CU*NorthWest

A Credit Union Service Organization

BUSINESS CONTINUITY PLAN

Version: v20230324-[PUBLIC]

**Portions of this document have been omitted and labeled as [CONFIDENTIAL] for distribution.*

Confidentiality Statement: *This document contains sensitive information regarding the operations of CU*NorthWest and the CU*Asterisk partner network. It may not be distributed without the consent of the CU*NorthWest Executive Team.*

Plan Contents

LEGAL DISCLAIMER

The information contained in this report does not constitute legal advice. We make no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained in this report. You should retain and rely on your own legal counsel, and nothing herein should be considered a substitute for the advice of competent legal counsel.

These materials are intended, but not promised or guaranteed to be current, complete, or up-to-date and should in no way be taken as an indication of future results. All information is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose. In no event will CU*NorthWest, its related partnerships or corporations, or the partners, agents or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information provided or for any consequential, special or similar damages, even if advised of the possibility of such damages.

NOTE

Data and information contained within this Plan (where applicable) has been provided by CU*NorthWest in the form of electronic files/documentation and as the result of notes taken during conversations with key personnel. It is the responsibility of CU*NorthWest to maintain this Plan to ensure contents are accurate and current.

**Portions of this document have been omitted and labeled as [CONFIDENTIAL] for distribution.*

Introduction

This document is designed for the purposes of equipping and preparing CU*NorthWest and its partners for the expected impact of unplanned disruptions to business functions and processes and for contributing to the resiliency of operations.

The Business Continuity Plan is "a roadmap for continuing operations under adverse conditions (i.e., interruption from natural or man-made hazards)." The plan is the primary tool used for preparedness training, testing and exercising. The best investment in business continuity management is a well-trained recovery team. The plan should be studied, and its contents well known prior to the next disruption.

Scope and objectives

A disaster is a unique event, and the provisions of this plan can be used as the basis for controlling specific recovery operations at management's discretion. Execution of this plan will help facilitate the timely recovery of core processing critical business functions.

The core framework of this plan was developed with the following objectives:

- To protect personnel and property (assets)
- To minimize the financial losses to the organization
- To serve clients with minimal disruptions
- To mitigate the negative effects of disruptions on business operations

The procedures contained within have been designed to serve as a guide for responding to emergencies based on recognized standards and best practices, written with the FFIEC published recommendations in mind. Details about these recommendations can be found at the FFIEC website or at https://ithandbook.ffiec.gov/it-booklets/business-continuity-management.aspx.

Confidentiality Statement

This plan is strictly confidential and is not to be shared with anyone outside the CU*Asterisk network without the express permission of the CEO. Full copies of the current Plan are kept by each management team member. All questions from the news media or other external sources regarding the plan or any disaster/incident should be directed to the Incident Manager or CEO.

*See "Crisis Communications" section.

Assumptions

The following assumptions have been considered during the creation of this recovery plan. The specific circumstances of any disruption may require modifications to the recovery effort.

- Key personnel have been identified and trained and are available to activate the recovery plan.
- Current backups of the application software and data are intact and available at a quickly accessible storage facility.
- Service agreements are maintained with the application hardware, software, and communications providers to support the emergency system recovery.

Plan Maintenance

The CU*NorthWest Business Recovery Plan will be revised every twelve months or as needed based on:

- Changes in potential threats or risks,
- Considerable changes in business operations, functions, or processes,
- Considerable changes in system or network architecture,
- Audit recommendations,
- Lessons learned from tests, exercises, and events.

Revised plans will be distributed to all Incident Response Team members, Board of Directors, and staff with direct roles and responsibilities within the plan. General information about the continuity plan and program will be made available on the corporate web site and a sanitized (scrubbed") version of the plan available to client credit unions upon request.

Revised on (Date)	Revised by:	Notes	Board Acceptance (Date)
3/24/2020	C. Green/ J. Lawrence	Annual revision, added pandemic testing	n/a
9/22/2021	C. Green/ J. Lawrence	Annual revision, added testing	n/a
3/24/2023	C. Green/ J. Lawrence	Annual revision, audit recommendations	3/28/2023

Awareness and Training

To ensure all personnel are knowledgeable of the Plan and aware of their roles during a recovery effort, CU*NorthWest will commit a portion of annual management and staff meetings for educating employees as part of the ongoing business continuity planning cycle. In addition, training events and exercises for those with specific roles and responsibilities will be conducted as needed, particularly when any plan modifications have been made.

Testing and Exercising

Recovery plans (or portions thereof) are to be tested regularly to:

- Ensure completeness and accuracy of the procedures within the plan.
- Identify areas within the plan that are weak and require modifications to improve plan effectiveness.
- Provide training and practice for recovery teams.
- Demonstrate (building confidence in) our ability to recover critical functions meeting acceptable time objectives.

Types of testing include:

- **Life safety exercises**
  - Examples are building evacuation or shelter-in-place drills.
- **Plan walk-through/tabletop reviews**
  - Example is a plan review/walk-through with recovery team member(s) in a conference/meeting room environment.
- **Stand-alone exercises**

- Recovery/relocation of a single business unit/department, single process/function, or single device/system.
- An example would be testing secondary data communications to simulate an outage of the primary data communications circuit.

- **Comprehensive exercises**
    - A large-scale recovery effort such as rolling core-processing from the primary data center to the secondary data center.
    - Recovery of local LAN servers using Unitrends cloud solution.

*See "Continuity and Recovery Strategies" section for more information.

Date of Testing Event	Areas of Plan Tested	Notes about Test Event	Test Participants
11/10/2019 – 11/17/2019	HA Rollover from Prod to HA in Kentwood, MI	Full rollover with credit unions operating on HA Server	CU*NorthWest, Site-Four, CU*South, CU*Answers
3/16/2020	Pandemic Testing	Employees worked remotely testing their pandemic plans	All CU*NorthWest staff
6/14/2020 – 6/21/2020	HA Rollover from Prod to HA in Kentwood, MI	Full rollover with credit unions operating on HA Server	CU*NorthWest, Site-Four, CU*South, CU*Answers
10/11/2020 – 10/18/2020	HA Rollover from Prod to HA in Kentwood, MI	Full rollover with credit unions operating on HA Server	CU*NorthWest, Site-Four, CU*South, CU*Answers
3/21/2021 – 3/28/2021	HA Rollover from Prod to HA in Kentwood, MI	Full rollover with credit unions operating on HA Server	CU*NorthWest, Site-Four, CU*South, CU*Answers
11/7/2021	Rollover to new iSeries	Full rollover to new iSeries unit	CU*NorthWest, Site-Four, CU*South, CU*Answers
3/20/2022 – 3/27/2022	HA Rollover from Prod to HA in Kentwood, MI	Full rollover with credit unions operating on HA Server	CU*NorthWest, Site-Four, CU*South, CU*Answers
11/6/2022 – 11/13/2022	HA Rollover from Prod to HA in Kentwood, MI	Full rollover with credit unions operating on HA Server	CU*NorthWest, Site-Four, CU*South, CU*Answers

*Most recent HA rollover report is included in the appendix of this document. Prior reports are available on our web site at: https://cunorthwest.com/due-diligence/

Executive Commitment

Board and senior management responsibilities in Business Continuity Planning include:

- Establishing policy by determining how the institution will manage and control identified risks.
- Allocating knowledgeable personnel and sufficient financial resources to properly implement the Business Continuity Plan.
- Ensuring that the Business Continuity Plan is independently reviewed and approved at least annually.
- Ensuring staff are trained and aware of their roles in the implementation of the Business Continuity Plan.
- Ensuring the Business Continuity Plan is regularly tested on an enterprise-wide basis.
- Reviewing the Business Continuity Plan testing program and test results on a regular basis.
- Ensuring the Business Continuity Plan is continually updated to reflect the current operating environment.

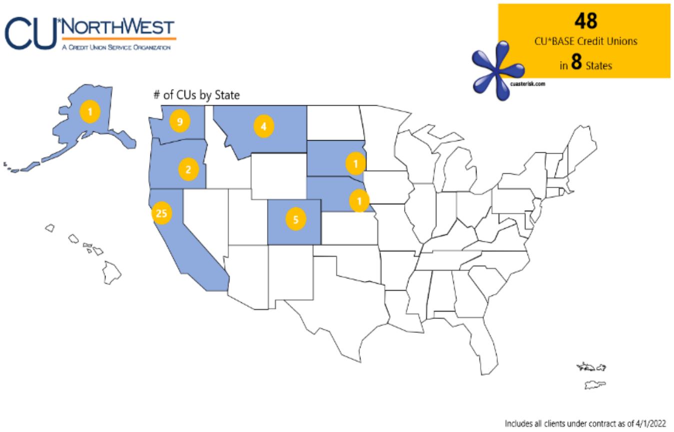
Corporate Environment

Operational overview

CU*NorthWest was founded in 2005 and is a 100% credit union owned CUSO located in Liberty Lake, Washington. CU*NorthWest offers a wide variety of services for credit unions including its flagship CU*BASE/GOLD core processing system in both an online (ASP) and in-house environment, as well as Internet development services featuring the ItsMe247 online/mobile banking product. CU*NorthWest provides expertise in implementing technical solutions to operational needs and helps credit unions form strategic alliances and partnerships.

CU*NorthWest is a strategic partner in the CU*Asterisk network that includes CU*Answers, CU*South, Site-Four, eDOC Innovations, CU*Axis, and Xtend. Each of these partners provides products and services that complement the core-processing CU*BASE/GOLD platform.

CU*NorthWest
A Credit Union Service Organization



CU*NorthWest employs 17 staff members and serves 48 client credit unions located in the following states:

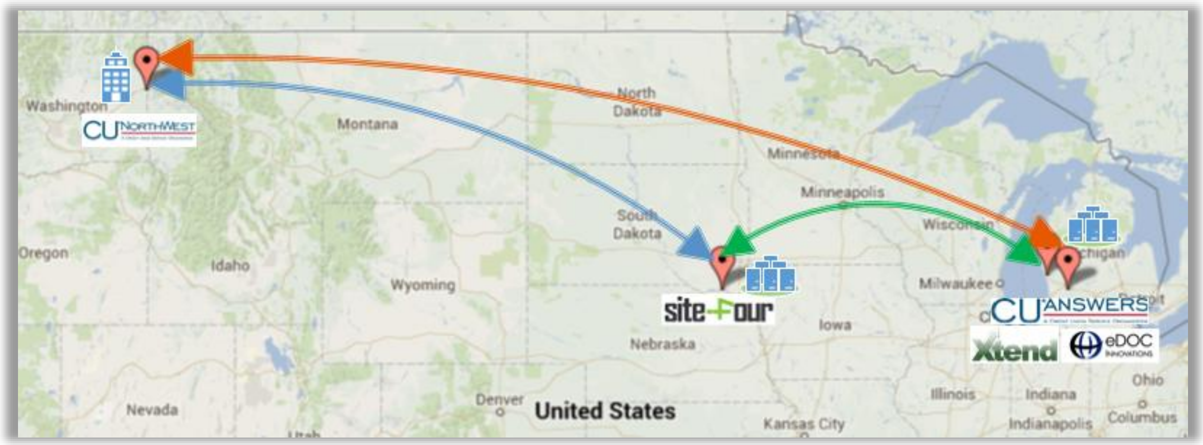
- Alaska
- California
- Colorado
- Montana
- Nebraska
- Oregon
- South Dakota, and
- Washington

CU*NorthWest is an active member of the CU*Asterisk network.

cuasterisk.com

Current Operational Environment

The systems and components required to provide products and services to the network of credit unions are spread among multiple, geographically dispersed CU*Asterisk partner locations as shown below.



CU*NorthWest currently maintains a contract with Site-Four to provide systems and networks for production and high-availability (HA) CU*BASE/GOLD core-processing services including third party EFT communications. The primary production host is located at the Site-Four data center in Yankton, SD. The secondary HA host is currently located at the CU*Answers production data center in Kentwood, MI. Site-Four owns and maintains all equipment required for core-processing at these two locations.

Additional products and services to complement CU*BASE/GOLD are provided by CU*Answers, Xtend, and eDOC Innovations. Systems and networks used to provide products and services for Xtend and eDOC Innovations are hosted within the CU*Answers data centers, located in west Michigan.

For the purpose of this recovery plan, we identify dependencies and alternate strategies for the recovery of:

1. CU*BASE/GOLD (core-processing)
2. Customer Support / Client Services (critical business functions)
3. Extended products / services that complement core-processing (i.e., online/mobile banking)
4. Back-office and internal operations

CU*BASE gold edition

The table that follows identifies key products and services provided by each CU*Asterisk partner.

Key products/services and business functions by CU*Asterisk Partner include:

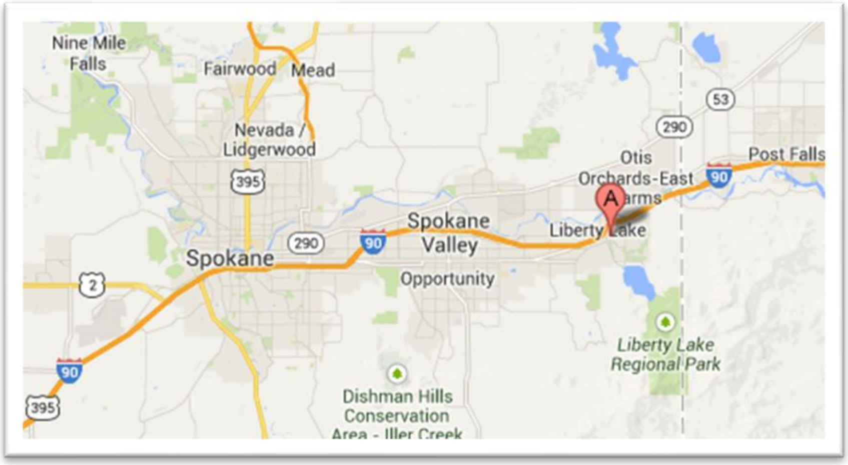
CU*NorthWest	CU*Answers
Departments/Functions • Client Support • Technical Support • Sales/Marketing • Finance • Human Resources/Payroll • Programming • Conversions Systems/Applications • Secondary Production System (CU*BASE) ○ Managed by Site-Four • Secondary Third-Party EFT Data Communications ○ Managed by Site-Four • Secondary Operations Support • File/Print Services • CU*BASE Development/QC • QuickBooks • SGMS Firewalls	Departments/Functions • After Hours Client Support • Technical Support Systems/Applications • It's Me 247 • CU*Talk • CU*Spy • CU*Checks/Check 21 • AnswerBook • VoIP Phones/Fax • Email (MS-Exchange) • Skype for Business • Great Plains/Dynamics • Nucleus (portal) • Corporate Web Site • Indirect Lending • PLM
Site-Four	**Xtend**
Departments/Functions • Primary Operations Support Systems/Applications • Primary Production System (CU*BASE) • Primary Third-Party EFT Data Communications	Departments/Functions • SRS Bookkeeping • Member Reach • Call Center Services • Shared Branching
eDOC	
Departments/Functions • eDOC application support and installation Systems/Applications • iDOCVault • ProDoc2020	

Corporate Office

The Liberty Lake office functions as the corporate headquarters for CU*NorthWest.

