. 16) Reporting on Controls at a Service Organization (SOC 1, Type 2)

For the Period January 1, 2016 to June 30, 2016

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 development services for processing user entities' transactions throughout the period January 1, 2016 to June 30, 2016, (description) and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The description indicates that 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. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

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 for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls 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. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, 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 January 1, 2016 to June 30, 2016.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description 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 those controls to achieve the related control objectives stated in the description. Our procedures included 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. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the

suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in management's assertion in Section II. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions 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 inadequate or fail.

Opinion

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

a) the description fairly presents the CU*BASE application development services that was designed and implemented throughout the period January 1, 2016 to June 30, 2016.
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 January 1, 2016 to June 30, 2016, and user entities applied the complementary user entity controls contemplated in the design of CU*Answers' controls throughout the period January 1, 2016 to June 30, 2016.
c) the controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period January 1, 2016 to June 30, 2016.

Description of Tests of Controls

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

Other Matters

The information in the section entitled "Section VI: Other Information Provided by CU*Answers, Inc." describes CU*Answers' overall company organizational model is presented by CU*Answers to provide additional information and is not a part of CU*Answers' description of controls that may be relevant to a user organization's internal control. Such information has not been subjected to the procedures applied in the examination of the description of the controls applicable to the processing of transactions for user organizations and, accordingly, we express no opinion on it.

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 CU*Answers, user entities of CU*Answers' CU*BASE application development services during some or all of the period January 1, 2016 to June 30, 2016, and the independent auditors of such user entities, who 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 misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Crowe Horwath LLP

South Bend, Indiana
October 31, 2016

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

Management's Assertion

CU*ANSWERS
A Credit Union Service Organization
6000 28th Street S.E. Ste. 100 • Grand Rapids, Michigan 49546
Phone: 616.285.5711 • 800.327.3478 • Fax: 616.285.5735

October 31, 2016

To the Users of CU*Answers CU*BASE Application Development Services:

We have prepared the description of CU*Answers, Inc. (CU*Answers) CU*BASE application development services systems (SDLC) for processing user entities' transactions for user entities of the system during some or all of the period January 1, 2016 to June 30, 2016, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that

a. the description fairly presents the CU*Answers CU*BASE application development services system made available to user entities of the system during some or all of the period January 1, 2016 to June 30, 2016, for processing their transactions. 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 transactions, including

      1. the classes of transactions processed.
      2. the procedures, within both automated and manual systems, by which those transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities of the system.
      3. the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports presented to user entities of the system.
      4. how the system captures and addresses significant events and conditions, other than transactions.
      5. the process used to prepare reports or other information provided to user entities' of the system.
      6. specified control objectives and controls designed to achieve those objectives including as applicable, complementary user entity controls contemplated in the design of the service organization's controls.
      7. other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.

WWW.CUANSWERS.COM

CU*ANSWERS
A Credit Union Service Organization
6000 28th Street S.E. Ste. 100 • Grand Rapids, Michigan 49546
Phone: 616.285.5711 • 800.327.3478 • Fax: 616.285.5735

ii. does not omit or distort information relevant to the scope of the application development services system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the application development services system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. the description includes relevant details of changes to the service organization's system during the period covered by the description when the description covers a period of time.

c. the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period January 1, 2016 to June 30, 2016, to achieve those control objectives. The criteria we used in making this assertion were that:

i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization;

ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

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

Governance

CU*Answers, Inc., is a data processing service organization incorporated under Michigan law and chartered as a Credit Union Service Organization (CUSO), and as a cooperative. Formerly known as West Michigan Computer CO-OP, Inc. (WESCO), CU*Answers has been providing core and peripheral data processing services to its client credit unions since 1970. CU*Answers is currently owned by 120 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.

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.

The corporate motto of the CU*Answers cooperative spirit is **Live It!**

Data Processing

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 approximately 170 credit unions representing more than 1,430,000 members. CU*BASE services are delivered through both on-line processing from CU*Answers' Kentwood, Michigan processing center, the Muskegon, Michigan processing center, or directly to in-house (self-processing) credit union sites. Clients using CU*BASE services are located across the country in 24 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, Online Banking and Mobile Banking options. The CU*BASE software package is designed to run on the IBM i-Series System-I (i-Series) 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 is production System-i computer. Data is replicated in real-time from the production system at the Kentwood processing center to an identical high availability system at the Muskegon processing center over a private fiber high speed connection. Roll-over testing is preformed three times per 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.

Growth Model

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.

Ancillary Services

A professional staff with a comprehensive blend of credit union industry and technical experience supports CU*Answers' services. The organization provides client services dedicated to assisting users 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.

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. 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.

