Crowe

Smart decisions. Lasting value.™

System and Organization Controls Report SOC 1® Type 2

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

Related to the CU*BASE Host Processing Services

Under the AICPA, Statement on Standards for Attestation Engagements No. 18 (SSAE No. 18), Section AT-C 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*

For the Period October 1, 2022 to March 31, 2023

site-four

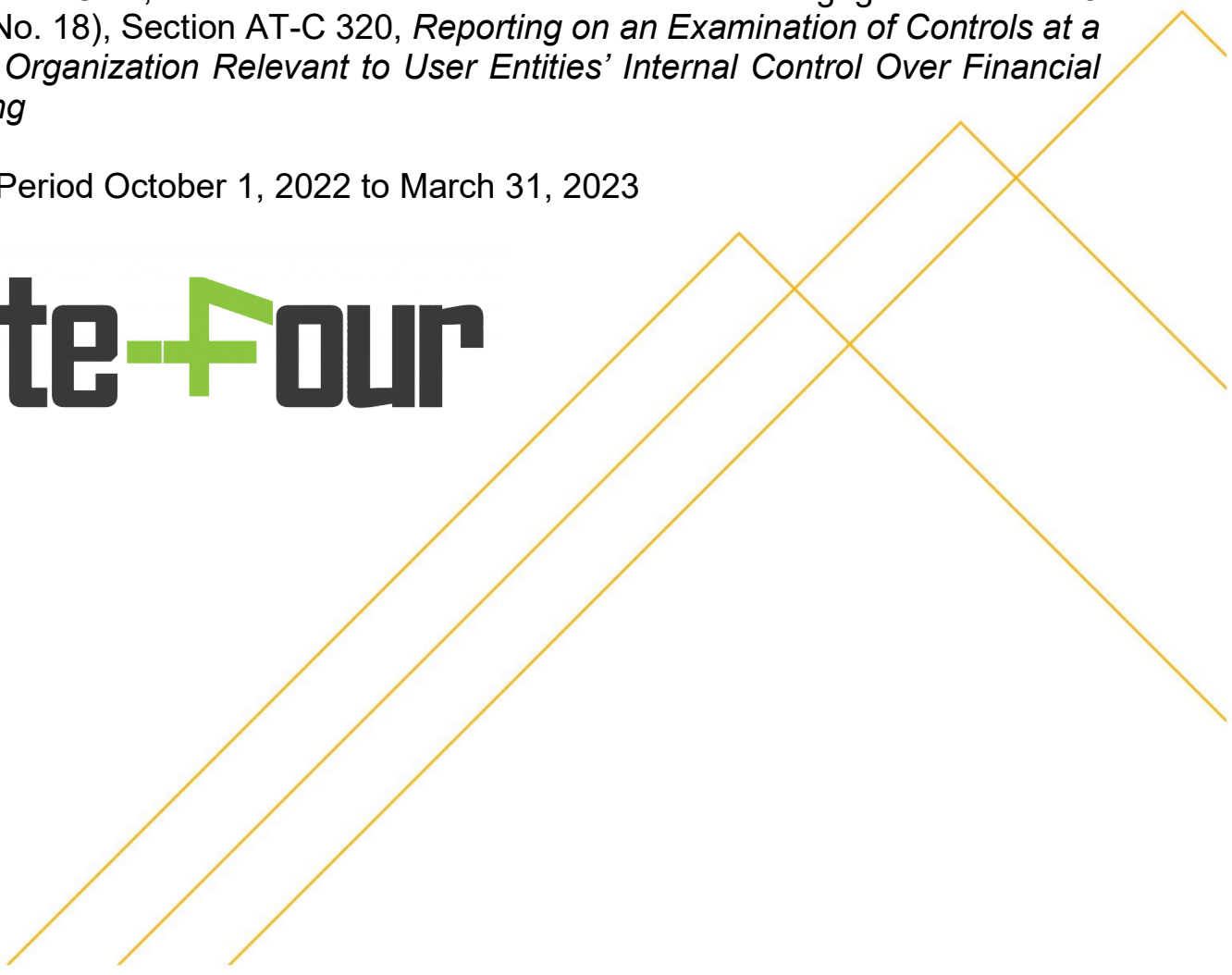

Table of Contents

SECTION I: Independent Service Auditor's Report

INDEPENDENT SERVICE AUDITOR'S REPORT

To Site-Four, LLC

Scope

We have examined Site-Four, LLC's (Site-Four or service organization) description of its CU*BASE Host Processing Services entitled "System Description Provided by Site-Four, LLC" for processing user entities' transactions throughout the period October 1, 2022 to March 31, 2023, (description) and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Assertion of Site-Four, LLC's Management" (assertion). The controls and control objectives included in the description are those that management of Site-Four believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the CU*BASE Host Processing Services that are not likely to be relevant to user entities' internal control over financial reporting.