[A]
CU*Northwest HQ
1421 North Meadowood Ln.
Suite 130
Liberty Lake, WA 99019
866-922-7646

- Corporate Office
- Client Services
- Technical Support
- Administration
- Sales/Marketing
- Conversions
- Etc.



To enable staff to perform critical business functions that support the products and services delivered to client credit unions, workspace and IT equipment are provided including:

- PC/Workstations
- VoIP Phones
- Printers
- File/Print servers
- Etc.

Systems and network devices at the corporate office are monitored 24x7 by CU*NorthWest Network Services.

*See "IT Recovery" section for procedures to recover IT equipment at the corporate headquarters.

UPS units are installed in the server room to maintain power to critical LAN components (FW, router, switch, file/print servers, OPS console, etc.) for short-term power outages. UPS has the capacity to power critical network devices for up to two hours.

*See "Emergency Response Procedures" for scenarios such as power outages for the corporate headquarters.

In the event the corporate headquarters is not available, alternate recovery locations include:

- Remote access (SSLVPN) for most support personnel with an Internet connection
  - Requires that the remote access environment at the corporate headquarters is available.
- Spokane Firefighters Credit Union (approx. 20 minutes from corporate headquarters)

*See "Establishing Command and Control" section for more information on alternate work locations.

CU*Asterisk partners are also available to assist with performing critical business functions in the event the corporate headquarters is not available.

- **Client Services** support is available at CU*Answers
- **Operations** support is available at Site-Four and CU*Answers
- **Programming, Management, Finance, Sales, Conversions, and Technical Services** support is available at CU*Answers.

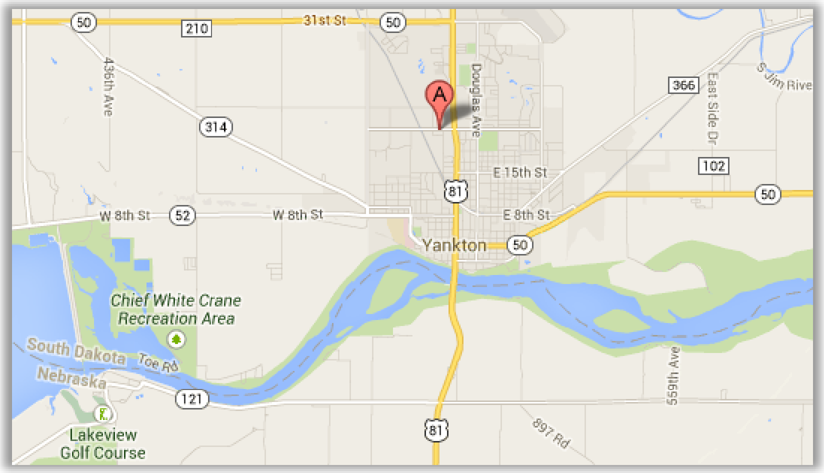
Site-Four

Site-Four is a CUSO and CU*Asterisk network partner. Primary production of CU*BASE/GOLD core-processing is provided by Site-Four from the state-of-the-art data center in Yankton, SD. Staff at Site-Four are responsible for daily operations of the host and network configurations that communicate client credit unions and third-party EFT vendors. Site-Four also provides core-processing CU*BASE/GOLD for CU*South (CUSO and CU*Asterisk network partner located in Fairhope, AL).

In the event that systems at the Site-Four location in Yankton are not available, rollover procedures are performed to bring core-processing online at the HA location at CU*Answers (Kentwood, MI).

[A]
Site-Four, LLC
609 West 21st Street
Yankton, SD 57078
605-689-4309

- Production Data center
- CU*BASE/GOLD
- iSeries Administration
- Operations Support
- Client VPN
- Third Party EFT
- Etc.



Site-Four Emergency contact information:

- [CONFIDENTIAL]

Prevention measures taken by Site-Four to mitigate the risk and/or impact of an emergency or disaster at the Yankton data center include but are not limited to:

- [PROCEDURES CONFIDENTIAL]

Site-Four has their own business recovery plans and performs regular recovery testing.

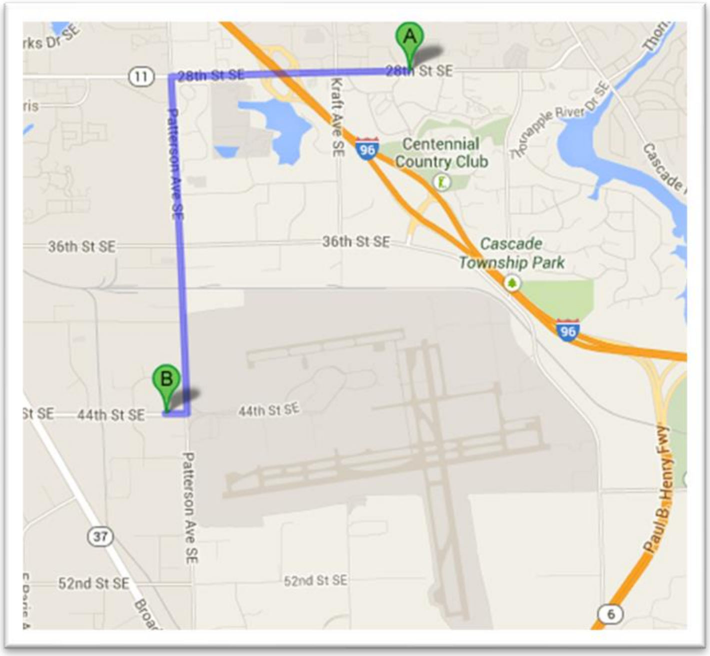
*See “Continuity and Recovery Strategies” section for additional details.

CU*Answers

CU*Answers is a CUSO and CU*Asterisk network partner. CU*Answers maintains three locations in Michigan and is the primary developer and vendor for CU*BASE/GOLD software. In addition to the corporate offices in Grand Rapids, MI, CU*Answers maintains a primary production data center in Kentwood, MI, a secondary non-core recovery data center in Grand Rapids, MI, and a high-availability environment at Site-Four as part of a colocation agreement.

[A]
CU*Answers Corporate Office /
Non-Core Recovery Data center
6000 28th street SE
Grand Rapids, MI 49546
800-327-3478

[B]
CU*Answers Production Data center
4695 44th street SE
Kentwood, MI 49512
800-327-3478
x132 Operations (24x7)
x266 Network Services



While Site-Four provides CU*BASE/GOLD core-processing for CU*NorthWest client credit unions, CU*Answers provides many of the complementary products and services including:

ItsMe247
CU*Checks
Exchange Email
Internal Portal
CU*A Imaging Solutions

CU*Talk
AnswerBook
VoIP Phone System
Corporate Web Site
Secondary Operations Support

CU*Spy
Move IT
Skype for Business (IM)
Great Plains/Dynamics

In addition, CU*Answers provides support for critical business functions from many departments including:

Client Services
Network Services
Accounting
Administration

Operations
Programming
Marketing
Collections

Conversions
Human Resources
Web Design
Internal Auditing

CU*Answers maintains a separate Business Continuity Program with regular recovery testing. Information about the program including reports from recovery exercises and test can be found at: https://www.cuanswers.com/solutions/business-continuity/

The HA network for CU*NorthWest is hosted at the CU*Answers production data center in Kentwood, MI. In addition to the HA host, secondary data communication lines for third-party EFT vendors and backup VPN communications for client credit unions have been installed and configured. The CU*Answers data center relationship and all equipment for the HA network is owned and managed by Site-Four.

The state-of-the-art data center includes redundant components such as:

- Power sources (utility, UPS, generator with auto-transfer switch),
- Internet Service Providers (ISP), and
- Computer Room Air Conditioning (CRAC) units.

The data center also includes physical access security (proximity fobs, video surveillance, etc.) and is staffed 24x7.

Systems at the Kentwood location are not mission critical for primary production core-processing when systems at the Site-Four location are available. CU*BASE/GOLD data is replicated in real-time to the HA host using iTERA software. Replication status is managed and monitored by Site-Four. Regular rollover exercises are performed to validate procedures and confirm operations from the Kentwood location.

Systems and network devices at the Kentwood location are monitored 24x7 by Site-Four and by CU*Answers Network Services. A copy of the CU*Answers SSAE-18 (SOC) reports are available at: https://www.cuanswers.com/about/due-diligence-materials/

CU*Answers Emergency Contact: 800-327-3478 x132

Xtend

Xtend is a CUSO and CU*Asterisk network partner that provides services for credit unions to reach members through marketing, call center, and shared branching services and to complement back-office accounting operations and mortgage processing. Products and services delivered by Xtend are hosted at the CU*Answers data center(s) in MI and are included in the recovery plans for Xtend and CU*Answers.

Products and services provided by Xtend to CU*NorthWest clients include SRS Bookkeeping, Contact Center, Communication Services, Shared Branching, etc.

Xtend Emergency Contact: 800-327-3478 x313

eDOC Innovations

eDOC Innovations is an electronic document solutions provider and CU*Asterisk network partner. The eDOC corporate office is located in Middlebury, VT. A remote office used primarily for software development and support is located in Midway, UT. The eDOC ASP environment is hosted at the CU*Answers Kentwood data center and part of the eDOC and CU*Answers recovery plan.

Products and services provided by eDOC include: ProDOC, iDOCVault, Check21, RDC, etc.

eDOC Emergency Contact: 800-425-7766

CU*Answers Imaging Solutions

CU*Answers Imaging Solutions (CIS) supports online and in-house electronic document products and strategies. The sole office for CIS is located within the CU*Answers headquarters in Grand Rapids, MI. Products and services delivered by CIS are hosted at the CU*Answers data center(s) in MI and are included in the recovery plans for CU*Answers.

Products and services supported by CIS include: ProDOC, iDOCVault, CheckLogic, CU*SPY, etc.

CIS Emergency Contact: 800-327-3478 x132

Recovery at a Glance

Planning for every possible scenario is neither practical nor effective. Possible scenarios considered for this plan include:

- Loss of site or denial of access (no physical access to one or more sites)
- Loss of critical functions (service, department, vendor, supplier, etc.)
- Loss of power or other services (utilities, cooling, etc.)
- Loss of critical equipment (hardware/software)
- Loss of communications (data, voice)
- Loss of skilled personnel (injury, illness, pandemic)
- Breach of security (network/system compromise)
- Anticipated disaster (forewarned, severe weather, etc.)

It's important to recognize that each incident is unique and requires careful assessment and an appropriate and coordinated response. Not every incident has the capacity to disrupt business functions, but every incident has the potential to create an impact.

Key factors to consider when making decisions during a disruption include:

- Safety of all personnel (evacuation, shelter, etc.)
- Security of data
- Availability of core services, including timing, expected duration of outage, etc.
- Proactive monitoring and controls to detect potential additional disruptions and to alert recovery staff
- Accurate initial assessment to enact proper plans and minimize downtime
- Existing service level agreements with clients and vendors
- Client and vendor expectations
- Each plan's inherent lead time (preparation, chasing down tapes, travel, etc.)
- Importance of the first few minutes and hours of an event
- Potential FUD factor (fear, uncertainty, doubt) of recovery teams, chaos during initial stages, remain calm
- The status of the work in progress at the time of the disruption

Several controls have been implemented during day-to-day operations in an effort to prevent, manage, control, and mitigate the impact of identified risks. During a disruption, additional inherent security risks must be considered such as:

- Reduced fault tolerance during the recovery
- Reduced redundancy of data during the recovery
- Compounded failures (snowball/domino effect, uncontrolled events have a tendency to escalate)
- Physical/network security at alternate sites
- Recovery team fatigue during lengthy recovery efforts

Additional financial considerations include:

- Lost revenue from service outage
- Need for temporary (skilled) staffing
- Equipment rental during the recovery efforts
- Extra shipping costs for moving equipment and materials
- Travel/lodging expenses for recovery teams and displaced staff
- Legal obligations for deadlines missed and service level agreements not met
- Overtime costs (labor) for staff and vendors
- Reputation/brand image (potential future revenue)

Recovery Timeline

This timeline provides a summary of the reaction and recovery process to a disaster. It is designed to help management keep perspective amid the crush of details and problems that occur during the disaster and to educate staff and volunteers who are not regularly involved in the disaster planning process.

The "Incident Response Team" is responsible for coordinating an assessment of the situation as quickly as possible. The purpose of this assessment is to identify the scope of the disaster and to provide the basis for a declaration of disaster. Specific areas that must be evaluated are the condition and availability of staff members, condition and availability of facilities and the condition of key computer and business systems.

1. **Incident detected.**
    a. Invoke Emergency Response Plan is required.
    b. Perform initial response to mitigate risk (fire extinguisher, fire alarm, power down, etc.).
    c. Evacuate premises or seek safe shelter if necessary.
    d. Call local authorities (911 or as appropriate).
    e. Alert recovery site (alternate branch or reciprocal arrangement) if necessary.

2. **Establish chain of command**
    a. A clear chain of command strategy should be determined prior to a disaster to anticipate scenarios where communication channels and/or select Management Team members are not available. It is important that this does not create a delay in key decision making, especially during the early stages of a recovery.

3. **Assess situation.**
    a. A quick and accurate assessment is required. Consider elements of the incident such as:
        i. The availability and condition of staff members
        ii. The condition and availability of facilities, and
        iii. The condition of key computer and business systems and vital records.
    b. Engage additional Emergency Response Units if needed (Fire, Police, EMT, etc.).
    c. Escalate the incident if necessary.
    d. Alert outsourced service providers if necessary (Site-Four, CU*Answers, Xtend, etc.).

