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 Core Processing Application

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 October 1, 2016 to March 31, 2017

Table of Contents

© 2017 Crowe Horwath LLP

SECTION I: Independent Service Auditor’s Report

© 2017 Crowe Horwath LLP

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Site-Four, LLC
Yankton, South Dakota

Scope

We have examined Site-Four, LLC's (Site-Four) description of its CU*BASE Core Processing Application for processing user entities' transactions throughout the period October 1, 2016 to March 31, 2017, (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 Site-Four, LLC's 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.

Site-Four uses CU*Answers for the application development for the CU*BASE application. In Section V, the description includes only the controls and related control objectives of Site-Four and excludes the control objectives and related controls of CU*Answers. Our examination did not extend to controls related to application development.

Service Organization's Responsibilities

In Section II, Site-Four 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. Site-Four 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 October 1, 2016 to March 31, 2017.

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.

© 2017 Crowe Horwath LLP

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 of this report. 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 Site-Four's assertion in Section II of this report,

a) the description fairly presents the CU*BASE Core Processing Application that was designed and implemented throughout the period October 1, 2016 to March 31, 2017.
b) the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2016 to March 31, 2017, and user entities applied the complementary user entity controls contemplated in the design of Site-Four's controls throughout the period October 1, 2016 to March 31, 2017.
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 October 1, 2016 to March 31, 2017.

Description of Tests of Controls

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

Restricted Use

This report, including the description of tests of controls and results thereof in Section VI, is intended solely for the information and use of Site-Four, user entities of Site-Four's CU*BASE Core Processing Application during some or all of the period October 1, 2016 to March 31, 2017, 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
April 24, 2017

© 2017 Crowe Horwath LLP

SECTION II: Site-Four, LLC's Management Assertion

608 Goeden Dr, Yankton, SD 57078
P: 605.689.4309 F:605.665.8317

April 24, 2017

To the Users of the Site-Four, LLC's CU*BASE System:

We have prepared the description of Site-Four, LLC's (Site-Four) CU*BASE core processing application system (description) for user entities of the system during some or all of the period from October 1, 2016 to March 31, 2017, 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:

(1) The description fairly presents the CU*BASE core processing application system made available to user entities of the system during some or all of the period October 1, 2016 to March 31, 2017, for processing their transactions. Site-Four uses CU*Answers for software development of the CU*BASE application. The description of this report includes only the controls and related control objectives of Site-Four and excludes the control objectives and related controls of the CU*Answers. The criteria we used in making this assertion were that the description:

a) Presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including:

- the classes of transactions processed.
- 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 and other information prepared for user entities of the system.
- 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.
- how the system captures and addresses significant events and conditions, other than transactions.
- the process used to prepare reports or other information for user entities of the system.
- 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.
- 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.

b) Does not omit or distort information relevant to the scope of the CU*BASE system, while acknowledging that the description is presented 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,

© 2017 Crowe Horwath LLP

therefore, include every aspect of the CU*BASE system that each individual user entity of the system and its auditor may consider important in its own particular environment.

(2) 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.

(3) The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period October 1, 2016 to March 31, 2017, to achieve those control objectives and subservice organizations applied the controls contemplated in the design of Site-Four's controls. The criteria we used in making this assertion were that:

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

b) 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

c) the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Sincerely,

Alan Rogers
Chief Executive Officer
Site-Four, LLC

SECTION III: Description of Systems Provided by Site-Four, LLC

Overview of Operations

Governance

Site-Four, LLC, was founded on the principle that CUSOs and credit unions, working together, could offer back-end data processing at a cost much lower than the market rate while still offering the same level of quality and security. Site-Four has the following founding members that also comprise its board of directors:

- **Services Center Federal Credit Union**. A long-time client of CU*Answers and its flagship data processing software, CU*BASE. Services Center FCU is the formal owner of the building that houses Site-Four's operations.
- **CU*Answers**. A collaborative CUSO owned by over 120 credit unions, and developer of CU*BASE, a flagship product for credit union data processing.
- **CU*NorthWest**. A CUSO and reseller of CU*BASE, whose credit union clients are currently processed by Site Four.
- **CU*South.** Another CUSO and reseller of CU*BASE. Their credit union clients also use CU*BASE and processed by Site Four.