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, Application Development, Maintenance and Documentation, Backup and Recovery Planning, On-Line Security, Physical Security, and e-Business Policies and Procedures.

Application Software Maintenance is described by the Software Development Life Cycle (SDLC) that 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

Controls provide reasonable assurance that CU*Answers is organized to provide internal segregation of duties.

CU*Answers is organized into eight functional groups: Leadership, General Administration, Invention, Production Area, Capture Market Share Area Teams, Client Interaction and Support, and cuasterisk.com Teams to provide internal segration 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.

Currently, CU*Answers has over 117 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.

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.

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.

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 is comprised of the Internal Auditor and the Accounting Manager. The Internal Auditor has experience in accounting, law, network infrastructure, client support, and system auditing. The intent of CU*Answers is to create the proper separation of responsibilities to ensure operations are constantly reviewed. CU*Answers approaches all audits with candid and transparent accountability to allow 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.

Internal Audit schedules external audits that include a review of the segregation of duties. CU*Answers undergoes regular regulatory examinations by state and federal authorities, and conducts its own thorough internal audits.

Backup and Recovery Procedures

Controls provide reasonable assurance that backup procedures and current off-site storage of important files exist.

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" 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 CIO and CFO. 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.

Application Development, Maintenance and Documentation

Controls provide reasonable assurance that all program change requests should require proper authorization, have adequate implementation procedures, and provide an audit trail to facilitate future program changes.

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. Regulatory changes may require amendments to the schedule. 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.

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, status changes are tracked in the database and changes are reported to both the project originator and the client.

After being logged into the database, Special Job Requests are given directly to the Programming Manager or CIO. In the event that custom programming is required, the CIO or Programming Manager 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 evaluated by senior management. 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, fix as resources allow, priority development, development as resources allow 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 senior management to perform initial analysis of each requested software correction by verifying 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 Programming 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.

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 Change

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 that 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 CIO. 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 are 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.

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 Writing Team. This documentation is communicated through CU*BASE online help. Other user documentation includes topical procedural booklets, also available online.

In addition to end user documentation, 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 notes. Documentation required for each change depends on the nature and complexity of each change.

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 that 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.

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 and 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.

Distribution of Releases to In-House Clients

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

On-Line Credit Unions

For on-line credit unions, released are implemented 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 Credit Unions

For in-house processors a standard release package for each credit union is created 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. 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.

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

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: i-Series 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 through MPLS. In addition, a thirty minute automatic time-out feature is set to prevent users from leaving terminals unattended and logged into the i-Series 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 Administrators maintain i-Series 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. Also, the i-Series 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 "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 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.

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 building security officer maintains a log 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 in February of each year and may be used on 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 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 System-i, Intel-based, and 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 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 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 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, on-staff security experts have crafted an aggressive security awareness campaign that includes comprehensive courses covering everything from security basics to advanced network defense principles and teaches these to both staff and clients alike. This campaign is an essential ingredient for creating and maintaining an attitude of "security is our way of doing business."

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

Complementary User Entity Controls

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

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 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.
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 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 CU*Answers is organized 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	Computer operators and network administrators do not perform programming functions.	Inspected the organization model and noted the degree to which operations, programming and network administrator functions are segregated.	No exceptions noted.
1.3	CU*BASE programming personnel do not perform network administration or operations duties.	Inspected the organization model and noted the degree to which operations, programming and network administrator functions are segregated.	No exceptions noted.
1.4	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.

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.	Reperformed the application of the control by selecting a sample of user organizations processed by CU*Answers and verified 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 CU*Answers and user functions are segregated.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
3.1	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.
3.2	Job descriptions have been prepared for personnel.	Inspected employee job descriptions and verified for completeness.	No exceptions noted.
3.3	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.
		Inspected Board Meeting minutes and verified that audit reports are presented to the Board for oversight.	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 Strategic 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.			
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	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.	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.

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: Application Development, Maintenance and Documentation

Control Objective 6: Controls provide reasonable assurance that all program change requests should require proper authorization, have adequate implementation procedures, and provide an audit trail to facilitate future program changes.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
6.1	User-initiated and internally generated requests for program changes are entered into a database.	Inspected program change control procedures with appropriate management and noted that detailed procedures for program implementation were in place.	No exceptions noted.
6.2	Programming change request are placed in the tracking database.	Reperformed the application of the control by selecting a sample of completed program change requests and verified that all applicable forms were present and completed on the database.	No exceptions noted.
6.3	Approved changes are assigned to a developer.	Reperformed the application of the control by selecting a sample of completed program change requests and verified that a programmer was assigned to the project.	No exceptions noted.
6.4	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.	Reperformed the application of the control by selecting a sample of completed program change requests and inspected project request forms and verified that each program change affected by the project request was tested by Quality Control. For custom requests, Crowe verified that an acceptance letter was received from the credit union.	No exceptions noted.
6.5	Programs in the release directories are supported by a Project Completion/ Modification Notice Form.	Inspected project request forms and verified that source modules, which were changed, were supported by a Project Completion/ Modification Notice form.	No exceptions noted.