4. **Declare crisis severity based on assessment (escalate)**
    a. Consider scope and duration of disruption based on the results of the assessment.
    b. Escalate based on scope and expected duration of outage (examples shown below):
        i. 0-24 hours (Disruption)
        ii. 24-96 hours (Emergency)
        iii. 96+ hours (Disaster)

5. **Establish command and control of incident and recovery effort.**
    a. Setup command post (alternate branch or other designated location).
    b. Determine appropriate response to contain incident and initiate recovery plan both during and after business hours.

6. **Notify recovery team members.**
    a. Communicate to recovery team members the description of the incident, extent of damage, recovery location, and prioritized action plan based on the circumstances of the incident.
    b. Invoke HA rollover procedures if conditions warrant.
    c. Invoke IT Contingency Plan if conditions warrant.
    d. See "Incident Response Team" section for recovery team leaders' contact information.
    e. See "Appendix" for all-staff contact information.
    f. Mobilize teams to alternate recovery location(s) if required.

7. **Notify key stakeholders (members, vendors, media, etc.)**
    a. See "Crisis Communications" section of Plan.
        i. Send CU*BASE Alert and Announcement (or request CU*Answers to issue)

8. **Recover core processing business functions.**
    a. Consider alternate recovery strategies based on circumstances of disruption.
    b. Document and log recovery efforts including personnel hours worked.
    c. Monitor and control all disaster recovery related expenses.
    d. Provide status report to all recovery teams.

9. **Notify Insurance Claims Adjustor**
    a. Notify [CONFIDENTIAL] for Insurance purposes.

10. **Recover remaining business functions.**
    a. See "Recovery at a Glance" section of Plan.
    b. Provide status report to all recovery teams and key stakeholders.

11. **Repair/replace facilities and systems.**
    a. Direct and control all salvage efforts related to facilities and vital records.
    b. Coordinate the restoration / building of permanent location.
    c. Procure replacement equipment and supplies as necessary.
    d. Schedule move back to main location.

12. **Return to permanent location.**
    a. Resume normal operations.
    b. Provide status report to all key stakeholders.

13. **Assessment of response and recovery efforts**
    a. Schedule debriefing meeting to evaluate the effectiveness of the disaster response.
    b. Identify required modifications for Recovery Plan.
    c. Prepare gap analysis report based on findings.

Emergency Response Plan

Initial response to a (potential) incident is key to an effective recovery.

No document can contain all of the practical responses for the wide variety of circumstances related to all potential incidents. The emergency response Plan provides critical information and a prioritized list of procedures to be performed for a variety of scenarios with the common goals of:

- Safety of personnel (staff and guests)
- Security of data
- Protection of assets

Emergency First Responders

Fire/Police/EMT: 911

Power Company: [CONFIDENTIAL]
Gas Company: [CONFIDENTIAL]
Water/Sewer Company: [CONFIDENTIAL]
Heating/Cooling: [CONFIDENTIAL]

Office: [CONFIDENTIAL]

The "**Incident Response Team**" is a group of people who are prepared for and respond to any emergency incident, such as a fire and explosion or an interruption of business operations. An accurate and prompt Initial assessment and response during the first few minutes are critical to minimize impact and injury.

A disaster may be declared, and this Plan activated by the Incident Manager of any member of the Incident Response Team.

Incident Response Team

Name	Position	Cell Phone	Alt. Phone	Recovery Role
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]

*See "Appendix" for staff emergency contact information

Responsibilities of Incident Response Team include (or delegation of):

- Identify the disruption.
- Assess the damage (facilities, equipment, services, etc.).
- Decide whether a disaster is to be declared.
- Alert recovery teams (keep track of mobilized personnel).
- Locate and confirm alternate site selection and availability.
- Adapt the Plan to account for prevailing circumstances.
- Prioritize recovery steps.
- Initiate, control and coordinate recovery operations.
- Initiate communications with internal and external stakeholders.
- Approve expenditures related to the recovery process.

- Procure the replacement of destroyed or damaged equipment.
- Offer guidance to local authorities, utilities, services, etc.
- Document and log events as they occur.
- Provide recovery status information to management and board of directors.
- Assemble and verify information for the Crisis Communications Team, who will control its release to stakeholders.

Characteristics and variables of threats to consider when taking action include:

- Speed of onset (some instant, others prolonged)
- Forewarning (some none, other tremors felt)
- Duration (early decisions can shorten or lengthen duration)
- Probability (doesn't only happen to others)
- Impact on functional areas (isolated, wide-spread, domino effect, etc.)

Declaration of Disaster

For incidents where long-term outages and high impact are expected, engaging and mobilizing recovery teams and invoking the proper recovery plan quickly is imperative. This decision is most likely performed by the Incident Manager or action member of the senior management team.

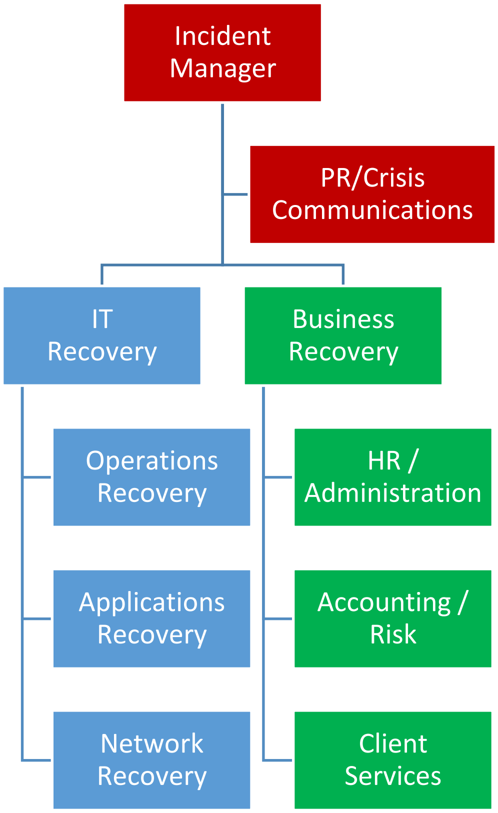
Considerations for making rollover/recovery decisions include:

- Knowing what is involved and the time it takes for performing a rollover is key.
    - Also knowing the amount of time to roll-back if necessary.
- The scope of the incident (list of critical products/services/functions that are disrupted).
- Timing of incident (day, night, weekday, weekend, proximity to open of business day, etc.)
- Status of daily processing (what needs to be completed before credit unions can access data, expected duration, etc.)
- Expected volume (holidays, etc.)
- Impact of disruption (who does it affect, which applications/services, etc.)
- Is the incident contained or is there the potential for it to expand in scope?
- Integrity of data (production and HA replication status)
    - Is rolling over even an option in this circumstance?
    - If we roll, what is the inherent risk?
    - If we don't roll, what is the impact?
- What is plan B if rolling is not an option (know your options)?
    - Recovering from tape?
        - If so, what data is at risk (does it meet RPO)?
        - What is the anticipated recovery time (does it meet RTO)?
- Can we suspend rolling until a more convenient time?
- What is the availability of recovery personnel (how does this impact our recovery effort)?

Roles and Responsibilities

Recovery teams are divided among two recovery paths (Technology and Business). The next several pages show recovery team hierarchy and each team's primary and secondary responsibilities. The Incident Manager has the authority to make changes as needed based on the circumstances of the event.

Perhaps the most important factor to ensure timely recovery is the quality and frequency of communication between recovery teams and management. It is critical that information is fed upstream to keep the decision-making team up to date on the state of the recovery efforts.



Staff emergency contact information is available in the "Appendix" section.

On the following pages you will find specific responsibilities for each recovery team identified above. Each incident or crisis has its own unique set of circumstances and may require individuals and teams to perform multiple roles. It is important that each team is knowledgeable and trained to perform these and other tasks assigned to ensure a timely recovery.

Incident Manager	Responsibilities
✪ [CONFIDENTIAL] ✪ [CONFIDENTIAL]	• Oversee the global efforts of all resumption teams and ensure that recovery goals and timelines are met. • Establish command/control center for management of incident/crisis from top level. • Primary decision maker on the invocation of the Emergency Response and Recovery plans (including HA Rollover activation if necessary) • Serve as liaison to the Board of Directors to get approval for the acquisition of major purchases and for strategic direction. • Communicate with department heads to inform them of strategic direction and the status of the recovery efforts. • Resolve issues of priority based on evolving circumstances. • Determine message communicated to external media (with Public Relations/Communications Team) • Oversee initial damage assessment and approve major equipment purchases. • Offer guidance to local authorities, utilities, services, etc. • Locate and confirm alternate site selection and availability. • Oversee, review, and approve any facility's renovation and construction. • Inform and update Executive Team on recovery status.

PR/Crisis Communications	Responsibilities
✪ [CONFIDENTIAL] ✪ [CONFIDENTIAL] *CU*Answers as needed (Writing Team)*	• Serve as communications point of contact for the entire organization with external media relations (TV, print, web, etc.), public affairs, etc. • Serve as a conduit for all internal communications to and from executive and technical teams, alert staff, clients, major vendors, etc. • Message content creation and distribution (official company holding statements to minimize adverse publicity) • Organize internal meetings/briefings on recovery status (distribute recovery plans as needed) • Organize external meetings/briefings on recovery status (press conferences, etc.) • Inform and update Executive Team on recovery status. • Assist Human Resources Team in communications with personnel and families. • Assist other teams as directed by Incident Manager • Assist in post-recovery cleanup.

HR/Administration	Responsibilities
✪ [CONFIDENTIAL] ✪ [CONFIDENTIAL] *CU*Answers as needed (HR Team)*	• Arrange travel, lodging, meals, and miscellaneous purchases for recovery staff as decided. • Ensure proper office working environment for recovery staff at all facilities. • Ensure injured/ill personnel receive prompt medical attention, families notified, etc. • Ensure all personnel/family issues are resolved (attendance, payroll, insurance/benefits, legal, etc.) • Answer questions about payroll continuation, employment, or securing temporary personnel during the recovery operation. • Ensure proper (safe/secure) working environment at all locations. • Ensure workers' compensation claims are properly filed and processed. • Verify hours worked for staff and schedule sufficient time off. • Hire temporary personnel as required. • Assist PR/Communications Team to organize internal meetings/briefings on recovery status (distribute recovery plans as needed) • Inform and update Executive Team on recovery status. • Assist other teams as directed by Incident Manager • Assist in post-recovery cleanup.

Accounting/Risk/Security	Responsibilities
✪ [CONFIDENTIAL] ✪ [CONFIDENTIAL] *CU*Answers as needed (Accounting Team)*	• Ensure adequate cash flow for expenses during recovery. • Contact supply vendors to increase credit limits and expedite shipping due to nature of event. • Establish emergency accounting and purchasing procedures. • Aid in all monetary details associated with the recovery operations, recording of expenses, post recovery cleanup, intermediate emergency credit arrangements, petty cash, travel advances, etc. • Act as liaison with insurance agency to document, file and settle claims Inform and update Executive Team • Ensure the safety and security of corporate and employee assets including employee and customer information during recovery. • Verify that control mechanisms are in place to ensure data integrity regardless of the emergency or circumstances. • Determine recovery status of vital records. • Purchase, receive, store, distribute all software, equipment and supplies, etc. • Maintain interface with supply channel vendors. • Verify and maintain all receipts and paperwork. • Notify external auditors, if necessary • Inform and update Executive Team on recovery status. • Assist other teams as directed by Incident Manager

Network Recovery	Responsibilities
✪ [CONFIDENTIAL] ✪ [CONFIDENTIAL] *CU*Answers as needed (Network Services Team)*	• Recover network infrastructure (LAN/WAN, etc.) including data and voice communications. • Ensure network/data security and availability. • Order, install, and configure networking equipment as needed. • Confirm recovery-site data-communications lines specifications. • Recover archived data environment and restore data from media for server and application recovery. • Recover/restore servers and appliances for critical business applications and services. • Inventory damaged and undamaged items, determine salvageable status of equipment. • Identify and inventory damaged or destroyed equipment for insurance and replacement purposes. • Repair, replace, install, configure all internal network user hardware (workstations, printers, etc.) • Make repair/replacement recommendations. • Mitigate damage to remaining equipment and facilities. • Assist in establishing/preparing temporary facilities during recovery efforts. • Coordinate movement and storage of salvageable items. • Inform and update executive team on recovery status. • Assist other teams as directed by Incident Manager • Assist in post-recovery cleanup.

Operations Recovery	Responsibilities
✪ [CONFIDENTIAL] ✪ [CONFIDENTIAL] *CU*Answers as needed (iSeries Team)*	• Recover and support iSeries environment hosts, applications, and services. • Ensure host security and availability. • Recover/restore core data processing daily operations and support. • Perform daily operations throughout recovery effort. • Secure/retrieve/deliver the correct tapes, documentation, equipment, media etc. to/from storage or alternate site. • Ensure the security/inventory of all stored media at all facilities. • Manage all backup tapes off- or on-site. • Establish secure storage at off-site locations. • Assist in receiving and storing needed equipment and supplies. • Inform and update Executive Team on recovery status. • Assist other teams as directed by Incident Manager • Assist in post-recovery cleanup.

Applications Recovery	Responsibilities
✪ [CONFIDENTIAL] ✪ [CONFIDENTIAL] *CU*Answers as needed (Operations Programming)*	• Recover/restore/support critical business applications and services throughout the organization. • Conduct quality control testing for recovered applications and services. • Ensure application/service security and availability. • Inform and update Executive Team on recovery status. • Assist other teams as directed by Incident Manager • Assist in post-recovery cleanup.

Client Services	Responsibilities
✪ [CONFIDENTIAL] ✪ [CONFIDENTIAL] *CU*Answers as needed (Client Services Team)*	• Receive and attend to all incoming client-support calls, route calls to appropriate departments if needed. • Assist PR/Communications Team and Human Resources Team in notifying staff, families, clients, vendors, partners, etc. • Inform and update Executive Team on recovery status. • Assist/support network end users including the installation and troubleshooting of all hardware and software issues (workstations, printers, etc.) • Assist other teams as directed by Incident Manager • Assist in post-recovery cleanup.