All of these organizations are material stakeholders in Site-Four and have significant interest in the success of Site-Four.

Building Safety and Security

Site-Four is housed in a secure facility located in Yankton, South Dakota. The facility has been built to withstand extreme weather, including F4 and F5 tornadoes. The computer operations center is heated and cooled using state of the art geothermal technology, with emergency air conditioning present. Room environmental conditions are monitored and logged. Site Four is also connected to on-site emergency generator power. UPS systems provide power to core systems. Fire suppression is through an FM200 system.

The building is secured 24/7, requiring key fob access in and out of the facility. The computer operations room itself is locked, with additional access required for the operations center and the data center rooms respectively. All building access is logged and equipment is configured to send alerts to Site Four personnel.

The building is continuously monitored by a CCTV DVR Surveillance System that comprises of 14 motion sensing cameras covering all areas of the facility and external entrances. All video surveillance is stored for a period of 2 months and access to the system is alerted and logged.

Network Operations and Redundancy

Site-Four has redundant fiber connections to and from the facility. The connections are such that if a credit union serviced by Site-Four would lose power, they could still run their operations on Site Four's backup channels. Firewalls and intrusion detection systems are also redundant. All connections are facilitated via VPNs terminated at the core, or third party devices as necessary to support other vendors.

© 2017 Crowe Horwath LLP

Backups and Disaster Recovery

Site-Four has high availability due to its co-location of systems at the CU*Answers Data Center located in Kentwood, MI. Site-Four can be positioned and/or transferred to serve customers from the High Availability location almost immediately, with CU*Answers personnel providing services until Site Four staff can arrive onsite.

In addition, Site-Four performs daily production, end of day, end of month, and end of year backups for the credit unions processed by its systems.

Operations and Data Processing

Site-Four utilizes run sheets to track and record operational processing tasks. The data center is staffed 24/7/365 via onsite or on-call personnel, and the team performs cross checking to ensure that millions of transactions are performed without error each day. The operators also ensure that the essential functions of the software run uninterrupted throughout the business day.

Local and Remote Systems

Anti-Virus and Anti-malware is installed and enabled on local systems. Firewall Content Filtering is also enabled and enforced. Workstation and laptop users do not have local administrative access. Guest accounts are disabled. VPN is configured using strong encryption for remote employees.

Control Objectives and Related Controls

The control objectives specified by Site-Four 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 Site-Four's 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 Site-Four 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.

© 2017 Crowe Horwath LLP

General Controls

General Controls are those policies, procedures, and safeguards that relate to all Information Systems (IS) activities. They include Organization and Administration, Backup and Recovery Planning, Computer Operations, On-Line Security, Physical Security, and e-Business Policies and Procedures.

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

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

Organization and Administration

Controls provide reasonable assurance that Site-Four policies and procedures are documented and functions and responsibilities are appropriately segregated between the company and user organizations.

Site-Four has an operational group that is responsible for daily processing and provides adequate segregation of duties. A senior operator oversees the group, and reports to the CEO.

The main function of the operations group is to monitor, post and process user organization transactions for the CU*BASE system. Operations personnel do not initiate or authorization transactions.

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 Site-Four hosted intranet. The handbook describes the company's policies for hiring, termination, salary administration, performance reviews, vacation, employee benefits, building and system security, and discrimination and harassment. 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.

Written job descriptions are maintained for operations personnel. Duties are defined to help provide appropriate segregation of duties and to maintain the accuracy of information processed.

The relationship between Site-Four and user organizations is contractual in nature. Each user organization signs a standard Site-Four agreement.

Planning activities are ongoing and reviewed as a standard part of management meetings. 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.

© 2017 Crowe Horwath LLP

Backup and Recovery Procedures

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

Site-Four has a Disaster Recovery and Contingency Plan. It explains the process of recovering from a disaster at the main location, as well as the protection of valuable credit union data. Further, the disaster recovery procedures are tested multiple times yearly.