Site-Four uses CU*Answers, a subservice organization, to provide software development and deployment and colocation services. The description includes only the control objectives and related controls of Site-Four and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by Site-Four can be achieved only if complementary subservice organization controls assumed in the design of Site-Four's controls are suitably designed and operating effectively, along with the related controls at Site-Four. Our examination did not extend to controls of the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

The information included in Section V, "Other Information Provided by Site-Four, LLC (Unaudited)" is presented by management of Site-Four to provide additional information and is not a part of Site-Four's description of its CU*BASE Host Processing Services made available to user entities during the period October 1, 2022 to March 31, 2023. Information about Site-Four's management's responses to identified exceptions has not been subjected to the procedures applied in the examination of the description of the CU*BASE Host Processing Services and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the CU*BASE Host Processing Services, and accordingly, we express no opinion on it.

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

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period October 1, 2022 to March 31, 2023. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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

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

Inherent Limitations

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

Description of Tests of Controls

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

Opinion

In our opinion, in all material respects, based on the criteria described in Site-Four's assertion:

a. the description fairly presents Site-Four's CU*BASE Host Processing Services that was designed and implemented throughout the period October 1, 2022 to March 31, 2023.

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, 2022 to March 31, 2023, and the subservice organization and user entities applied the complementary controls assumed in the design of Site-Four's controls throughout the period October 1, 2022 to March 31, 2023.

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2022 to March 31, 2023, if complementary subservice organization and user entity controls assumed in the design of Site-Four's controls operated effectively throughout the period October 1, 2022 to March 31, 2023.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Site-Four, user entities of Site-Four's CU*BASE Host Processing Services during some or all of the period October 1, 2022 to March 31, 2023, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than the specified parties.

Crowe LLP

Crowe LLP

South Bend, Indiana
June 7, 2023

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

June 7, 2023

Assertion of Site-Four, LLC's Management

We have prepared the description of Site-Four, LLC's (Site-Four or service organization) CU*BASE Host Processing Services entitled, "System Description Provided by Site-Four, LLC" for processing user entities' transactions throughout the period October 1, 2022 to March 31, 2023 (description), for user entities of the system during some or all of the period October 1, 2022 to March 31, 2023, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by the subservice organization and user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

Site-Four uses CU*Answers, a subservice organization, to provide software development and deployment and colocation services. The description includes only the control objectives and related controls of Site-Four and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by Site-Four can be achieved only if complementary subservice organization controls assumed in the design of Site-Four's controls are suitably designed and operating effectively, along with the related controls at Site-Four. The description does not extend to controls of the subservice organization.

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

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

a. the description fairly presents the CU*BASE Host Processing Services made available to user entities of the system during some or all of the period October 1, 2022 to March 31, 2023 for processing user entities' transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description

   i. presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable,
      (1) the types of services provided, including, as appropriate, the classes of transactions processed.
      (2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.
      (3) the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
      (4) how the system captures and addresses significant events and conditions other than transactions.

(5) the process used to prepare reports and other information for user entities.
(6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
(7) the specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls.
(8) other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

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

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

b. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period October 1, 2022 to March 31, 2023 to achieve those control objectives if the subservice organization and user entities applied the complementary controls assumed in the design of Site-Four's controls throughout the period October 1, 2022 to March 31, 2023. The criteria we used in making this assertion were that:

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

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

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

Site-Four, LLC

SECTION III: System Description Provided by Site-Four, LLC

Scope of Report

The scope of this report covers Site-Four's CU*BASE Host Processing Services for those credit unions for which Site-Four, LLC hosted CU*BASE and performed processing of user entities transactions for the period of October 1, 2022 through March 31, 2023.

Site-Four uses CU*Answers, a subservice organization, to provide software development and deployment and colocation services for the CU*BASE Core Processing Application, which is not included in the scope of this report. Refer to the 'Subservice Organization' section for further information regarding CU*Answers.