Establishing Command and Control

Most incidents are relatively small in impact and have a short duration period. For example, a power outage, though somewhat frequent in occurrence (once or twice each year) is short lived (90% less than one hour) with an impact that has been dampened with the deployment of controls such as redundant power sources (UPS). Other incidents can have a much greater impact but may be less frequent (building fire or explosion) however, they still require immediate action to limit and prevent injury and damage. With each incident, our response may be different, but the priorities are still the same.

Priorities:

1. Safety of personnel (staff and guests)
2. Security of data
3. Protection of assets

Once an incident is detected, it is important to establish command and control early in the recovery effort. Normal reaction may be that of confusion and chaos in an emergency situation. Therefore, coordination of personnel and resources during emergencies is a critical function of the **Incident Response Team**.

The Incident Response Team will establish a Command Center upon declaration of a disaster event. Alternative locations to the main branch include alternative office space, home offices (remote working), or a reciprocal credit union site. The location will be disseminated to staff via established call tree processes and as specified in the Crisis Communications section.

Typical items necessary at a command center may include:

- Office supplies (pens, paper, paperclips, envelopes, files, folders, staplers, etc.)
- Fax/printer/copier (with supplies – paper/toner)
- Folding tables and chairs
- Whiteboard and dry-erase markers
- Check stock and specialized forms.

Emergency Response Checklist

- □ Conduct initial status meeting with Recovery Team leaders.
- □ Determine the extent of response and recovery actions to be performed.
- □ Establish frequency of communications to provide support and on-going status of current response and recovery activities.
- □ Observe all staff behaviors and as needed provide periods of rest and relief to relieve stress and correct inappropriate behavior.
- □ Maintain a log of recovery activities (problems encountered, suggestions for improvements to the plan) of each business function affected.
- □ Conduct an initial assessment.
- □ Determine the status of the work in progress at the time of the disruption and provide a status update to the stakeholders and management.
- □ Perform damage assessment.
- □ Determine criticality of damaged/destroyed items or components (salvage).
- □ Cell phone cameras can be used to document disaster area damage.

Incident Assessment

The purpose of the assessment is to gain relevant information and to determine the best strategies for recovering each system and/or critical business function.

System Outage Assessment Report to include:

- Cause of the system disruption, including type, scope, location, and time of disruption
- Location of failing components and those users without service
- Impact of the disruption or components damaged.
- Functional status of all system components (fully, partially, nonfunctional)
- Potential for additional disruption or system damage
- Identification of a single point of failure
- Items to be replaced (hardware, software, firmware, supporting materials)
- Anticipated downtime of the system (i.e., longer than two days?)
- Classification of system failure as minor or major

Post-Incident Assessment

- What was learned?
- What happened that we did not expect?
- What worked, didn't work and why?
- What needs to be done to improve our preparedness?

Post Incident Assessment Report

Date of report: ______________________ Prepared by: ________________________________

Incident Summary		
Date/Time of incident:	Beginning:	End:
Incident reported by:		
Description of incident: (i.e., power outage, technology failure, vandalism, etc.)		
Cause of incident:		
Incident Scope		
Was this a security incident? (If yes, please describe.)		
List branches affected:		
List departments affected:		
List business services interrupted:		
How were members affected?		
Damage Assessment		
Were any injuries reported? (If yes, please describe.)		
List property damage from incident:		
List equipment repaired/replaced:		

Crisis Communications		
Who was contacted during the incident?		Method used (phone, email, Facebook, web site, etc.)?
Staff/Board		
Members		
Emergency Response		
Police/Security		
Media/Public Relations		
Tech Support		
Vendor Support		
Insurance Agency		
Regulatory Agency		
Other		

Recovery Process	
What steps were taken to recover?	
Who participated in the recovery?	
List workaround procedures used during disruption:	

Observations and Notes	
Overall impact to business operations:	
How could the incident have been prevented or avoided?	
How could the response have been more effective?	
Action items for follow up.	

Continuity Insurance

Insurance allows for the organization to recover losses that cannot be completely prevented, and expenses related to recovering from a disaster. Insurance coverage is obtained for risks that cannot be entirely controlled yet represent a potential for financial loss or other disastrous consequences.

Evaluation of Insurance Options

To offset potential losses, CU*NorthWest has purchased insurance coverage for identified perils. This coverage is referred to as business-interruption or additional-expense insurance. Exposures not addressed by insurance will be taken into account in the Business Recovery Plan. There are two basic types of insurance: property coverage and time-element coverage. Property coverage covers buildings, personal property, and equipment and machinery. Time-element coverage covers such items as business income, extra expenses, leasehold interest, and rental value.

CU*NorthWest maintains both types of insurance coverage.

Covered Perils:

- Explosions
- Fire or lightning
- Leakage
- Mine subsidence
- Riot or civil commotion
- Sinkhole or collapse
- Smoke
- Vandalism
- Volcanic action
- Wind or hail

Extensions to Normal Coverage:

- Electrical arcing
- Falling objects
- Glass breakage
- Mechanical breakdown
- Steam explosion
- Water damage
- Weight of ice, snow, or sleet

Property Coverage:

The value of insured assets is generally determined by a combination of methods including actual cash value, replacement-cost value, functional-replacement value, and book value.

Time Element Coverage:

The expenses incurred during the recovery of critical functions. Examples include business income - the loss suffered because we cannot provide our services.

Extra Expenses:

Coverage for those expenses that are beyond the normal operating expenses required to continue operations when premises are damaged during an interruption. The damage must be caused by an insured peril. Examples include:

- Disaster-declaration fees
- Rent for alternative office site.
- Rent for fixtures, machinery, and equipment.
- Light, heat, and power at temporary locations
- Insurance at temporary locations
- Moving and hauling
- Installation of operation at temporary location
- Employee expenses
- Administrative expenses
- Emergency command-post expenses
- Operating expenses

Common Policy Provisions

This section includes policy ground rules, duties under the policy and duties after a loss. These provisions apply to the coverage in the Property, Expense/Income, Lending and Liability sections of the Policy.

The following steps must be done in the event of loss or damage to Covered Property:

- Notify the police if a law may have been broken.
- Give CUNA Mutual Group prompt notice of the loss or damage. Include a description of the property involved. But failure to furnish such notice or proof of loss as soon as reasonably possible will not invalidate or reduce a claim unless CUNA Mutual Group rights are jeopardized.
- As soon as possible, give CUNA Mutual Group a description of how, when and where the loss or damage occurred.
- Take all reasonable steps to protect the Covered Property from further damage. If feasible, set the damaged property aside and in the best possible order for examination. Also keep a record of your expenses for consideration in the settlement of the claim.
- If requested, give a complete inventory of the damaged and undamaged property. Include quantities, costs, values and amount of loss claimed.
- Permit CUNA Mutual Group to inspect the Covered Property and records proving the loss or damage.
- If requested, permit CUNA Mutual Group to question you under oath at such times as may be reasonably required about any matter relating to this insurance or your claim, including your books and records. In such event, your Answers must be signed.
- If requested, send a signed, sworn statement of loss containing the information requested to settle the claim. You must do this within 60 days after CUNA Mutual Group's request. CUNA Mutual Group will supply you with the necessary forms.
- Cooperate with CUNA Mutual Group in the investigation or settlement of the claim.
- Promptly send any legal papers or notices received concerning the loss.
- Make no statement that will assume any obligation or admit any liability for any loss for which CUNA Mutual Group may be liable, without consent.
- In case of loss to "valuable information" make every reasonable effort to collect amounts owed to you.

Insurance Agency:

[CONFIDENTIAL]

Emergency Response Procedures

Response procedures are identified below for the following scenarios:

- Fire/Explosion (requiring building evacuation)
- Severe Weather (requiring seeking safe shelter)
- Flood and Water Damage
- Power Outage
- Injury/Illness/Mass Absence (Pandemic)

Respond to the fire alarm

Evacuate in an orderly manner

Report to assembly areas

Fire/Explosion

When a fire is discovered:

- A member of the Management Team is to notify the authorities and follow any instructions given.

Fire Departments

Spokane	Dial 911	or	534-7377
Liberty Lake	Dial 911	or	928-2462

- Make the following statement: *"This is CU*NorthWest. We are located at 1421 N. Meadowood Lane, Suite 130. We have a fire."*
- Do not hang up until instructed. Be as accurate as you can about details.
- In the event of a minor fire, a fire extinguisher should be activated. Fire extinguishers are located by the door next to the operations room, next to the back door and in the hallway outside the office near the women's restroom.
- Alert other tenants in the building if the fire cannot be extinguished.
- The Management Team will calmly oversee the evacuation of all employees and clients to the parking lot of the shopping center directly behind the building.
- The Incident Manager is to notify the Board of Directors of the situation.

Post-Fire Procedures

- A member of the Management Team will obtain permission to re-enter the building from the Fire Department.
- The Accounting Department is to notify the insurance company:
- Employees are not to re-enter the building until authorized by management.
- Employees are not to open drawers, cabinets, or move any documents until instructed by management.
- Containers holding records should be completely cooled before opening.
- When preparing to open containers, it is advisable to have a fire extinguisher and/or water available in the event of flash ignition.
- Records, which have become brittle or charred, may be placed between glass sheets for further protection until reconstruction begins.
- If necessary, the Management Team will proceed with Step 2 of the Disaster Recovery Plan, including activating backup sites.

Building Evacuation

Upon instruction to evacuate the building, all employees should do the following, **providing time permits and in no way will endanger the employee**:

1. Log off your terminal.
2. Power down terminals, personal computers and printers, time permitting.
3. Log out of phone system.
4. Close and lock file cabinets containing sensitive data in the accounting office.
5. Notify CU*Answers CSR and Site-Four that we are in an emergency situation (time permitting).
6. All personnel who are assigned laptops should make every effort to take their laptops out of the building with them as long as this will not affect their personal safety.
7. A member of the Management Team will oversee that all employees and visitors exit the building and proceed to the parking lot directly behind the building.
    a. **Under no circumstances shall employees or visitors leave the property without notifying a member of the Management Team.**
8. A member of the Management Team will ensure that all windows are closed, and that interior doors are closed but NOT LOCKED so as to allow easy access to fire personnel.
9. A member of the Management Team will stand as close as possible to the main entrance in order to direct police and fire personnel.
10. Members of the Management Team will keep non-essential personnel out of the building, if possible.

Severe Weather / Shelter-in-Place

In case of tornado, flood, or other severe weather condition endangering the safety of CU*NorthWest employees and property, the following steps should be taken:

Tornado

A tornado watch is a forecast of weather conditions, which are ripe for the development of a tornado. Normal CU*NorthWest activities will continue, but management should be kept informed of weather conditions.

- If the watch is upgraded to a tornado warning, management will execute safe shelter plans, relocating all customers and employees to the following location:

    Liberty Lake: Basement of building

- No employee shall be permitted to leave the shelter area or the building until directed by management.
- In the event of damage due to tornado, management shall notify the authorities and follow any instructions given.

Fire Departments	
Spokane Valley	Dial 911 or 534-7377

- Make the following statement: “This is CU*NorthWest. We are located at <building location>. We have been hit by a tornado.” Do not hang up until instructed. Be as accurate as you can about details.

- The CEO is to notify the Board of Directors of the situation.
- The Accounting Department is to notify the insurance company:

CUNA Mutual
5910 Mineral Point Road
Madison, WI 53705
Randy Hefty
[CONFIDENTIAL]
[CONFIDENTIAL]

- If necessary, the Management Team will proceed to activate the necessary backup sites.

Flood/Water Damage

Excess water and flooding can cause damage to multiple areas in the building, including the computer rooms. Repairs for structural damage can prevent staff from returning to their work areas. In severe cases, where large areas of flooring and drywall are in need of replacing, renovation can take up to 30 days or more.

Sources of water can include:

- Restroom (sink, toilet, water feeds, etc.)
- Kitchen (sink, dishwasher, etc.)
- Ceiling (water source and drainpipes, roof leaks, AC unit condensation leaks, etc.)
- Exterior doors, windows and walls where water retention is possible.
- Floor drains (failed sump pump)
- Fire rescue efforts (sprinkler system or fire hoses)

Damage can occur to:

- Electrical systems (building and computer room)
- Structure (weakening walls, floors, etc.)
- Paper documents
- Electronic media (tapes, hard drives, etc.)

In the event of flooding or other water damage:

- Determine if the Building Evacuation plan needs to be activated.
- Determine proximity/risk to computer room (power off equipment as necessary).
- Cover equipment with plastic tarps to protect from roof leaks (warning about humidity and corrosion on computer equipment).
- Determine source of water (roof, pipe, drain, wall, floor, etc.) and location of water-source shut off.
- Determine if sump-pump is functioning properly (between elevator and computer room on west side of building).

During the recovery efforts:

- Ensure that any hardware that is determined to be unsafe to operate is properly labeled. If determined to be safe, unplug equipment from the power source.
- Do not simply power equipment up until you are sure that that any moisture has been removed.
- Visually inspect equipment for external and internal damage. Do not power up any equipment prior to passing this inspection.
- Secure media in dry storage area.

In the event of a flood or threat of flood, the following procedures should be followed:

- Management will monitor weather conditions and determine whether or not evacuation is warranted.

If evacuation is necessary, use the same procedures as outlined for fire evacuation on Page 36. If necessary, employees should evacuate to higher ground located at the Liberty Lake golf course.

- Management will determine possible relocation of materials, such as records, time permitting.
- Management will determine if and when power will be shut down. If necessary, the Client Services department will notify clients of the situation via phone or fax.
- Management is to notify the authorities and follow any instructions given.

Fire Department	
Spokane Valley	Dial 911 or 534-7377

- The CEO is to notify the Board of Directors of the situation.
- The Client Services department will notify clients of the situation.
- The Accounting Department is to notify the insurance company:
- If necessary, the Management Team will activate the Disaster Recovery Plan, including activating backup sites.

Power Outage

The corporate headquarter location has UPS units to power critical LAN appliances and devices for short-term utility power outages up to two hours. In the event a power outage will last longer than an hour, actions must be taken to gracefully power down the equipment beginning with nonessential systems. That decision will be made by a member of the Management Team based on the circumstances of the event.

In the event of a prolonged power outage, contingency plans include enabling remote access to the Site-Four and/or CU*Answers network for connectivity to CU*BASE for product support.

Injury/Illness/Mass Absenteeism (Pandemic Policy)

In the event of injury to personnel (staff or guest):

- Determine if medical help is required.
- Ask for CPR qualified individuals if necessary.
- First aid supplies kits (including AED) are located in the break room.
- Contact the Human Resources department, who will contact family members if needed.
- Record identity of eyewitnesses and notes from event.