Control Objective 6: Controls provide reasonable assurance that all program change requests should require proper authorization, have adequate implementation procedures, and provide an audit trail to facilitate future program changes.			
Control Activity	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
6.6	Changes to production programs are supported by a "Project Completion/ Modification Form".	Inspected source code review procedures and reviewed the CUBASEPTF libraries and haphazardly selected a sample of modified program during the period and verified that the project request forms were appropriately completed.	No exceptions noted.
6.7	Each major release is tested at several beta sites prior to full distribution to all users.	Inspected beta site procedures.	No exceptions noted.
6.8	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.	Inspected documented procedures and the checklist used regarding a change.	No exceptions noted.

Control Objective 7: On-Line Security

Control Objective 7: Controls provide reasonable assurance that on-line security measure 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**
7.1	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 about security concerning data communications.	No exceptions noted.
7.2	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 iSeries security reports and inquired with iSeries Administrator about the capabilities within the operating system software and verified terminal addresses for validity and that each terminal corresponds to the appropriate user.	No exceptions noted.
7.3	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.
7.4	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.
7.5	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.
7.6	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 documentation within software application to confirm that employees are restricted by menus available to them based on their requested access.	No exceptions noted.
7.7	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.

Control Objective 7: Controls provide reasonable assurance that on-line security measure 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**
7.8	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.
7.9	Program source code is not installed on the CU*BASE computer operation's production system.	Inspected iSeries library listing and noted that source programs not installed on production systems and discussed with management procedures that prohibit testing in production environment.	No exceptions noted.
7.10	Access to source code 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.
7.11	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 management monitors system activity.	No exceptions noted.

Control Objective 8: Physical Security

Control Objective 8: 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**
8.1	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.
8.2	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.
8.3	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.
8.4	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 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.
8.5	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 8: 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**
8.6	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.
8.7	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 and noted the presence of a natural gas generator and inquired with Internal Network Manager about the weekly testing of the generator.	No exceptions noted.
		Inspected the results of the last generator inspections for each facility and verified both generators are being maintained.	No exceptions noted.

Control Objective 9: e-Business Policies and Procedures

Control Objective 9: 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**
9.1	Policies and procedures for e-Business activities are documented, reviewed by management, and provided to CU*Answers staff.	Inspected the e-Business policy and inquired with Manager of Network Engineering and Implementation to verify procedures are documented.	No exceptions noted.
9.2	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.
9.3	The firewall is set up to log suspicious and unauthorized access attempts. Network Administrators review the firewall logs on a daily basis.	Reperformed the control by selecting a sample of days and verified review of firewall logs by appropriate company personnel.	No exceptions noted.
9.4	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 to confirm that the security devices have been configured to appropriately restrict access from the Internet, user institutions, and business partners.	No exceptions noted.
9.5	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.
9.6	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 9: 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**
9.7	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) 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. This Organizational Model 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. It represents a digital intelligence about how CU*Answers is organized and how its people are deployed. This is a succession planning resource.

Areas of our Organization

- Leadership
- General Administration
- Invention
- Production
- Capture Market Share
- Client Interaction and Support
- cuasterisk.com

Leadership

There are leaders throughout CU*Answers and at every level of the firm. But for the OM, we have organized the Leadership area around our senior leadership team, which we call the Executive Council. It's based on dividing the company into five basic quadrants that I believe every company needs to function well:

- Financial Leadership: The CFO and the teams he leads.
- Technical Leadership: The CIO and the teams she leads.
- Client Leadership: The EVP Client Interactions and the teams he leads.
- Market Leadership: The EVP Sales & Marketing and the teams he leads.
- Vision & Coordination: The CEO, who pulls everything together, and the teams he leads.

Bottom line...the individuals that make up these teams balance their activities between running a competent and efficient business and building the business for the future. Each team member must know when to prioritize their activities between "run" versus "build". We build tools to enhance our clients' abilities to run their day-to-day operations. We must be just as focused on our daily operations to be effective with our clients. At the same time, we must look forward, capitalizing on new opportunities and creating a future where daily work is actually required.

General Administration

These team configurations represent the day-to-day operations of our administrative teams. The big picture is spelled out in the Leadership area (under the Finance team). The day-to-day operations are broken down in each specific area below.