Site-Four has a hot-site agreement to provide equipment and facility backup should the service organization site be destroyed or rendered inoperable. Various optional recovery and restoration tools are available to on-line and self-processing clients.

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. 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. All member data is encrypted when backup tapes are created. Complete policy and procedures for Production 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. Significant files and programs are replicated in real time using iTera disk to disk replication. The iSeries Administration Team completes the iTera HA Daily Tasks List to monitor replication status.

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

Site-Four maintains an insurance package that includes IS equipment, media, extra expense, general liability, building and contents casualty coverage, workmen’s compensation, umbrella liability coverage, employee dishonesty coverage, and errors and omissions coverage.

Computer Operations

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

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

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

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

Processing is performed for on-line clients. Reports and statements are available to clients online from a dedicated server.

© 2017 Crowe Horwath LLP

Standard Operating Procedures and Run Sheets

Standard operating procedures and run sheets have been created to conduct daily operation of both the CU*BASE system and all Intel-based servers, including managed hosting assets. The procedures describe the purpose, times, and reasoning for computer operator duties, while the run sheets contain all the tasks an operator would need for processing the daily work. Operators initial completed jobs on these run sheets and record the start and end time of processes as required.

Each shift also compiles an “End of Shift Report” that is sent to key personnel and all operators that documents all issues that occurred during the shift and any outstanding issues passed along to the next shift operators. “Run Sheet Change Requests” are documented directly on the RunSheets so that Operators can request run sheet modifications for changed or outdated information and communicate pertinent information to the management and programming teams. Run sheets are reviewed on a daily basis for completeness and accuracy, to follow up on any outstanding problems or incidents, and for any modifications in content. The run sheets are retained for a minimum of one year and are disposed of via a secure shredding facility.

Processing is controlled by job streams so that prior processing steps are completed before proceeding with the next processing step. For incoming ACH, totals from FEDLINE are compared to system totals prior to processing. A shift summary report is emailed by Site-Four operations staff at the end of each shift to note any exceptions or issues.

System restart / rerun procedures are in place and assist in the proper recovery of application processing should a program abnormally terminate. Control features within the operating system software note any hardware errors occurring during processing. Operations personnel perform preventive maintenance as needed.

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

Site-Four operates IBM Midrange systems at the main facility. Primary hardware consists of two IBM System-i servers: one in the Yankton data center (Production) and one in the Kentwood data center (High Availability). System-i operating systems are standard OS/400 Releases are upgraded as needed. Operating system revisions are normally accomplished during a period where minimal processing activity is expected. Site-Four utilizes third party security monitoring tools to complement their security program.

Site-Four employs a high availability infrastructure for its production System-i computer. Data is replicated in real-time from the Production system at the Yankton data center to an identical High Availability system at the Kentwood data center. Data replication is facilitated by iTera Echo2 software. Network Services provides managed high availability services for client System-i servers utilizing the same tool sets.

Hardware malfunctions are reported immediately to IBM using the ECS over a secure VPN. The CEO is informed of all severe hardware problems. Hardware issues are logged by operations personnel and reported to the appropriate vendor.

© 2017 Crowe Horwath LLP

Software Release, Installation and Documentation

Controls provide reasonable assurance that new releases, upgrades, and patches to vendor software are installed to ensure system integrity.

As enhancements to CU*BASE become available from CU*Answers, Site-Four will accommodate updates on the date as prescribed through the release procedures. The CU*Answers release team works directly with Site-Four Operations and performs the updates jointly following an installation procedure delivered to Site-Four by the CU*Answers Release Team. Currently, Site-Four is on the same release schedule as CU*Answers online Credit Unions. When a new release is announced, Group Providers are responsible for sending the user institutions an alert indicating when the release will be installed and the necessary documentation changes that will need to be made. These releases are loaded during a scheduled maintenance window when downtime will be minimized. A full system backup is conducted before the installation of the new release.

Special processing requests for the Site-Four CU*BASE report writer package are received by operations via fax or email. All requests are run as soon as possible by operations and the reports are delivered remotely to the requesting party generally on the same or next day.

User documentation in the CU*BASE application is maintained by the documentation department of CU*Answers. 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.