CU*NorthWest Pandemic Policy

This document describes the procedures and controls implemented by CU*NorthWest to provide for continuation of business operations necessary to support our clients and partners should a large scale-absence impact our staff.

Definition

A large-scale absence, for the purposes of this document, is defined by CU*NorthWest as missing 50% or more of the employee population for a period of up to two consecutive weeks.

Method

Team leaders were asked to assess specific needs and concerns that they would face in a large-scale absence event for their area(s) within the company. These needs and concerns, the response or reaction to those concerns, and any preventative measures that can be taken have been used in the development of this planning document.

Client Service:

Possible Delays in Service (longer than normal wait before the phone is answered, longer than normal responses to questions that require research, etc.)

Delays in servicing our clients should be expected. However, we would want to communicate this to the client appropriately by sending out a scripted message using our alert procedures. Management would be key in assisting the employees in prioritizing the workload.

Coverage of All Shifts

Cross training and management involvement will help the client service areas to make sure all necessary shifts are covered across all areas of the company. Employees and managers who have the capability to work from home would be encouraged to do so, if the situation allows.

Prioritizing Daily and Pending Duties

Consider the time of the month—there might be things that must be done as they are time sensitive. For instance, is it the end of month? If so, divert team members across departments.

Management would make decisions on readjusting the priority list and delay of non-critical project travel.

Programming

Impact Pending Projects and Other Departments

The projects to be worked on will be prioritized by management; inevitably some projects will need to be delayed or put on hold for a short period of time. We would want to communicate this to the clients appropriately by sending out a scripted message using our alert procedures.

Managing Project Timelines

Management will adjust these timelines and workloads (i.e., briefly delay CU*BASE releases, CU*BASE prototypes and demos if necessary.)

Responsibility for resulting GOLD issues.

Cross training and updated documentation will be an important preventative measure to take in making sure a greater number of employees can be responsible for any GOLD issues. Employees and managers who have access will be encouraged to work from home, if the situation allows.

Delivery

Delivering Quality Service to the Clients

For services that require travel, employees will be expected to be aware of their ability to complete their responsibilities without negative effects on clients. If necessary (i.e., in a conversion situation), CU*NorthWest management may need to make a decision regarding whether or not more employees will need to be sent to supplement for the incapacitated employees.

For services delivered from our offices, cross-training and up to date documentation will be necessary to be able to continue to provide quality service. In some cases, CU*NorthWest may need to contact staffing agencies if additional staff is needed.

Handling Time Essential Duties

Essential duties will still need to be completed; other team members will be assigned these tasks by management as necessary. If possible, management will adjust these timelines and workloads by reprioritizing duties.

At the Client Site

Scenario #1: The entire conversion team is "down for the count". What happens at the client site?

Until additional staff can arrive on site, web and phone conferences would have to be utilized for training, support, sign-off etc. Several concurrent sessions could be scheduled to facilitate training by department.

Depending on the location of the credit union, the VP/Director of Client Experience may tap other CU*NorthWest employees as support staff.

Scenario # 2: What if the Credit Union is going through an event? What would we do for sign offs?

Past experience does give us some guidance in this situation; we can use CPAs and Board members as alternatives to a CEO for sign-off authorization.

Additional support may have to be rescheduled for a particular department. For example, 'live week' may be postponed if several credit union employees are unavailable for the necessary training.

Operations

Shift Coverage and General Department Responsibilities

Primary operations are performed by Site Four. If necessary, adjust schedules of remaining team members to cover all shifts and run with reduced staff per shift. Managers will provide additional coverage as needed. Beginning of Day, End of Day, and File Transmissions must be delegated to other trained team members in the absence of operators from the shift on which the processes are carried out. Operations cross-trains team members on an ongoing basis to ensure delivery of time-sensitive items. An email/call chain is in place in order to contact the Operations Team to let them know of any changes in shift and duties they must fulfill as the situation changes.

Communication

The determination that CU*NorthWest is experiencing a large-scale absence event will happen at the management level. In such an emergency, staff at CU*Answers and CU*South will be alerted for support call coverage.

Should senior CU*NorthWest management determine that conditions warrant informing and alerting clients, the following script may be used as a template to create the email message:

Dear Credit Unions,

*We are notifying you via our alert system that CU*NorthWest is experiencing a large-scale absence of staff due to extenuating circumstances. As a result of this, you may experience delays. If the person you are trying to contact cannot be reached or you need immediate assistance, please call the CU*NorthWest operator and they will be able to help you or direct you to someone who can in a timely manner. Thank you for your patience.*

CU*NorthWest' Management Team

Managers will be responsible for communicating to their staff members any new priorities or changes in responsibilities resulting from the event.

<u>Travel during a Management Declared Event</u>

The travel expectations during an event will be decided upon by CU*NorthWest Senior Executive Team and communicated to the employees by the Human Resources department. Depending on the circumstances surrounding the event, any decision could be made up to and including the suspension of ALL travel.

Staff Interaction during an Event

The staff interactions during an event will be decided upon by CU*NorthWest Senior Executive Team and communicated to the employees by the Human Resources department. Depending on the circumstances surrounding the event, decisions will be made regarding:

- Severely discouraging or disallowing large assemblies of employees (on or off work premises)
- Closing all meeting rooms
- Limiting all staff interactions as much as possible
- Encouraging or forcing employees to work at home.
- Offering masks and setting up for cleaning stations around the office
- Specifically Addressing the Flu Season: Controlling the spread of infection

With the COVID pandemic that started in early 2020 and spread across the globe, we are all a little more aware of methods to limit the spread of infection. This is not the only virus that could create an event to be proactive about, but we will use it as a steppingstone to understand how we will handle a pandemic event if one does occur in the future.

- Infected staff should defer coming to work for the length of the incubation period of the virus.
- Staff should utilize the hand-sanitizing stations provided around the office and wash their hands often.
- Clean keyboards and other equipment, especially if workstations are shared between staff members.
- A certain degree of social distancing could be practiced; reducing frequency, proximity, and duration of contact can also help reduce the spread.

Security Incident Report

[FORM CONFIDENTIAL]

Cybersecurity Incident Response Plan

Introduction

This document is designed for use by the Incident Response Team (IRT) as a framework for detecting, containing, and responding to security incidents involving corporate assets. This plan is a working guide, meaning its contents and usage are subject to adjustments and changes to ensure relevance in the ever-changing field of incident response. This is not a comprehensive guide but offers general guidelines for responding appropriately and in a timely manner to security incidents. The Cybersecurity Incident Response Plan should be used in conjunction with other information security policies and employee handbook.

While the Business Continuity Plan seeks to prepare the organization for any event or scenario that could potentially create a disruption of business operations, Incident Response focuses on those types of events where the security of IT assets, including sensitive information (i.e., PII) is at risk. Like Business Continuity, having an effective Incident Response program requires an understanding of the stages of a typical response.

Stages of an incident response include:

- **Preparation**
    - This stage includes all the activities such as awareness training, risk assessments, testing and exercises, as well as the controls (administrative, physical, and logical) that have been implemented to minimize the impact of a cyber incident.

- **Detection**
    - This stage involves the tools and strategies for monitoring, alerting, and early detection to quickly confirm the existence of an incident and limit the scope. Response teams are notified, and plans executed based on the circumstances of the incident.

- **Containment**
    - Once an incident has been confirmed, prompt action is required to contain the impact, spread, and to minimize the risk of further exposure. Attention must be applied in this and corresponding stages to protect the evidence for proper forensics and analysis.

- **Eradication**
    - Once the incident has been contained, actions in this stage involve cleaning and securing all potentially infected devices to the point that confidence is restored before reintroducing it to the network. Where cleaning is not an option, wipe and reinstall, repair and/or replace may be required.

- **Recovery**
    - This stage involves all steps required to bring the network back to a stable and secure state with close monitoring to ensure that a repeat incident does not occur. Restoring servers or devices from the last known "clean" backup may be one of the options to meet Recovery Time and Recovery Point Objectives (RTO/RPO). Notification is provided to affected stakeholders where necessary (potentially with the guidance of legal counsel).

- **Post-Incident Analysis**
    - Activities throughout the incident should be documented and results reviewed to identify areas for improving the overall security posture and incident response process. A report is prepared and provided to key stakeholders.

- **Risk Mitigation**
    - Experience and lessons learned during each stage of a response aids in enhancing the organization’s ability to manage information security risk.

Incident Response Team

At the heart of the Incident Response Plan is the Incident Response Team (IRT) comprised of a group of people from diverse departments across the organization, prepared for responding to incidents that threaten an interruption of business operations and/or the security of information assets.

The role of the IRT includes:

- Quickly identify threats to the organization’s information assets
- Assess the level of risk and take immediate steps to mitigate impact and loss.
- Notify appropriate authorities and mobilize response and recovery teams.
- Respond and recover to bring operations back to normal.
- Document the response process and report findings along with lessons learned.

The CU*NorthWest Incident Response Team is comprised of the following positions:

- Corporate Officers and Directors
- Department Managers
- Site-Four and CU*Answers IRT members

Responding to an incident requires participation from all business units and departments across the organization. Leadership during a response is a critical role where key decisions are made that may impact the duration of the incident and associated costs. Maintaining business operations during a response effort is desired, assuming the scope of the incident can be contained. Communications and/or public relations to keep key stakeholders informed throughout the incident is important for legal, regulatory, and reputational considerations.

Roles and Responsibilities

Individual roles and responsibilities follow the same structure as the Business Continuity Plan. with added emphasis on the security of IT assets (including systems, infrastructure, and information/data). Actions taken during each stage of the response must consider the impact on business operations overall. Scenarios involving the security risk to IT assets must be documented thoroughly in the event of potential legal ramifications.

Chain of Custody

A proper chain of custody for the evidence should be maintained. A chain of custody is a history that shows how the evidence was collected, analyzed, transported, and preserved. Evidence should be protected from unauthorized access and from modification or damage. Transfers or copies should be approved and witnessed. The IRT will take note of actions and results.

- Logging events clearly in chronological order with a time stamp for each event
- Use a consistent format. See the Security Incident Response Report in the Appendix.
- Include facts, not speculation or unsure interpretation.
- Correct mistakes if found and record the cause of mistakes.

Third-party support during an Incident Response

Effectively responding to security incidents may require skills and expertise not readily available from the CU*NorthWest staff. In such cases, the Executive Team may determine that engaging outsourced support is necessary. Examples include data breach experts and legal counsel. All such activities must be documented and filed with the official incident report.

Forensic evidence

Affected machines should be removed from the network and physically isolated for forensic examination.

- Determine if any countermeasures, such as encryption, were enabled when the compromise occurred.
- Analyze backup, preserved, or reconstructed data sources.
- If applicable, ascertain the number of members affected and type of information compromised.

Chain of custody as outlined above will be followed. The organization will preserve the machines offline and untouched if instructed by law enforcement. All actions will be logged/recorded.

Communications

Communicating in a crisis is a critical component of an effective incident response, both internally among teams and externally to key partners, vendors, customers, as well as law enforcement and regulatory agencies when necessary. Characteristics include the proper content, frequency, and methods used for informing each group of stakeholders.

The Crisis Communications section of the Business Continuity Plan provides additional details including notification and posting of alerts.

Scenarios

Networks and systems today have become highly integrated with multiple external vendors and service providers and are accessed in more ways, due in part to the expansion in type and volume of digital services available 24/7 to a global market. Planning and preparing for every scenario are an exhausting effort.

With early detection and accurate initial assessment, the appropriate response level can be applied (high, medium, low) depending on the scope and duration of the impact, availability of a workaround process, and sensitivity of data or system at risk. Key decisions that must be made include whether to take systems or networks offline during the response effort.

For the purpose of this plan, process, and procedures for types of incidents are grouped into categories based on the nature of the attack and response effort required. These may include, but are not limited to, the following:

- General Incident Response guidelines
- Malware Outbreak (virus suspected or confirmed, or other malicious code)
- Ransomware
- Denial of Service attack (DoS)
- Lost or Stolen Devices

Not all incidents require equal priority. Denial of service attacks, while inconvenient, does not represent the same level of seriousness as does a disclosure of confidential information to unauthorized parties. The Incident Response Team will assign priority based on the actual circumstances and will adjust activities accordingly. If the incident in question specifically deals with the breach of sensitive data, that will take preference.

The threat landscape is constantly changing. Maintaining a strong security posture involves regularly assessing risk, implementing mitigating controls, conducting regular training exercises and penetration tests, maintaining secure networks and devices through hardening and system patching, as well as responding to vulnerabilities in a timely manner.

Vulnerability Management

Vulnerability management is one of many orchestrated steps taken to minimize the risk of an attacker (external or internal) exploiting a vulnerability. Vulnerabilities can be detected in a number of ways, including:

- Announced by professional security organizations.
- Announced by software/hardware vendors.
- Result of regular vulnerability scans (internal and external)
- Result of an actual cyberattack (attempted or successful)

Typically, when announced, vendors will provide either countermeasures for mitigating the risk and/or a software update to apply to correct the vulnerability.

When vulnerabilities are announced or detected, it's important to determine if it's already been exploited (attempted or successful) and the criticality and impact to users on the network to apply the resolution. Is it critical enough to take offline during business hours or is the risk low enough that an after-hours resolution can be scheduled?

Incident Handling Guidelines

Incidents that threaten the security, confidentiality, and availability of IT assets can come from a number of sources from internal threats to cyber-attacks over Internet connections or through trusted vendor networks. Below are general incident handling guidelines with some specific actions for different scenario types.

Early detection and containment are key to an effective incident response. It's important that staff and teams are mindful of potential threats that could be the early signs of an attack. Cybersecurity awareness training is provided to all staff to aid in detection and reporting when social engineering attempts are spotted.

Other forms of detection can come from controls in place such as Intrusion Detection Systems (IDS), Endpoint Detection and Response (EDR), Security Information and Event Management (SIEM), or an external source such as vendor or even law enforcement.