Company Overview

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:

- **Explorers Credit Union**. A long-time client of CU*Answers and its data processing software, CU*BASE. Explorers CU 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 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.
- **Vermillion Federal Credit Union.** Another credit union located in Vermillion, South Dakota

All of these organizations are stakeholders in Site-Four.

Relevant Aspects of the Control Environment, Risk Assessment, Information and Communication, and Monitoring

Control Environment

Site-Four is overseen by its Board of Directors, which meets monthly and receives reports from the CEO. Site-Four has created an Organizational Chart to clearly establish reporting lines and authority, which is approved annually. Site-Four has an operational group that is responsible for daily processing and provides adequate segregation of duties. An Operations Supervisor oversees the operational team, and reports to the CEO.

Risk Assessment

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 and presents to the Board of Directors. As part of planning activities, key risks are identified and addressed as needed to support management in achieving Site-Four's strategic objectives.

Additionally, Management has a Vendor Management Program in place to ensure appropriate oversight is performed over third-party vendors. The Vendor Management Program provides procedures for determining the criticality of specific relationships or vendors and evaluates reputation risk, financial risk, and compliance risk for the organization.

Information and Communication

Through Site-Four's organizational chart, lines of authority and communication are defined. Written job descriptions are maintained, which define the skills and responsibilities of each role within the organization. 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. 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.

As part of their effort to maintain open and effective lines of communication with their partners, Site-Four has established two groups that meet to discuss any concerns and facilitate progress. The Operations Development Team (ODT) meets at least monthly to discuss topics that revolve around programming changes, automation and enhancements to augment the current processes. The Operations Team meets bi-weekly to discuss the current state of Site-Four Operations, highlights upcoming changes including credit union conversions and deconversions, and keeps the CUSO teams appraised of any ongoing projects being implemented. These teams play a critical role in keeping Site-Four and their partners on the same page.

Monitoring

Monitoring of Site-Four's operations is performed by management to ensure that hosting and processing of client transactions is secure and uninterrupted. The Board of Directors also provides oversight through its monthly meetings.

Building Safety and Security

Site-Four is housed in a secure facility located in Yankton, South Dakota. The building is secured 24/7, requiring electronic badge 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 16 high definition motion sensing cameras covering all areas of the facility and external entrances. All video surveillance is stored for a period of 2 months.

Backups and Disaster Recovery

Site-Four utilizes the CU*Answers Data Center located in Kentwood, MI for colocation services (i.e. High Availability location). 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 transactions are performed without error each day. The operators also ensure that the essential functions of the software run uninterrupted throughout the business day.

Description of Controls

Organization and Administration

Control Objective 1: Controls provide reasonable assurance that Site-Four policies and procedures are documented, and functions and responsibilities are defined between the company and user organizations.

Site-Four has created an Organizational Chart to clearly establish reporting lines and authority, which is approved at least annually (typically in August annually) (1.1). Site-Four has an operational group that is responsible for daily processing and provides adequate segregation of duties. An Operations Supervisor oversees the operational team, and reports to the CEO. The CEO reports to the Site-Four Board of Directors (BoD) on a monthly basis (1.3).

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 (1.4). 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 (1.5). Duties are defined to help provide appropriate segregation of duties and to maintain the accuracy of information processed. The main function of the operations group is to monitor, post and process user organization transactions for the CU*BASE system.

The relationship between Site-Four and Group Providers is contractual in nature. A Group Provider is a CUSO that contracts directly with Credit Unions to provide services, support and processing on a single core system. These Group Providers contract with Site-Four to provide hosting and processing services. Each Group Provider signs a standard Site-Four Master Services Agreement detailing the nature of the relationship which is documented, signed and retained (1.2).

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 and presents to the Board of Directors, typically in July or August annually. In addition, prior year's major accomplishments are analyzed and compared to the strategic plan (1.6).

Management has a Vendor Management Program in place to ensure appropriate oversight is performed over third party vendors (1.7). The Vendor Management Program provides procedures for determining the criticality of specific relationships or vendors. Vendor Management evaluates control of reputation risk, financial risk, and compliance risk for the organization. When assessing the risk of each vendor, Site-Four reviews key risk information:

- Extent to which the vendor has access to non-public member information and/or stores non-public member information;
- Extent to which the vendor has access to the organization's physical location;
- Extent to which the vendor has access to the organization's IT infrastructure;
- The service provided by the vendor is intolerant (disaster recovery/business resumption) to the disruption of member services; and
- Extent to which the service provided is vital to the organization and financially woven into the strategies of the organization.