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 Site-Four system requires terminal access passwords to be changed every 60 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 via Site-to-Site AES256 encrypted VPNs. 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 Site-Four Security Administrators maintain i-Series terminal access security for both internal users and credit unions. An Account Maintenance Request Form is used to notify the Security Administrator of all internal additions, modifications, and deletions to security. Access for terminated Site-Four employees is removed from the system in a timely manner. Access to sensitive functions within operating system is restricted to authorized users. File transfers are further controlled by a separate third party Firewall and requests for access must be approved by the Credit Union Security Officer and submitted to Site-Four. A feature of CU*BASE allows credit unions to re-enable user profiles for their own employees that disable their profiles due to as few as three invalid sign-on attempts.

© 2017 Crowe Horwath LLP

Site-Four Security Administrators 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. User organizations have access to only the information for their institution and cannot access data of other institutions. 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.

Site-Four is located in a secure facility. 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 Site-Four 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. Each employee is issued their own code to deactivate the perimeter alarm system at the facility. Key employees are issued electronic building KeyFOBs 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 the computer rooms may be gained only by authorized employees using electronic building KeyFOBs on the computer room doors. Smoking, eating and drinking are prohibited anywhere in the Site-Four facility, including the computer room.

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 water 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. A written action plan relating to emergency situations is distributed to employees.

The buildings are also protected against fire by hand held extinguishers. These extinguishers are inspected 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 the facility. 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 a minimum of 30 minutes on battery only in the event of a power failure. Diesel powered electric generator is in place in Yankton to supply continuous power to all critical systems for an unlimited amount of time. These systems are tested weekly. There are specific test procedures for the UPS and generator systems that are detailed in the Disaster Recovery Manual.

© 2017 Crowe Horwath LLP

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 Site-Four. Because security is such a complex issue, no single solution or "silver bullet" can be expected to provide adequate protection. Policies and procedures for e-Business activities are documented, reviewed by management, and provided to Site-Four staff.

The 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. 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.

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 Site-Four 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.

© 2017 Crowe Horwath LLP

SECTION IV: Complementary User Entity Controls Provided by Site-Four, LLC

Complementary User Entity Controls

This section outlines specific complementary user entity controls, or issues each Site-Four, LLC (Site-Four) 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 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. Assign a Data Processing Coordinator to be responsible for coordinating, communicating, and monitoring any processing changes made by Site-Four 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.

© 2017 Crowe Horwath LLP

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 Site-Four 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 Site Four employees.

© 2017 Crowe Horwath LLP

SECTION V: Subservice Organization Utilized by Site-Four, LLC, Provided by Site-Four, LLC

Subservice Organization

The description of controls in this report includes only the policies, procedures, and control objectives at Site-Four, LLC, and does not include policies, procedures, and control objectives at the third party service provider described below. The examination by the Independent Service Auditors did not extend to policies and procedures at the third party organization. The primary, relevant third party service provider used by Site-Four is listed below:

Third Party Service Provider	Services Provided
CU*Answers	Application development for the CU*BASE system

As the subservice organization is used, control objectives and controls related to these activities are not discussed in this description and/or report. Management obtains and reviews the CU*Answers SOC reports to validate controls are designed and operating effectively.

© 2017 Crowe Horwath LLP

SECTION VI: 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 Site-Four policies and procedures are documented and functions and responsibilities are appropriately segregated between the company and user organizations.			
Control Number	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
1.1	Site-Four 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	The relationship between Site-Four and user organizations is contractual in nature.	Reperformed the application of the control by selecting a sample of user organizations processed by Site-Four and verifying that a current signed contract is maintained on file	No exceptions noted.
1.3	Operations personnel do not initiate or authorize transactions.	Inspected Site-Four policies and procedures of the service organization and made inquiries of management regarding standards for initiating or authorizing transactions.	No exceptions noted.
1.4	Site-Four 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.
1.5	Job descriptions have been prepared for all personnel.	Inspected sample of employee job descriptions and verified for completeness.	No exceptions noted.