When an incident is detected or reported, it's important to:

- [PROCEDURES CONFIDENTIAL]

Malware Outbreak

Many cyber-attacks include some form of malicious software (malware) used to create backdoors, steal credentials, cover tracks, and upload/download files under the radar of controls in place. It's important that all measures of caution are taken to securely quarantine, eradicate, and recover systems to normal operations. These actions may include:

- [PROCEDURES CONFIDENTIAL]

Ransomware

Ransomware is one of the most active threats today, often using a two-pronged approach to obtain money (digital currency) in exchange for your data back (hostage) and the promise not to expose/sell it to the dark web (extortion).

Most ransomware attacks involve social engineering to lure a network user to click on a link or open an attachment in an email message. Several controls have been implemented to minimize the risk, including regular staff cyber awareness training and logical controls such as web filtering, secure DNS, limited access controls, etc. In addition, protected data backup volumes are maintained with predetermined Recovery Objectives (RTO/RPO) and the capability of restoring systems to pre-incident configurations.

Ransomware has proven to be a lucrative attack vector for multiple groups, including well-funded nation states. At the same time, users, by nature, are not immune to taking the bait. As such, it is important to follow specific guidelines when a ransomware attack is detected.

- [PROCEDURES CONFIDENTIAL]

Lost or Stolen IT Asset

Any IT asset (i.e., laptop or mobile device) that is stolen or destroyed is an incident and potential crime. A common example is the theft or destruction of a mobile device such as a laptop. When these incidents occur, it is important to:

- [PROCEDURES CONFIDENTIAL]

Distributed Denial of Service Attack Response

DDoS

Distributed Denial of Service attacks are just one type of threat faced by organizations that depend on the Internet for business transactions and communications. In response to the heightened awareness surrounding the recent activity from these types of attacks, the following is an overview of the documented DDoS Incident Response Plan.

PREPARATION

The best defense against such security attacks begins with a layered security strategy starting at each hardened host and expanding to security appliances at and beyond the network perimeter. Key to an effective incident response are the skilled and knowledgeable personnel that make up the Incident Response Team.

COMMUNICATION

A critical component of any incident response is timely, accurate and consistent communications at all points within the response phase to all internal and external stakeholders including senior management, affected clients and partners, legal counsel, vendors, and agencies including law enforcement (if appropriate). For use with all incidents and disruptions, CU*Answers has deployed the CU*BASE Alerts Notification Site, (accessible to CU*BASE on-line and in-house clients only) for posting current alert status information in conjunction with broadcast alert email notifications. All affected non-client stakeholders will be contacted using methods identified in the "**Crisis Communications**" section of the *Business Continuity Plan*.

DETECTION

Proper detection of potential incidents begins with 24x7 network and host monitoring from multiple presence points within the network. With these monitoring and alerting tools in place, IRT members are notified around the clock of potential incidents that may require prompt response. Personnel are trained and skilled to take immediate measures to identify the type and scope of the incident and to accurately assess the risk to the organization (particularly the security, integrity, and availability of data on the CU*Asterisk networks).

MITIGATION

Once an incident is detected, mobilized IRT members may determine that mitigating steps are required, ranging from the limiting of access to/from specific hosts and networks to the complete protection of assets by prohibiting all traffic to/from specific hosts and networks.

Depending on the circumstances of the attack, the Incident Response Team may engage the cooperation of upstream service providers and security vendors if necessary.

REMEDIATION AND RECOVERY

Once it has been determined that the incident/attack has elapsed and/or the risk has been reduced, the Incident Response Team will reintroduce services to the network until all have been restored.

Post-attack procedures include the collection of logs and potential forensic evidence (if applicable) and documenting response and mitigation procedure gaps, weaknesses and lessons learned.

Continuity and Recovery Strategies

The products and services that comprise "core processing" are provided by systems at data centers outside of the CU*NorthWest corporate office. CU*BASE GOLD and online/mobile banking applications are configured in a high availability (HA) environment with regular live production rollovers performed to ensure capabilities.

The limited tolerance for downtime for CU*BASE/GOLD core-processing applications require the implementation of real-time data replication on hosts located in geographically dispersed data centers with redundant power and communication resources.

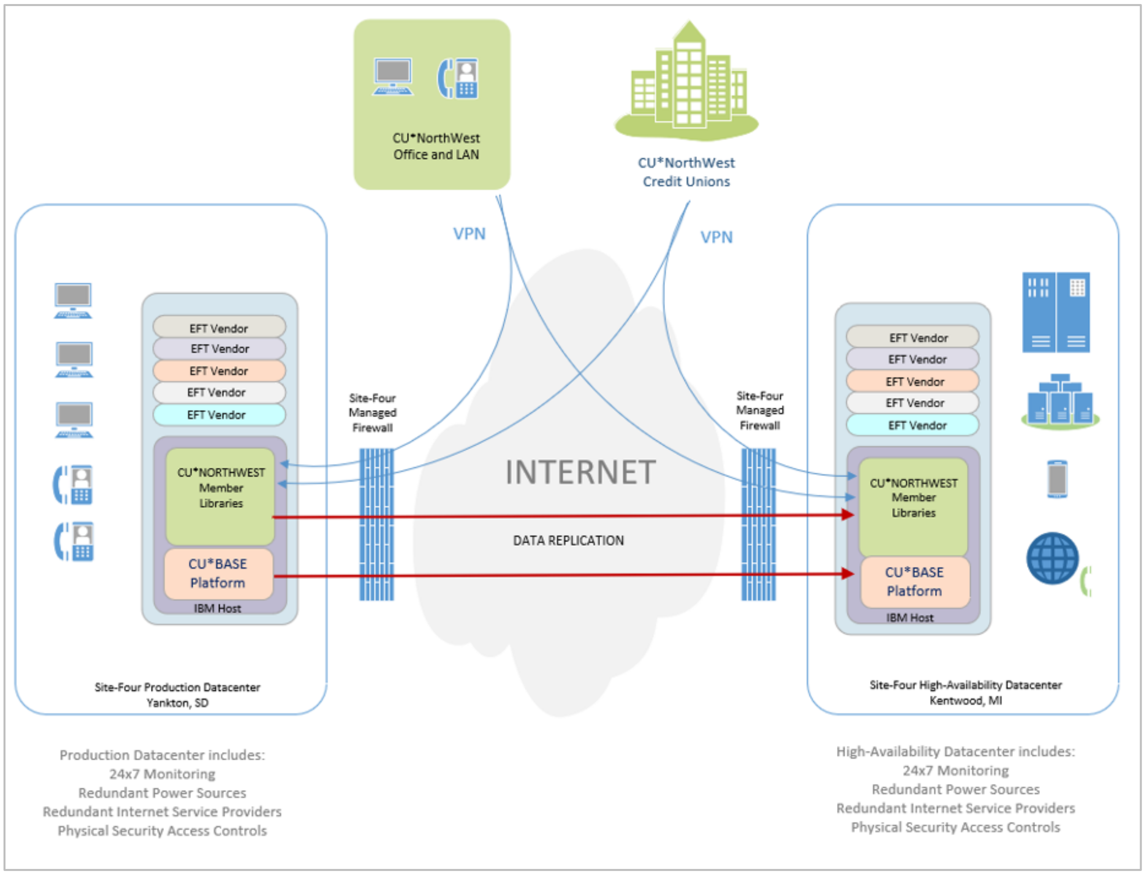
To accomplish this, CU*NorthWest has contracted with Site-Four for providing CU*BASE/GOLD core-processing services in an ASP environment to meet these strict availability and security requirements.

"High Availability" *refers to a multiprocessing system that can quickly recover from a failure with minimal downtime. A "highly available" system or component is continuously operational for a desirably long length of time. Availability can be measured relative to "100% operational".*

For those products and services identified as "(non)core-processing", alternate continuity recovery strategies have been implemented and plans developed and tested to ensure an effective and efficient recovery. Where possible and feasible, redundant components have been included in host and network configuration (i.e., redundant power supplies, hard drives, etc.) to eliminate or reduce single points of failure and to mitigate identified risk.

*See "IT Recovery" section for more information.

Overview of the High Availability strategy



CU*NorthWest Office and LAN
CU*NorthWest Credit Unions
VPN
VPN
EFT Vendor
EFT Vendor
EFT Vendor
EFT Vendor
EFT Vendor
CU*NORTHWEST Member Libraries
CU*BASE Platform
IBM Host
Site-Four Managed Firewall
INTERNET
DATA REPLICATION
Site-Four Managed Firewall
EFT Vendor
EFT Vendor
EFT Vendor
EFT Vendor
EFT Vendor
CU*NORTHWEST Member Libraries
CU*BASE Platform
IBM Host
Site-Four Production Datacenter Yankton, SD
Site-Four High-Availability Datacenter Kentwood, MI
Production Datacenter includes:
24x7 Monitoring
Redundant Power Sources
Redundant Internet Service Providers
Physical Security Access Controls
High-Availability Datacenter includes:
24x7 Monitoring
Redundant Power Sources
Redundant Internet Service Providers
Physical Security Access Controls

Owned and managed by Site-Four, IBM hosts are located at state-of-the-art data centers in Yankton, SD and Kentwood, MI. Vision Solutions' iTERA software is used to replicate member data between the hosts in real-time. Client credit unions connect to both primary (Yankton) and secondary (Kentwood) data centers through Internet VPN communications. Secure third-party EFT vendor networks are also located at both primary and secondary data centers as are ACH transmissions through FedLine VPN appliances. Both sites include redundant communications, redundant firewalls, redundant power (utility, UPS, generator) and 24x7 monitoring. An independent CRAC (Computer Room Air Conditioner) is provided to maintain optimal temperature and humidity. Physical access security and video surveillance are also provided.

In the event the host (PROD) at the primary data center is not available, a manual process is initiated to "rollover" or "swing" production to the host (HA) at the secondary data center. This manual process includes several data integrity checks and audits and a carefully orchestrated sequential process to bring subsystems up on the stand-by host. The rollover process also includes procedures to redirect client credit unions to the secondary data center and to backup EFT vendor communications if necessary.

Performing a core-processing rollover involves several teams. The rollover technical process is primarily managed and performed by staff at Site-Four with the assistance from CU*NorthWest and CU*Answers Network Services for DNS, routing, and firewall modifications. *See "HA Rollover Procedures" section below.

Communications to affected third party vendors is handled by Site-Four while communications to clients and affected stakeholders is handled by staff at CU*NorthWest (see "Crisis Communications" section).

The rollover process may require up to three hours or more (to ensure data integrity, system stability, and vendor availability) depending on the circumstance of the incident. For short-term disruptions or those during non-business hours, the Incident Manager may determine that a rollover is not a practical solution.

Reports published following scheduled rollover events can be viewed at:

https://cunorthwest.com/due-diligence/

*See Appendices for Procedures to perform the HA Rollover and Rollback

Overview of DR strategy (in case the HA Rollover is not an option)

If the rollover process is unsuccessful or if circumstances of the incident are such that the rollover process is impossible or induces increased risk, a host recovery from tape may be necessary. Note that recovery from tape may require 24-48 hours or more before services are restored. This would be considered a disaster scenario.

Host recovery from tape would include "wiping" one of the two hosts, installing the IBM operating system, CU*BASE environment and member libraries. This host recovery effort would be performed by staff at Site-Four with the assistance from technical staff at CU*NorthWest and CU*Answers.

Procedures for recovering PROD are maintained by Site-Four. Procedures for recovering IBM I on the same or different host is available from the IBM web site at: [*Systems Management: Recovering your System*] SC41-5304-10

During a recovery effort, it is important that all stakeholders involved in the recovery or affected by the disruption are notified. Please see "Crisis Communications" section for more information.

Third Party Vendor Communications

Primary data communications for third party EFT vendors are available through the network at Site-Four in Yankton, SD. In the event of an outage at Site-Four, backup data communications are available for most vendors through the network at the CU*Answers data center in Kentwood, MI.

Backup third party communications connectivity is tested during high-availability rollover exercises.

The table below lists the third-party EFT vendors and available data communications. Contact information for each is available in the "Appendix" and "HA Rollover Procedures" section of this plan.

Vendor	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
CO-OP	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
CUSC/NGN	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
FIS EFT	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
FISERV	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
FSCC	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
MAP VISA DPS	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
PEMCO/JHA	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
PSCU/STAR	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
SHAZAM	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
TNB/Vantiv	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
5/3 (Vantiv)	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]

Client Network

Client credit unions have primary data communications through Internet VPNs to the Site-Four data center in Yankton, SD with backup VPN connections at the Kentwood data center. Several client credit unions have deployed redundant communications through multiple ISPs. Client connectivity is monitored and supported by CU*NorthWest and CU*Answers Network Services 24x7. Management of the ISP connections at each client site is the responsibility of the client. Clients with redundant ISP connections are configured for auto-failover in the event of a disruption.

The diagram and images below show a typical credit union connection to both primary and secondary data centers as well as 24/7 monitoring of the VPN circuits.

[DIAGRAM CONFIDENTIAL]

[IMAGES CONFIDENTIAL]

IT Recovery

Overview of IT environment

The corporate office LAN is comprised of workstations, phones, printers, and servers, supported by CU*NorthWest Network Services and CU*Answers. The network infrastructure is protected from power interruptions by UPS units.

[DIAGRAM CONFIDENTIAL]

Data on LAN servers is backed up at regular intervals using the Unitrends solution. In the event of a disaster, servers can be restored locally or virtually in the cloud. The Unitrends solution is also used for backing up managed client networks as part of the "All Care" service.

[IMAGE CONFIDENTIAL]

[Image above shows computer racks at the corporate headquarters]

[IMAGE CONFIDENTIAL]

[Image above shows the computer rack at the Site-Four data center]

[IMAGE CONFIDENTIAL]

[Image above shows the HA network at the CU*Answers data center]

Data Communications

At the corporate office are redundant Internet circuits provided by CenturyLink and Comcast as well as an MPLS* circuit provided by CenturyLink. Data communications at Yankton, SD data center is provided and managed by Site-Four while data communications at the Kentwood, MI data center is provided and managed by CU*Answers.