Each vendor reviewed is evaluated in accordance with the above variables and based upon this evaluation was assigned a tier level appropriate for the ongoing monitoring and continued due diligence of the vendor. The subservice organization is subject to at least annual evaluation in accordance with the vendor risk assessment process (1.8).

Backup and Recovery Procedures

Control Objective 2: Controls provide reasonable assurance that backup and recovery procedures and current off-site storage of client files and programs is in place.

Site-Four has a Business Continuity 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 on at least an annual basis (2.2).

Site-Four has a colocation agreement to provide a hot-site with equipment and facility backup should the service organization site be destroyed or rendered inoperable (2.3). Various optional recovery and restoration tools are available to on-line and self-processing clients.

Site-Four has established a backup and retention policy, which details the operational teams' responsibilities for backups completed on the host. Client files and programs are backed up daily, within the production environment. A file retention schedule and a schedule for off premise rotation of master files and programs have been established (2.1). Numerous backup tapes are created for the purposes of restoration of data for testing and research, for application backups, and for disaster recovery. In addition to the physical backups, Site-Four utilizes a third-party tool, iTera, to perform real-time replication of client files and program data to the colocation (located within the CU*Answers Data Center). The Site-Four administration team completes the iTera HA Daily Tasks List to monitor replication status (2.4).

Computer Operations

Control Objective 3: 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, including but not limited to:

- 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.

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, including managed hosting assets. Processing is controlled by job streams so that prior processing steps are completed before proceeding with the next processing step (3.5). 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. The operations department utilizes the run sheet, described above, for processing and backup of the system on a daily basis (3.2). For incoming ACH, totals from FEDLINE are compared to system totals prior to processing (3.4). The operators initial completed jobs on these run sheets and record the start and end time of processes as required. The run sheets are reviewed by the senior operator, at end of day (3.1).

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 (3.3). “Run Sheet Change Requests” are documented directly on the Run Sheets 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.

System restart / rerun procedures are in place and assist in the proper recovery of application processing should a program abnormally terminate (3.6). Control features within the operating system software note any hardware errors occurring during processing. Operations personnel perform preventive maintenance as needed.

Change Management

Control Objective 4: Controls provide reasonable assurance that system changes are evaluated prior to deployment in the production environment.

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. New versions of the operating system are implemented by CU*Answers. CU*Answers provides notice to Site-Four of upcoming operating system upgrades which are authorized and approved prior to being implemented into the production environment (4.1). Operating system version updates are normally accomplished during a period where minimal processing activity is expected.

As enhancements to CU*BASE become available from CU*Answers (refer to Subservice Organization), Site-Four will accommodate updates on the date prescribed through the release procedures. The CU*Answers release team controls of the system development life cycle process, including the deployment phase and providing release information to users. CU*Answers programmers conduct weekly meetings to discuss upcoming releases within the production environment. Site-Four management obtains minutes from these meetings each week to monitor matters that may impact their hosting and processing services (4.2).

Logical Security

Control Objective 5: Controls provide reasonable assurance that logical access to applications and system data is restricted to authorized individuals.

There are two levels of security used by user credit unions: i-Series terminal access security and CU*BASE application security.

The i-Series terminal access is restricted via site-to-site AES256 encrypted VPNs (5.1). A user is required to enter a unique identification name (username) and password to login to the i-Series host. The password parameters on the i-Series network is configured by the Site-Four operational team and is configured to require a minimum length of 8 characters, a mix of alphanumeric and special characters, and an expiration after 30 days (5.2). The password parameters are reviewed and updated as necessary in relation with common IT security frameworks when permitted.

Site-Four assists in the creation of new credit unions being onboarded to the host environment. The Site-Four operational team will create a user profile and libraries related to the new credit union. These separate libraries and user profiles logically restrict the user’s from accessing data within other user institutions on the system (5.4). The credit unions are then responsible for maintaining their users’ access after onboarding. Procedures necessary for the appropriate onboarding of a user organization, are completed by the ‘Group Providers Conversion’ team. Additionally, the system is configured to send activity reports to each user credit union on a daily basis (5.5). This allows for the user organizations to properly monitor the activity occurring within their ‘environment’.