© 2017 Crowe Horwath LLP

Control Objective 1: Controls provide reasonable assurance that Site-Four policies and procedures are documented and functions and responsibilities are appropriately segregated between the company and user organizations.			
Control Number	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
1.6	On an annual basis, management reviews and develops strategic plans for the upcoming year. In addition, prior year's major accomplishments are analyzed and compared to the strategic plan.	Inspected the Business Plan for the current year and verified completeness.	No exceptions noted.

© 2017 Crowe Horwath LLP

Control Objective 2: Backup and Recovery Procedures

Control Objective 2: Controls provide reasonable assurance that backup procedures and current off-site storage of important files exist.			
Control Number	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
2.1	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 Object Code • Operating System Code	No exceptions noted.
2.2	A formal written disaster plan has been prepared and testing has been performed.	Inspected the disaster recovery plan and verified completeness.	No exceptions noted.
		Inspected disaster recovery test results and verified that recovery procedures were adequately tested.	No exceptions noted.
2.3	Site-Four has a hot-site agreement to provide equipment and facility backup should the service organization site be destroyed or rendered inoperable.	Inspected the hot-site agreement and verified it is current and provides equipment and facilities if a disaster were to occur.	No exceptions noted.
2.4	Significant files and programs are replicated in real time using iTera disk to disk replication. iSeries Administration team completes the iTera HA Daily Tasks List to monitor replication status.	Reperformed the control by selecting a sample of days and verified that iTera Daily Tasks Lists were present, and completed.	No exceptions noted.

© 2017 Crowe Horwath LLP

Control Objective 3: Backup and Recovery Procedures

Control Objective 3: Controls provide reasonable assurance that insurance coverage exists relative to loss of equipment, records, and data processing capability.			
Control Number	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
3.1	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.	No exceptions noted.

© 2017 Crowe Horwath LLP

Control Objective 4: Computer Operations

Control Objective 4: Controls provide reasonable assurance that Computer operations and data control procedures are used to help ensure complete, authorized and accurate processing.			
Control Number	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
4.1	The operations department utilizes a daily checklist for processing. The checklist are reviewed by the operations manager for completeness.	Reperformed the application of the control by selecting a sample of days during the period and verified a daily processing checklist was present, complete, and reviewed.	No exceptions noted.
4.2	The daily checklist is used by operators to document that necessary files have been backed up.	Inspected a daily processing checklist and verified the operator must document the backup process.	No exceptions noted.
4.3	A shift summary report is emailed by Site-Four operations staff at the end of each shift to note any exceptions or issues.	Inspected a shift summary report and verified the operator documented any exceptions or issues noted during the shift.	No exceptions noted.
4.4	For incoming ACH, totals from FEDLINE are compared to system totals prior to processing.	Inspected the run sheets and inquired with Assistant Operations Manager and verified that the totals from FEDLINE are compared to system totals before processing begins.	No exceptions noted.
4.5	Operations personnel perform preventive maintenance as needed.	Inspected daily operations run sheets and inquired with Assistant Operations Manager and verified preventative maintenance is performed as needed.	No exceptions noted.
4.6	Processing is controlled by job streams so that prior processing steps are completed before proceeding with the next processing step.	Inspected the Operations Job processing procedures and inquired with management and verified prior processing steps must be completed before next steps can begin.	No exceptions noted.
4.7	System restart / rerun procedures are in place and assist in the proper recovery of application processing should a program abnormally terminate.	Inspected the Operations Job Processing procedures and inquired with management and verified that the system restart / rerun procedures are implemented when program abnormalities have occurred.	No exceptions noted.

© 2017 Crowe Horwath LLP

Control Objective 4: Controls provide reasonable assurance that Computer operations and data control procedures are used to help ensure complete, authorized and accurate processing.			
Control Number	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
4.8	Control features within the operating system software note any hardware errors occurring during processing.	Inspected an example of a robot message and inquired with Assistant Operations Manager and verified any hardware malfunctions that may occur are brought to management's attention.	No exceptions noted.