- Accounting Services Team
- Disaster Recovery/ Business Resumption Team
- Facilities Team
- General Administration Team
- Internal Audit Team
- Organizational Resource Development: Client Interaction Quality Assurance Team
- Organizational Resource Development: Employee Education Team
- Organizational Resource Development: Employee Resources Team

Invention

These team configurations represent the day-to-day operations of our technical teams. The big picture is spelled out in the Leadership area (under the Technical team). The day-to-day operations are broken down in each specific area below.

- CU*Answers Network Services: Advantage CIO Team
- CU*Answers Network Services: Engineering & Implementations Team
- CU*Answers Network Services: iSeries Administration Team
- CU*Answers Network Services: Network Solutions Team
- Design/ Development Coordination Team
- Quality Control Team
- Software Development: Analytics Team
- Software Development: Application Development Team
- Software Development: ASP Team
- Software Development: Conversions Team
- Software Development: EFT Team
- Software Development: GOLD Presentation Team
- Writing: Product Design Team

Production Area

From OL to ASP to SAAS, the technical marketplace loves its acronyms to explain how you sell operations to clients. The CU*Answers network is an online network. Our clients rely on the members of our Production Team to run the trains on time, push the right buttons, verify the work, and simply get things done behind the scenes.

The CU*Answers Production area is a combination of traditional teams that were once siloed in different areas. Today our Operations team needs to work closely with network system designers, a programming team focused on effective operations, and the growing integration of Item Processing based on Check 21 concepts. Our Production area is a company in itself.

Along with its importance as an executing team, it also hosts some of our most important infrastructure, so this team plays a critical role through its constant due diligence about our investments in data center capabilities.

- IP/FD - CU*Check21 Team
- Operations Team
- Software Development: Operations Development & Support Team

Capture Market Share Area Teams

These are the teams that design the strategies and tactics to carry our brand to the marketplace and sell our products to our current and potential customers.

- Core Processing Sales Team
- CU*Answers Equity Sales Team
- CU*Answers Network Services Sales Support Team
- cuasterisk.com Sales Team
- eDOC Partnered Sales Support Team
- IP/CU*Check21 Sales Team
- Marketplace Relations and General Marketing Team
- Xtend Sales Support Team

Client Interaction and Support

In the simplest configuration of OM, every single team is about supporting our clients. But this area represents the day-to-day execution teams responsible for responding to client inquiries, developing education tools, writing documentation, and monitoring the effective operations of all of the software applications provided in the CU*Answers suite.

These are the shared service teams that help credit unions build the expertise through working together to tackle the challenges of serving members, employees, and their partners.

- Client Services and Education Team
- Conversions Team
- CU*Answers Management Services: Audit Link Team
- CU*Answers Management Services: Electronic Document Strategies Team
- CU*Answers Management Services: Gividends Team
- CU*Answers Management Services: Lender*VP Collections Team
- CU*Answers Management Services: Lender*VP General Team
- CU*Answers Management Services: Lender*VP Mortgage Services Team
- CU*Answers Management Services: SettleMINT Team
- CU*Answers Management Services: Web Services Solutions Team
- CU*Answers Network Services: Client Support & Operations Team
- CU*Answers Network Services: Logistics Team
- Writing: Documentation Team

cuasterisk.com Area Teams

Every day, CU*Answers encourages credit unions to collaborate with their peers and create shared capabilities to enhance their own. cuasterisk.com is a working example of CU*Answers putting its money where its mouth is. It is a network of CUSOs and vendor businesses that collaborate to execute and build capabilities for our credit union owners and clients. There are two types of cuasterisk.com companies today:

- CU*BASE-centric wholesale companies that emulate CU*Answers as a core processing provider. These companies leverage everything CU*Answers, to sell and support clients with CU*BASE at the core. They may be involved in anything from sales to shared client support to the actual programming and development of CU*BASE software features. They maintain their own identities, their own Boards, and their own special marketplace differentials. They create the opportunity for CU*Answers team members to look at the marketplace from a different point of view.

- Organizations that add capabilities to the network. These firms fill in the gaps around CU*Answers' tool kits and services. In the case of Xtend, these teammates enhance our tools by picking them up and doing the work for the clients (shared personnel). In the case of eDOC Innovations, these teammates offer a compatible service that extends the value of CU*BASE with the power of electronic imaging strategies and tactics. cuasterisk.com is focused on getting the job done from start to finish, and any firm needed to enhance how we get the job done in our network is a candidate for this type of cuasterisk.com company.

In many cases, these teammates may be leased by CU*Answers to the partner organization, to maximize efficiencies related to employee resources, training, etc. In some cases, these employees are separate, and will be noted in this section more for what they bring to the team effort.

- CU*Answers Network Services Team
- CU*NorthWest Team
- CU*South Team

- eDOC Innovations Team
- Lender*VP Team
- Xtend: Member Reach Team
- Xtend: SRS Bookkeeping Team
- Xtension Call Center Team