**A project is initiated in 2023 by CU*Answers to migrate off of all MPLS circuits due to EOL status.*

[DIAGRAM CONFIDENTIAL]

The following data communications lines are owned and managed by CU*NorthWest at the Greenstone office location:

Primary Service Provider: CenturyLink Fiber

- [CONFIDENTIAL]
- [CONFIDENTIAL]

Secondary Internet Service Provider: Comcast

- [CONFIDENTIAL]
- [CONFIDENTIAL]

MPLS Provider: CenturyLink

- [CONFIDENTIAL]
- [CONFIDENTIAL]
- [CONFIDENTIAL]
  - [CONFIDENTIAL]
  - [CONFIDENTIAL]

More details in “[CONFIDENTIAL]”

Loss of Corporate Phone System

The Interaction Client (Genesys) VoIP phone system is provided by CU*Answers from servers at the Grand Rapids, MI data center. Voice lines for both local and long distance are delivered using three carriers AT&T, Lumen/Century Link, and Inteliquent. Redundant Genesys servers and Cisco voice gateways provide voice communications for:

- CU*NorthWest, CU*SOUTH, CU*Answers, eDOC, and Xtend corporate offices
- Incoming faxes to DID #s
- CU*TALK

Probable causes of service outages include:

- Call routing at carrier
- Physical line damage (back-hoe, groundhog, laying sidewalk, etc.)
- VoIP GW hardware/software failure
- CIC server hardware/software failure
- LAN switch-stack failure
- phone firmware upgrade

CU*Answers Network Services (CNS)
800-327-3478 x266

PC/Workstation Build Checklist

CU*NorthWest
A Credit Union Service Organization

Internal Workstation Build Checklist

[PROCEDURES CONFIDENTIAL]

Business Recovery

A disruption that imposes the relocation of IT systems and/or staff to another area within the facility or to an alternate/temporary facility can be the result of several scenarios such as:

- Loss of service (HVAC, communications, power) is expected to last several days.
- Loss of access or physical damage to the structure (fire, water, flying debris, other)
- Large-scale renovation project (planned)
- Hazardous material spill (quarantine)

Recovery steps include:

- Conducting an initial assessment of outage to determine the duration and scope of the event and business functions to resume.
- Identifying alternate facilities and arranging for operations
- Notifying employees and providing instructions on where to report and when.
- Determining if alternate skilled staff is required for the recovery effort.
- Swinging communications to an alternate site (if needed)
- Retrieving records, supplies and resources required to resume operations from off-site.
- Determining the impact of the work in process at the time of the disaster
- Determining materials needed (Office and IT equipment)
- Approving and arranging for purchases
- Setting up shipping/receiving operations for the facility (UPS, FedEx, USPS, etc.)
- Ensuring security of assets and safety of staff at each location (physical access, video surveillance, lighted parking lot, etc.)
- Coordinating the repair and restoration of the disaster site

Office workspace recovery options include:

- Relocating to an alternate space/floor within the same building (if damage is contained to small area and access to building granted)
- Working remotely from home, a hotel or a conference room (assuming SSLVPN access is available)
- Leasing equipped work-recovery-area services (dedicated, shared, mobile)
- Working from client main or branch office (See Alternate "Recovery Locations" section below)
- Securing available commercial space from landlord (Greenstone)

Office workspace recovery requirements include:

- Workstations (monitor, mouse, keyboard, scanners)
- Power distribution units, lighting
- Desk, table, chair
- Printer, copier, fax, shredder, phone
- LAN, switch, cables
- Paper, envelopes, blank checks,
- Extra cell phone chargers
- Whiteboard, markers, easel, flipcharts
- Pens, pencils, staplers, paperclips

Alternate Recovery Locations

Alternate Emergency Operations Center (EOC) locations.

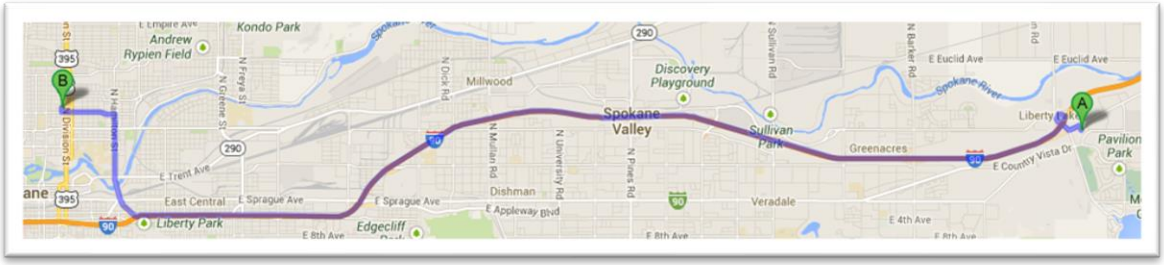
In the event that the Greenstone Offices are not available, an agreement has been made with Spokane Firefighters Credit Union to provide recovery workspace and resources to coordinate the recovery effort and perform critical business functions. The decision to send to alternate recovery location(s) will be determined by the Incident Manager or a member of the Emergency Management Team based on circumstances of the event.

*See "Establishing Command and Control" section for more information.

Several personnel have remote access capabilities to either SSLVPN appliances at the Corporate Headquarters or the CU*Answers location. In a disaster scenario, CU*Answers Network Services personnel can quickly activate any CU*NorthWest employee who does not currently have remote access capabilities.

CU*Answers Network Services: 800-327-3478

Spokane Firefighters Credit Union (approx. 20-minute drive)
2002 North Atlantic
Spokane, WA 99205
(509) 484-5650



[Directions from Greenstone Office to Spokane Firefighters Credit Union shown above]

This location provides up to four workstations with network access and a 12-person board room for an acting Emergency Operations Center.

In the event Spokane Firefighters Credit Union is not available, other optional recovery locations include:

- Cheney Federal Credit Union (approx. 35-minute drive)
  - 520 First Street
  - Cheney, WA 99004
  - 509-235-6533

- Prime Source Credit Union (approx. 25-minute drive)
  - 9707 North Nevada Street
  - Spokane, WA 99218
  - 509-838-6157

CU*NorthWest Business Units and Critical Functions

Each department has identified critical functions performed along with recovery time objectives using the following categories:

- **< 4 hours**: Clients need and expect us to be able to provide this with minimal downtime.
- **< 8 hours**: Clients can operate but would feel the impact if downtime exceeds 8 hours.
- **< 24 hours**: Clients can operate and close the day but expect us to be back by the next day.
- **24-48 hours**: Clients can operate and close for two days but expect us to be back by the third day.
- **48-72 hours**: Clients are inconvenienced but not significantly impacted.
- **72+ hours**: Clients benefit from this but are not impacted during downtime.

Administration/Human Resources (minimum staff 1) [CONFIDENTIAL]

Critical Functions	Recovery Time Objectives
Employee communications concerning the emergency event	< 24 hours
Employee terminations & resignation processing	24 – 48 hours
Disability, leave and/or workers compensation (potentially)	48 – 72 hours
Submitting payroll info and timekeeping/payroll approvals vendors	48 – 72 hours
Processing unemployment claims, garnishments, etc.	48 – 72 hours
General file maintenance (legal implications of losing all personnel files)	48 – 72 hours
Budget and strategic planning	72+ hours
Employee annual planning	72+ hours
Employee coaching and discipline	72+ hours
All hiring and new employee activities	72+ hours
Policy administration	72+ hours
Benefit administration	72+ hours
Security of building	< 4 hours
Communication between executive team and staff	< 8 hours
Creating and distributing key fobs	< 24 hours
Guest services	< 24 hours
Overall facility management	< 24 hours
Processing mail/shipping	24 – 48 hours
Travel arrangements for staff	< 24 hours
Ordering office supplies	24 – 48 hours
Event planning	72+ hours

Dependent on [CONFIDENTIAL]

Client Services (minimum staff 4) [CONFIDENTIAL]

Critical Functions	Recovery Time Objectives
CU*Base user support (clients and WESCO passwords)	< 4 hours
Handle inbound client support calls	< 4 hours
Statement processing	< 24 hours
Support trainers on the road	< 24 hours
File downloads for clients	48 – 72 hours
Client training	72 + hours
Invoicing for billable work done	72 + hours
CU logo and name changes	72 + hours

Notes: [CONFIDENTIAL]

Software Development (minimum staff 1) [CONFIDENTIAL]

Critical Functions	Recovery Time Objectives
Other application support	< 4 hours
CU*BASE support	< 4 hours
Online ATM/Debit/Credit Card vendor switches	< 4 hours
New client conversions (based on conversion date)	< 4 hours
EFT conversions (based on conversion date)	< 4 hours
Technical support and assistance for vendor related file extracts and maintenance, planned and un-planned	< 8 hours
Outside vendor communications	< 8 hours
CU*BASE development	72 + hours
Other application development	72 + hours

Notes: [CONFIDENTIAL]

Network Services (minimum staff 2) [CONFIDENTIAL]

Critical Functions	Recovery Time Objectives
Firewall management – internal	< 4 hours
Manage communication to clients	< 4 hours
Manage communications to third parties	< 4 hours
System backups/recovery	< 4 hours
Execute daily internal run sheets	< 24 hours
Internal system/network maintenance	< 24 hours
Client projects	< 24 hours
Internal projects	< 24 hours

Notes: [CONFIDENTIAL]

Operations (minimum staff 1) [CONFIDENTIAL]

Critical Functions	Recovery Time Objectives
Work w/ Site-Four to make sure they are backing up operations team	< 4 hours
If needed – assist with HA disaster recovery roll	< 4 hours
Support with operations processing (if needed)	< 4 hours

Notes: [CONFIDENTIAL]

Accounting/Bookkeeping (minimum staff 1) [CONFIDENTIAL]

Critical Functions	Recovery Time Objectives
Cash receipts, bank deposits	< 4 hours
Month end processing	< 8 hours
ACH payment processing (weekly)	< 8 hours
Invoicing (daily/weekly/monthly)	< 24 hours
Paying bills (weekly)	< 24 hours
Printing checks (weekly)	< 24 hours

Notes: [CONFIDENTIAL]

Other Department? (Minimum staff 1) [CONFIDENTIAL]

Critical Functions	Recovery Time Objectives
3rd party communications	< 8 hours
Conversion weekend (depends on date)	< 8 hours
Data conversion planning/mapping	< 8 hours
Data conversion testing/verification	< 8 hours
New client communication (email, written, phone)	< 24 hours
New client configuration in CU*BASE	< 24 hours
On-site support (depends on date)	< 24 hours

Notes: [CONFIDENTIAL].

Crisis Communications

In a crisis situation, communication can make or break a complex recovery effort. It is important that internal stakeholders are informed of the situation and know what is expected of them (where to report and when) and that external stakeholders are made aware of the (potential) disruption to business functions and services.

Crisis communications must begin early in the recovery process beginning with notification of recovery teams and continue through the event until business has returned to normal.

Communications to external stakeholders during a crisis situation is best performed by a trained and/or experienced media spokesperson.

With effective crisis communications:

- Employees feel reassured.
- Stakeholders feel confident in the response.
- Media reports are accurate.

Communication in a crisis is all about who, what, when and how.

- Who?
  - Staff (and their families), board of directors, members, vendors, service providers, emergency personnel, media, local/state/federal agencies, etc.
- What?
  - A carefully constructed message that generates confidence and assurance.
- When?
  - Timing and frequency of the message throughout the disruption
- How?
  - Which communications channel to use for each group (email, phone, fax, web, etc.)

Key stakeholders

Circumstances with each crisis scenario will determine who needs to be contacted and when. Stakeholders can be categorized as internal and external, each requiring unique message content.

Key stakeholders include:

- Internal audiences such as
  - Employees, and family members
  - Corporate management
- External audiences such as
  - Credit unions,
  - Vendors,
  - Partners,
  - Regulators
  - Media including
    - Print,
    - TV,
    - Radio,
    - Web
- See “Appendix” for contact information.

To internal stakeholders consider stating:

- Facts about the situation
- The response initiated by management.
- The ways employees can report to their managers.
- Employee assistance programs offered.
- How the event might affect operations over subsequent days

To external stakeholders consider stating:

- Facts about the situation
- What CU*NorthWest is doing to resolve the incident and what each stakeholder can expect as a result of the incident (how it may affect them)
- Expected duration of the event
- Open issues that management continues to investigate.

Communicating in a crisis

All questions from the news media or others regarding the Plan or any disaster should be directed to the Incident Manager or CEO.

Methods of communication include:

- Email (corporate or personal)
- Instant messaging or phone texting
- Corporate web site
- Social media tools such as Facebook, Twitter, LinkedIn, Skype, Zoom, etc.
- Phone (voice)
- Press conference.
- Press release (print)
- Fax

Creating holding statements, which are pre-written statements for use in a variety of crises such as natural disaster, fire, explosion, public health emergency, and workplace violence incident, helps ensure that all relevant information is provided quickly and accurately.

Holding statements should identify the primary audience, the optimal delivery time, suggested method of delivery, as well as who should/should not deliver the message. Also expect and be prepared for follow-up questions.

Key points to remember during and after the incident.

- Remind employees that only media-trained personnel should speak to the media.
- Weigh the desire for information against the need to issue a statement.
- You will not know everything immediately.
- Give them what they need to know in the most appropriate method possible.
- Update the status often, even if there is no material development. This helps those connected feel they are in the loop on key details.
- Keep the information fresh and frequent (minimize waiting time between comments).
- Realize that the media is one of your best resources.

Publishing CU*BASE Alerts

This document outlines the basic steps for requesting an Alert to be published on the client Alerts website.

Procedure for Requesting a CU*BASE Alert (from CU*Answers documentation)

STOP **DO NOT JUST SEND AN EMAIL!!!! You must actually speak to the person on the phone or in person. By the time an email is read, it may be too late to publish an alert!**

CALL OR VISIT the first person on the publishing list below. If they are unavailable, contact the second person, then the third person, and so on. Do NOT contact all of them at the same time or multiple alerts might be published.

Who Can Publish

The following people have the ability to create alerts and are listed in the order in which they should be contacted when an alert is needed.

CU*NorthWest Publishers

	Name	Phone Ext.	Location
	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]

CU*Answers Publishers

	Name	Phone Ext.	Location
	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]

CU*South Publishers

[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]

Special Note about After-Hours (Operations) Alerts

If alerts are needed early in the morning or after normal working hours, then the three names in Operations move up to 1st and 2nd position on the list.

Instructions for Publishers

Rules for Publishing Alerts

Alerts are designed for quick communications about urgent matters, particularly ones that won't live for a long time. Things like **It's Me 247** or CU*TALK being down, a data integrity issue found in the software, errors we are working on right now -- anything with a relatively quick ETA.

If the problem will likely be resolved more quickly than it will take to create the alert (send it out, clients receive their emails and read them, etc.), an Alert may not even be created. That should be a judgment call on the part of the publisher and the programmers or other parties involved.