© 2017 Crowe Horwath LLP

Control Objective 5: Computer Operations

Control Objective 5: Controls provide reasonable assurance that changes to system software are authorized, tested, and reviewed, prior to implementation.			
Control Number	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
5.1	New versions of the operating system are implemented by the operations personnel and have the authorization of management prior to implementation.	Inspected the Operations Implementation and the Change Request policy and verified that procedures exist for system software implementation and that management authorization is required prior to implementation into the production environment.	No exceptions noted.
5.2	Operating system revisions are normally accomplished during a period where minimal processing activity is expected.	Inspected the Operations Implementation and the Change Request policy and verified operating systems revisions are installed during a period of minimal processing activity.	No exceptions noted.

© 2017 Crowe Horwath LLP

Control Objective 6: Software Release, Installation and Documentation

Control Objective 6: Controls provide reasonable assurance that new releases, upgrades, and patches to vendor software are installed to ensure system integrity.			
Control Number	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
6.1	Program releases are sent to Site-Four with detailed instructions for installation.	Inspected release documentation provided by the vendor and made inquiries with management regarding the adherence to release installation procedures.	No exceptions noted.
6.2	These releases are loaded during a scheduled maintenance window when downtime will be minimized. A full system backup is conducted before the installation of the new release.	Inspected release documentation for system backup procedures and made inquiries with management regarding release installation periods.	No exceptions noted.
6.3	Formal management approval is required prior to installation into production.	Obtained documentation from the most current system release and verified that release was approved by management prior to being installed.	No exceptions noted.

© 2017 Crowe Horwath LLP

Control Objective 7: On-Line Security

Control Objective 7: Controls provide reasonable assurance that on-line security measures should provide the ability to restrict users to the data files and menu functions to which they are authorized.			
Control Number	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
7.1	All customer data transmitted to and from our servers is protected via VPN encryption.	Inspected network documentation and inquired with management and verified security concerning data encryption.	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 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 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 Site-Four employees.	Inspected the User Profile Listing and verified that user identifications are restricted to only the required access.	No exceptions noted.
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.

© 2017 Crowe Horwath LLP

Control Objective 7: Controls provide reasonable assurance that on-line security measures should provide the ability to restrict users to the data files and menu functions to which they are authorized.			
Control Number	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
7.9	A third party audit tool is used to monitor sensitive system activity.	Inspected reports generated by the third party audit tool, Softlight, to confirm that a third party audit tool is used to monitor system activity.	No exceptions noted.
		Reperformed the application of the control by selecting a sample of days during the period and verified a daily processing checklist was present noting review of system messages.	No exceptions noted.

© 2017 Crowe Horwath LLP

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 Number	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
8.1	All doors to the service organizations main 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 facility.	Inspected the Physical Security Policy and inquired with Site-Four Operations Management and verified only authorized personnel are allowed access to the buildings.	No exceptions noted.
8.3	The computer room is 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 facility. Further, hand held fire extinguishers are located throughout the facility.	Toured the entire Site-Four facility and computer room 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.

© 2017 Crowe Horwath LLP

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 Number	**Description of Controls**	**Tests of Operating Effectiveness**	**Results**
8.6	An Uninterruptible Power Supply (UPS) system with power conditioners is installed to protect the computer room facility from short or long-term power failures.	Toured Site-Four computer room and noted the presence and location of an UPS system.	No exceptions noted.
		Inspected the results of the last UPS inspection for the facility and verified the UPS system is being maintained.	No exceptions noted.
8.7	A diesel generator is installed at the facility to protect the building from power failures.	Toured the Site-Four facility and noted the presence of a diesel generator and inquired with Operations Manager about the weekly testing of the generator.	No exceptions noted.
		Inspected the results of the last generator test for the facility and verified the generator is being maintained.	No exceptions noted.

© 2017 Crowe Horwath LLP

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 Number	**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 Site-Four staff.	Inspected the e-Business policy documents and inquired with Manager of Network Engineering and Implementations to verify procedures are documented.	No exceptions noted.
9.2	Site-Four 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 management 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. Management reviews the firewall logs on a periodic basis.	Inspected configuration of the firewall logs with management and verified that specified system events are recorded and are retained.	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 management and confirm that the security devices have been configured to appropriately restrict access from the Internet, user institutions, and business partners.	No exceptions noted.

© 2017 Crowe Horwath LLP