For all new Site-Four employee access requests, an iSeries User Profile Change Request, will be used to document the access requested and the roles and responsibilities of that user (5.6). Likewise, for an internal employee leaving the company, their access within the system will be removed in a timely manner and documented using the same form (5.7). However, as there were no terminated employees during the period control 5.7 was not invoked during the period. The system is also configured to run an automated termination, or system purge, on a weekly basis. The automated job removes all accounts that have not been accessed in over 92 days, both internal and external users (5.8).

Additionally, access to sensitive functions within operating system is restricted to authorized users (5.3). Due to the sensitive nature of the access granted to the operational team, the system is configured to log the sensitive system activity, including but not limited to system setting changes, logging, and object modifications using a third party tool, SoftLight Auditor (5.9).

Physical Security

Control Objective 6: 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 which requires a key fob to access (6.1). 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 upon arrival and must be escorted by an employee 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 in order to enter or exit the facility. Key employees are issued electronic building badges that allow access to the building on a five or seven-day system (6.2).

Access to the server room may be gained only by authorized employees using electronic building badges on the computer room doors (6.3). Visitors must be admitted to the area by operations personnel.

The server room is 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 (6.4). 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 handheld extinguishers. These extinguishers are inspected each year and may be used on electrical devices, liquids, and other combustible materials. Sensors are installed in the server room 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 60 minutes on battery only in the event of a power failure (6.5). Diesel powered electric generator is in place in Yankton to supply continuous power to all critical systems for an unlimited amount of time (6.6). There are specific test procedures for the UPS and generator systems that are detailed in the Disaster Recovery Manual.

Complementary User Entity Controls

The Site-Four, LLC (Site-Four or service organization or organization or Company) CU*BASE Host Processing Services control structure is designed with the assumption that certain controls would be implemented by user entities. This section describes user entity controls identified by Site-Four as necessary to achieve the specified control objectives.

The user entity controls described below should not be regarded as a comprehensive list of all controls which should be employed by user entities. Each user entity's internal control over financial reporting should be evaluated in conjunction with Site-Four's controls and the complementary user entity controls identified below.

User entities are responsible for the following:

Input Controls

1. Verify and balance all incoming third party files, such as ATM, ACH, and share drafts. (Control Objective 3)

2. Balance system generated general ledger entries to reconcile the G/L interface against the member trial balance. (Control Objective 3)

3. Monitor daily exception reports, application suspense accounts and application activity reports. (Control Objective 3)

4. Develop internal data security and employee access to system features, as well as all key parameter configurations. (Control Objective 5)

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. (Control Objective 4)

2. Test program changes after general release to verify that results are as published. (Control Objective 4)

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. (Control Objective 3)

4. Review operations logs on a daily basis. (Control Objective 3)

5. Review standard forms generated by the system for regulatory compliance. (Control Objective 3)

Output Controls

1. Review and document the reports generated by the system each day to determine that all reports have been received. (Control Objective 3)

2. Control the distribution of reports to user personnel to ensure that reports are distributed to only authorized personnel. (Control Objective 5)

3. Balance application totals to the independently posted general ledger to verify the overall accuracy of the daily processing results. (Control Objective 3)

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. (Control Objective 3)

5. Review unposted transaction to establish control for research, correction, and re-entry. (Control Objective 3)

6. Independently verify master file change listing to help ensure the accuracy and propriety of file maintenance posting. (Control Objective 3)

7. Review each application's exception report to help identify any unusual application activity. (Control Objective 3)

8. Independently monitor usage of interest and accounts payable checks printed by the data processing department to safeguard and maintain accountability for such items. (Control Objective 5)

9. 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. (Control Objective 3)

Logical Access Security Controls

1. Assign a Logical Security Coordinator who is responsible for defining and monitoring the users' security assignments. (Control Objective 5)

2. Assign each user with a unique username and password to provide accountability for system activity. (Control Objective 5)

3. Periodically change passwords to maintain the confidentiality of each user's sign-on. (Control Objective 5)

4. 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. (Control Objective 5)

5. Review on a periodic basis the Member File Maintenance, General Transaction Register, General Journal Report and the Employee Activity Audit for changes made by Site-Four employees. (Control Objective 5)

Subservice Organization

Site-Four has determined that certain control objectives specified by Site-Four can be achieved only if complementary subservice organization controls assumed in the design of Site-Four's controls are suitably designed and operating effectively, along with the related controls at Site-Four. The description of controls in this report includes only the policies, procedures, and controls at Site-Four and does not include policies, procedures, and controls 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:

Subservice Organization & Services Provided	Related Control Objectives	Complementary Subservice Organization Controls
CU*Answers *Providing application development and deployment for the CU*BASE Core Application and colocation services.*	Control Objectives 2, 4, 5, and 6	• Environmental and physical security access controls and safeguards including back-up power generation have been implemented. • Access to application source code is restricted. • Software development procedures have been implemented. • Program changes are properly authorized and approved before being placed into production. • User Access Requests (Additions, Modifications, Removals) are documented and executed appropriately. • Access to sensitive functions on the system and application are restricted. • Physical security controls over equipment and servers, located within CU*Answers datacenter are in place.

Subservice Organization Monitoring Controls

Management meets with the subservice organization on a weekly basis and obtains and reviews vendor due diligence documentation in accordance with the vendor review program at least annually. Further, Site-Four, LLC has a vendor management program that details procedures for evaluating and reviewing subservice providers.

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

Overview of Crowe LLP's Test Procedures

Our examination was restricted to the control activities specified by Site-Four's management in Sections III and IV of this report to address the control objectives that were stated in the description. Our examination did not extend to any other control procedures, including those that may be described in Section III but not listed in Section IV.

The following table clarifies certain terms that may be used within this section to describe the nature of the tests of controls performed:

Type of Testing	Description
Observation	Observed the application, performance or existence of the specified controls as described.
Inspection	Inspected manually or systematically maintained documentation to evidence performance of the specified controls.
Reperformance	Reperformed the specified controls as performed by management to compare our independent results to those of management.

As Crowe conducted inquiry with appropriate Site-Four personnel for all controls, inquiry was not listed specifically by each control within Section IV.

In addition, when using information produced by Site-Four, we performed procedures as required by AT-C Section 320 to validate whether the information was sufficiently reliable for our purposes by obtaining evidence about the completeness and accuracy of such information, as well as evaluating whether the information produced was sufficiently precise and detailed for our purposes.

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 defined between the company and user organizations.			
Control Number	**Description of Controls**	**Tests of Controls**	**Results**
1.1	Site-Four maintains an Organizational Chart to clearly establish reporting lines and authority which is approved annually.	Inspected Site-Four's organizational chart to determine that reporting lines and authority are documented, however the scheduled timing for the annual review of the Organizational Chart was timed to occur outside the examination period.	The operation of this annual control is timed outside the examination period and, therefore, operating effectiveness testing was not performed.
1.2	For all group providers that Site-Four provides services to, a contract detailing their relationship is documented, signed and retained.	Inspected the contracts for a sample of group providers to determine their relationship is documented in a contract, which is signed and retained.	No exceptions noted.
1.3	The Site-Four CEO reports to the Board of Directors on a monthly basis.	Inspected the Board of Director (BoD) minutes for a sample of months to determine that the CEO reported to the BoD and those meetings were conducted and documented.	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 to determine the company's policies for hiring, termination, salary administration, performance reviews, vacation, employee benefits, building and system security, and discrimination and harassment are documented.	No exceptions noted.
1.5	Roles and responsibilities for operations personnel are defined in documented job descriptions to support Site-Four.	Inspected a sample of job descriptions for operations personnel per the organization chart to determine management has documented roles and responsibilities which are available to employees.	No exceptions noted.

Control Objective 1: Controls provide reasonable assurance that Site-Four policies and procedures are documented, and functions and responsibilities are defined between the company and user organizations.			
Control Number	**Description of Controls**	**Tests of Controls**	**Results**
1.6	On an annual basis, management reviews and develops strategic plans for the upcoming year and presents these to the Board of Directors. In addition, the major accomplishments of the prior year are analyzed and discussed within the plan.	The scheduled timing for the annual preparation and review of the strategic plan was timed to occur outside the examination period.	The operation of this annual control is timed outside the examination period and, therefore, operating effectiveness testing was not performed.
1.7	Management has vendor management policies and procedures in place to ensure oversight is performed over third-party vendors.	Inspected evidence of management's documented policies and procedures pertaining to vendor management and vendor oversight standards.	No exceptions noted.
1.8	The subservice organization is subject to annual evaluation in accordance with the vendor risk assessment process.	Inspected vendor risk assessment documentation completed by management to determine that the annual review occurred during the period.	***Exception Noted:*** The annual review of the subservice organization was timed to occur October 2022. Management subsequently completed the review April 2023.

Control Objective 2: Backup and Recovery Procedures

Control Objective 2: Controls provide reasonable assurance that backup and recovery procedures and current off-site storage of client files and programs is in place.			
Control Number	**Description of Controls**	**Tests of Controls**	**Results**
2.1	Client 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.	Inspected the backup policy and procedures to determine that management has a file retention schedule in place for off premise file rotations. Inspected run sheets for a sample of days to determine if the operator documented that backups were completed.	No exceptions noted.
2.2	A business continuity plan exists, and testing is performed at least annually.	Inspected the business continuity plan and high availability program report to determine that the plan exists, and testing was performed during the audit period.	No exceptions noted.
2.3	Site-Four has a colocation agreement with a third party to utilize equipment, infrastructure, and a backup facility for disaster recovery and business continuity support.	Inspected the colocation agreement to determine if a third party is responsible for providing equipment, infrastructure, and a backup facility for disaster recovery and business resumption support.	No exceptions noted.
2.4	Client files and programs are replicated real-time to Site-Four's colocation using disk to disk replication, and the operational team monitors the replication process which is documented on the High Availability checklists.	Inspected system configurations to determine that client files and programs are configured for real-time replication to the Site-Four colocation. Inspected High Availability checklists for a sample of days to determine that monitoring of the replication process was completed.	No exceptions noted.

Control Objective 3: Computer Operations

Control Objective 3: 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 Controls**	**Results**
3.1	The operations department utilizes a daily run sheet for processing. The run sheet is reviewed by the senior operator.	Inspected a sample of daily run sheets to determine if the completed daily processing run sheets were reviewed by a senior operator.	No exceptions noted.
3.2	The daily run sheet is used by operators to document that necessary files have been backed up.	Inspected a sample of daily run sheets to determine if the operator documented that backups were completed.	No exceptions noted.
3.3	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 sample of daily shift summary reports and verified the operator documented any exceptions or issues noted during the shift.	No exceptions noted.
3.4	For incoming ACH, totals from FEDLINE are compared to system totals prior to processing.	Inspected a sample of daily run sheets to determine if incoming ACH totals are compared to system totals prior to processing.	No exceptions noted.
3.5	Processing is controlled by daily run sheets so that prior processing steps are completed before proceeding with the next processing step.	Inspected a sample of daily run sheets to determine if processing steps must be completed before proceeding with the next processing step and that each step is documented.	No exceptions noted.
3.6	System restart / rerun procedures are in place and assist in the proper recovery of application processing should a program abnormally terminate.	Inspected a sample of daily run sheets to determine if operators check for terminated programs and perform restart / rerun procedures should a program abnormally terminate.	No exceptions noted.

Control Objective 4: Change Management

Control Objective 4: Controls provide reasonable assurance that system changes are evaluated prior to deployment in the production environment.			
Control Number	**Description of Controls**	**Tests of Controls**	**Results**
4.1	Site-Four is notified of new versions of the operating system which are authorized and approved prior to being implemented within the production environment.	Inspected documentation supporting that notification of an operating system version update was provided to Site-Four and authorized during the period prior to implementation.	No exceptions noted.
4.2	Site-Four obtains minutes of weekly CU*Answers programmer meetings to monitor matters that may impact the Site-Four environment.	Inspected documentation to determine that Site-Four management was configured to receive weekly minutes of CU*Answers programming meetings and that such minutes were obtained for a sample of weeks.	No exceptions noted.

Control Objective 5: Logical Security

Control Objective 5: Controls provide reasonable assurance that logical access to applications and system data is restricted to authorized individuals.			
Control Number	**Description of Controls**	**Tests of Controls**	**Results**
5.1	Access to the iSeries Host is restricted using VPN encryption.	Inspected SonicWall firewall settings to determine that the tool is configured to require each user credit union to connect to the Site-Four environment through an encrypted VPN.	No exceptions noted.
5.2	Local and remote users are subject to password requirements set by system policies when authenticating to the mainframe.	Inspected system settings to determine that password parameters are defined for user authentication to the mainframe.	No exceptions noted.
5.3	Access to sensitive functions within the operating system is restricted to authorized users.	Inspected a listing of users with access to sensitive functions and determined access was restricted based on job responsibilities.	No exceptions noted.
5.4	User organizations have access to only the information for their institution and cannot access data of other institutions.	Inspected iSeries settings to determine that user organizations are only able to access their institution data. Inspected mainframe library reports for a sample of user credit unions to determine that user profiles have been established to logically restrict users from accessing other user organization data.	No exceptions noted.
5.5	The system is configured to send activity reports to each user credit union on a daily basis.	Inspected settings for the mainframe to determine that the system is configured to automatically send activity reports to each user credit union.	No exceptions noted.
5.6	Requests for Site-Four employee system access will be documented in an i-Series User Profile Change Request form and granted based on the documented roles and responsibilities the employee will be performing.	Inspected User Profile Change Request form for a sample of new hires to determine that access requested and the roles/responsibilities of the new hire are documented.	No exceptions noted.

Control Objective 5: Controls provide reasonable assurance that logical access to applications and system data is restricted to authorized individuals.			
Control Number	**Description of Controls**	**Tests of Controls**	**Results**
5.7	Access for terminated employees is documented in an i-Series User Profile Change Request form and removed from the system in a timely manner.	Inspected system-generated termination report and determined that no users were removed from the system during the examination period.	***Control Not Invoked:*** The circumstances that warranted operation of this control did not occur as there were no terminated Site-Four employees during the period. Accordingly, testing of operating effectiveness was not performed.
5.8	The system is configured to purge all inactive accounts (accounts not used in >92 days) on a weekly basis.	Inspected the iSeries configurations to determine the system is setup to remove all inactive accounts on a weekly basis.	No exceptions noted.
5.9	A third-party audit tool is configured in the environment to log sensitive system activity.	Inspected the SoftLight program configurations to determine the third-party tool is configured to report sensitive system activity on a daily basis.	No exceptions noted.

Control Objective 6: Physical Security

Control Objective 6: 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 Controls**	**Results**
6.1	A security (badge) system restricts access to the main facility.	Observed the main facility to determine the doors were locked and access is controlled via a security (badge) system.	No exceptions noted.
6.2	Authorized personnel have been issued electronic building badges.	Inspected documentation showing all issued electronic building badges to determine that building was restricted to authorized personnel.	No exceptions noted.
6.3	Access to the server room is restricted via the security (badge) system and is limited to personnel requiring access for their job responsibilities.	Inspected documentation showing all issued electronic building badges to determine that server room access was restricted to authorized personnel. Observed the server room access points to determine that access is restricted via the security (badge) system.	***Exception Noted:*** The key fob issued to the janitor was identified to have server room access which was determined not to be required for their job responsibilities.
6.4	Heat, smoke, FM200 automated suppression system and intrusion detectors are connected to a monitored alarm system to the computer room facility. Further, handheld fire extinguishers are located throughout the facility.	Observed the Site-Four facility to determine that the building has heat, smoke, FM200 automated suppression, and intrusion detectors connected to the alarm system, and fire extinguishers are present in the facility.	No exceptions noted.
6.5	An Uninterruptible Power Supply (UPS) system with power conditioners is installed to protect the server room facility from short or long-term power failures.	Observed the Site-Four server room facility to determine that the facility had Uninterruptible Power Supply (UPS) devices.	No exceptions noted.
6.6	A diesel generator is installed at the facility to protect the building from power failures.	Observed the Site-Four Facility to determine that the facility had a diesel generator installed.	No exceptions noted.

SECTION V: Other Information Provided by Site-Four, LLC (Unaudited)

The information included below is presented by Site-Four to provide additional information to their customers and is not part of Site-Four's description of their CU*BASE Host Processing Services. The information presented here has not been subjected to Crowe's examination procedures and, accordingly, Crowe expresses no opinion on it.

Management's Responses to Identified Exceptions

Site-Four's Control	Results	Management's Response
1.8 The subservice organization is subject to annual evaluation in accordance with the vendor risk assessment process.	The annual review of the subservice organization was timed to occur October 2022. Management subsequently completed the review April 2023.	CU*Answers audit frequency differs from Site-Four and Site-Four reviews all audits performed at CU*Answers which pertain to Site-Four. While documentation of the critical vendor is reviewed throughout the year, the formal documentation process will be enhanced and documented at least annually as part of the annual business plan cycle.
6.3 Access to the server room is restricted via the security (badge) system and is limited to personnel requiring access for their job responsibilities.	The key fob issued to the janitor was identified to have server room access which was determined not to be required for their job responsibilities.	This is due to the growing pains involved in switching security vendors. Upon review it was determined that the janitor profile was granted excess permissions and a request was submitted to Explorers CU for a logging history and to have additional changes implemented to further segregate the Operations and Datacenter areas within the security system and applied to the profile. Site-Four was notified that this request has been forwarded to the security vendor and will be monitored for resolution.