Need help writing the content of an alert? Contact someone on this list for help:

[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]

Sometimes an actual email would be better:

- If the communication isn't urgent
- If the information will need to be referred to again (such as a schedule of upcoming HA rollovers)
- If the communication is "official" and may need to be communicated to a Board or printed and put into a file (such as a security breach)

In cases like this you can still publish an alert, but also do a normal announcement that can be emailed and posted on the News or other page of the website for later reference.

Library of Common Alerts

Go to the Portal > CU*Answers > Responding to Emergencies and look just below the publisher list for a list of common alerts. Just copy and paste this content into your alert, adjusting it as needed for the particular situation.

Tips for using the Alert Software

The Alerts site is available to all CU*BASE clients via the option on the Net drop-down menu in CU*BASE GOLD. For those authorized to publish, here are some tips:

- [URLs CONFIDENTIAL]

If you have any problems with the software, contact [CONFIDENTIAL] or someone in Web Services.

Sending the Alert Email

After an alert is published, an email must be sent manually to the broadcast email list (email groups are in an Outlook public folder). The only difference between these is the ATTENTION line and the URL, so you can combine them or change them up as needed. **Remember that self-processors sometimes get alerts that online CUs don't and vice versa!** Regarding the Xtend email, you will only send one email, not two, to all online and self-processors (one email because the link is the same – to the Xtend Alerts page).

Refer to the separate "Announcing Something to Clients" document for hints on setting up your Outlook and addressing the email itself to all clients.

→For text you can copy, look below the pictures.

Sample Email to Online Clients

[IMAGE CONFIDENTIAL]

Sample Email to Self-Processors

[IMAGE CONFIDENTIAL]

Choosing the Email Addresses when Sending the Alert Email

[PROCEDURES CONFIDENTIAL]

Threat Assessment

	Corporate Office	
Scenario:	Probability:	Severity:
Environmental:		
Tornado/High Winds	M	H
Flood	L	M
Snowstorm	L	L
Electrical Storm (Lightning)	L	M
Fire	L	H
Excessive Heat	M	M
Ice/Freezing Conditions	L	M
Contamination and Environmental Hazards	L	L
Earthquake	L	M
Organized and / or Deliberate Disruption		
Act of Terrorism	L	M
Act of Sabotage	L	M
Blackmail	L	L
Theft	L	M
Arson	L	H
Bomb Threat	L	M
Loss of Utilities and Services		
Electrical Power Failure	M	H
Loss of Gas Supply (Natural, LP, or Diesel)	L	M
Data/Voice Communication Disruption	L	H
Loss of Water/Sewer Service	L	L
Equipment or System Failure		
Internal Power Failure	L	H
Heating or Cooling Failure (HVAC or CRAC)	L	M
Network Infrastructure	L	H
IT Systems Failure	L	M
Equipment Failure	L	M
Serious Information Security Incidents		
Cyber Crime	M	H
Loss of Vital Records or Data	L	M
Disclosure of Sensitive Information	L	H
Other Emergency Situations		
Workplace Violence	L	M
Employee Safety	L	L
Robbery/Crime	L	M
Public Transportation Disruption	L	L
Neighborhood Hazard	L	L
Health and Safety Regulations	L	L
Mergers, Acquisitions, Conversions	L	L
Negative Publicity (Reputation)	L	M
Scandal/Legal Problems	L	M

Appendix

CU*NorthWest Staff Emergency Contact Information

(Updated as of 01/20/2023) Staff Emergency Contact Numbers			
Please keep a copy accessible at home or on your cell.			
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]

CU*South		HOME	CELL
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]

Board of Directors

Board Member	Credit Union	Contact	Term
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]

Vendors and Service Providers

Vendor Name	Contact	Phone Number	Email Address
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]

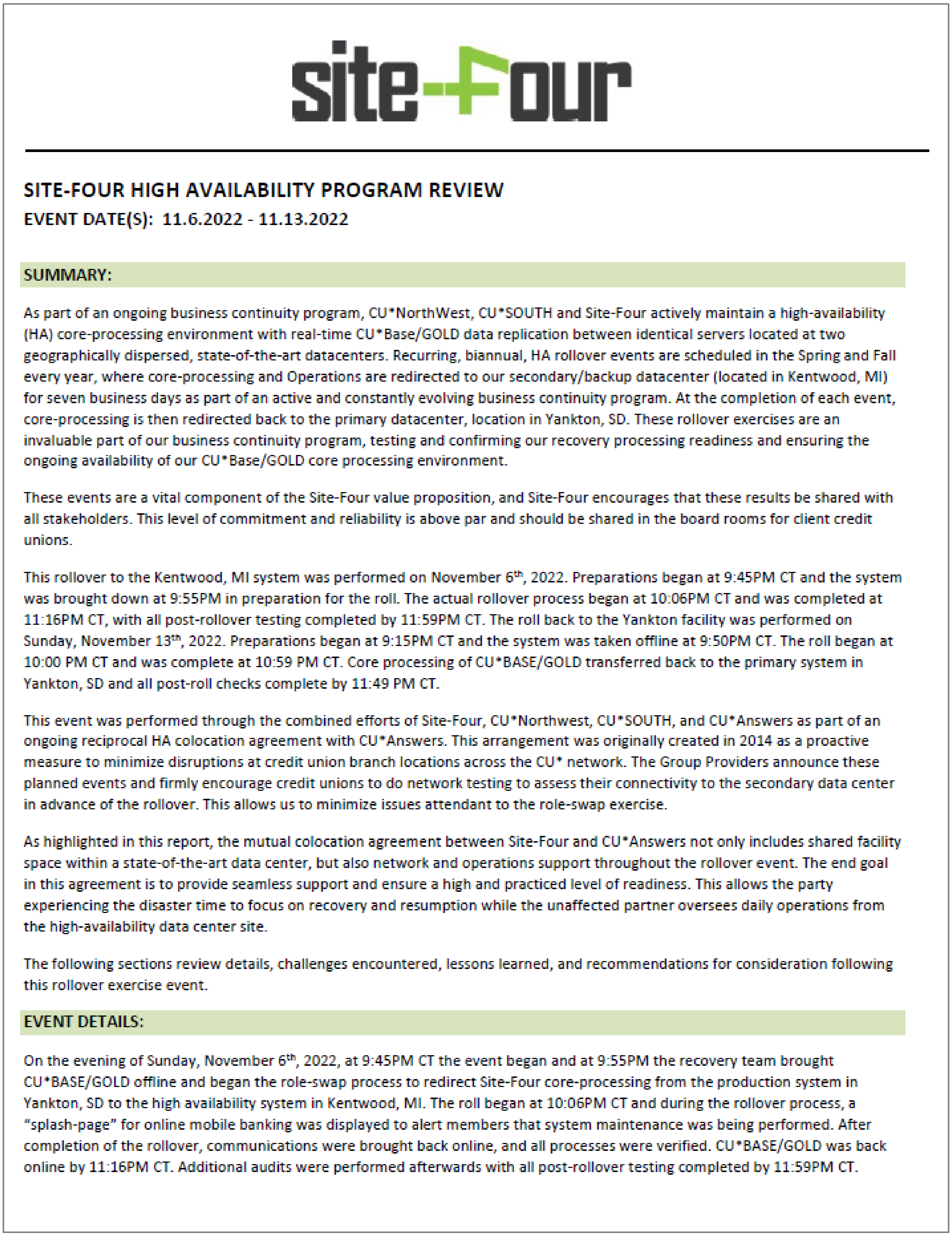
Vendor Name	Contact	Phone Number	Email Address
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
	[CONFIDENTIAL]	[CONFIDENTIAL]	
	[CONFIDENTIAL]	[CONFIDENTIAL]	
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
	[CONFIDENTIAL]	[CONFIDENTIAL]	
	[CONFIDENTIAL]	[CONFIDENTIAL]	
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]
[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]	[CONFIDENTIAL]

Organizational Chart

(As of 1/11/2023)

[CHART CONFIDENTIAL]

Most Recent HA Rollover Results



site-Four

SITE-FOUR HIGH AVAILABILITY PROGRAM REVIEW

EVENT DATE(S): 11.6.2022 - 11.13.2022

SUMMARY:

As part of an ongoing business continuity program, CU*NorthWest, CU*SOUTH and Site-Four actively maintain a high-availability (HA) core-processing environment with real-time CU*Base/GOLD data replication between identical servers located at two geographically dispersed, state-of-the-art datacenters. Recurring, biannual, HA rollover events are scheduled in the Spring and Fall every year, where core-processing and Operations are redirected to our secondary/backup datacenter (located in Kentwood, MI) for seven business days as part of an active and constantly evolving business continuity program. At the completion of each event, core-processing is then redirected back to the primary datacenter, location in Yankton, SD. These rollover exercises are an invaluable part of our business continuity program, testing and confirming our recovery processing readiness and ensuring the ongoing availability of our CU*Base/GOLD core processing environment.

These events are a vital component of the Site-Four value proposition, and Site-Four encourages that these results be shared with all stakeholders. This level of commitment and reliability is above par and should be shared in the board rooms for client credit unions.

This rollover to the Kentwood, MI system was performed on November 6th, 2022. Preparations began at 9:45PM CT and the system was brought down at 9:55PM in preparation for the roll. The actual rollover process began at 10:06PM CT and was completed at 11:16PM CT, with all post-rollover testing completed by 11:59PM CT. The roll back to the Yankton facility was performed on Sunday, November 13th, 2022. Preparations began at 9:15PM CT and the system was taken offline at 9:50PM CT. The roll began at 10:00 PM CT and was complete at 10:59 PM CT. Core processing of CU*BASE/GOLD transferred back to the primary system in Yankton, SD and all post-roll checks complete by 11:49 PM CT.

This event was performed through the combined efforts of Site-Four, CU*Northwest, CU*SOUTH, and CU*Answers as part of an ongoing reciprocal HA colocation agreement with CU*Answers. This arrangement was originally created in 2014 as a proactive measure to minimize disruptions at credit union branch locations across the CU* network. The Group Providers announce these planned events and firmly encourage credit unions to do network testing to assess their connectivity to the secondary data center in advance of the rollover. This allows us to minimize issues attendant to the role-swap exercise.

As highlighted in this report, the mutual colocation agreement between Site-Four and CU*Answers not only includes shared facility space within a state-of-the-art data center, but also network and operations support throughout the rollover event. The end goal in this agreement is to provide seamless support and ensure a high and practiced level of readiness. This allows the party experiencing the disaster time to focus on recovery and resumption while the unaffected partner oversees daily operations from the high-availability data center site.

The following sections review details, challenges encountered, lessons learned, and recommendations for consideration following this rollover exercise event.

EVENT DETAILS:

On the evening of Sunday, November 6th, 2022, at 9:45PM CT the event began and at 9:55PM the recovery team brought CU*BASE/GOLD offline and began the role-swap process to redirect Site-Four core-processing from the production system in Yankton, SD to the high availability system in Kentwood, MI. The roll began at 10:06PM CT and during the rollover process, a "splash-page" for online mobile banking was displayed to alert members that system maintenance was being performed. After completion of the rollover, communications were brought back online, and all processes were verified. CU*BASE/GOLD was back online by 11:16PM CT. Additional audits were performed afterwards with all post-rollover testing completed by 11:59PM CT.

The roll back to the Yankton facility was performed on Sunday, November 13th, 2022. Preparations began at 9:15PM CT and the system was taken offline at 9:50PM CT. The roll began at 10:00 PM CT and was complete at 10:59 PM CT. All processes were verified, communications were established, and CU*BASE/GOLD was back online with all post-roll checks complete by 11:49PM CT.

CHALLENGES:

As we continue to expand and improve our products and services to a growing client network, systems and environments experience an increased number of changes at a very rapid pace. Performing these rollover exercises in a planned, controlled setting during non-peak business hours is a deliberate investment to prepare for an actual crisis. It is the position of Site-Four that any role-swap event which does not reveal any issues is regarded as a missed opportunity to learn and improve.

Immediately following the rollover on 11.6.22, the ISOFISB switch (Transfund) would not come back online. Operations staff had to coordinate with the FIS monitoring center to cycle the FISB switch on both ends to in order to bring this switch online.

On Monday evening, Site-Four began experiencing connection instability between the Yankton, SD and Kentwood Mi facilities. This was causing EFT communications to drop into Stand-In and GOLD sessions to disconnect. Site-Four immediately contacted the ISP and firewall support teams. It was eventually discovered that when the VPN was connected through the SDN Communications ISP, we were getting traffic corruption introduced on the Internet somewhere between CenturyLink in Michigan and the SDN in Yankton. This would cause the VPN to drop and renegotiate the connect, sometimes as often as every 30 minutes. Originally, we saw this as the connection bouncing back and forth between service providers in Yankton so we began the process of isolating the traffic to a single provider to test them individually. This issue was resolved on Wednesday morning when it was determined that locking the VPN to utilize our Midco Communications ISP eliminated the corruption and allowed the connection to stabilize.

Ongoing, residual issues continued as connectivity issues were not conveyed back to the Site-Four staff and assuming the original issue was still causing problems. Once this was discovered, we were able to manually cycle the switches affected and eliminate the ongoing issues.

After coming back up from the roll back on 11.13.22 there were no issues bringing communications back online, but due to DNS caching, the Yankton host was unable to start the DDM Server System. It would not update the IP address of the production host from the DNS servers but continued to pull the outdated data from the DNS cache. This caused the Integrated File System (IFS) to be unavailable. Once it was determined what was happening, the admin team was able to research the solution and bring the server fully online.

During the roll event, a couple of new tools were put to the test. The ISO Monitor which watches the EFT subsystems is being modified to use NETSTAT functionality to further enhance our ability to detect subsystem instability. The newly updated Subsystem Dashboard was also utilized for managing subsystems during the roll. Some issues were encounter, but the cause of these issues were identified and resolved, further improving our ability to streamline the rollover process.

CONTINUING EFFORTS AND RECOMMENDATIONS:

Each recovery test and high-availability rollover exercise provides us the opportunity to improve the process, expand capabilities, and adjust procedures as the production environment changes. The best way to accomplish this is to execute, document, and improve in regular iterations. The best way to be ready for a disaster is to practice.

CU*NorthWest staff assisted on all roll-over processing from start to finish, including making networking changes. Having multiple personnel with hands-on experience performing our roll-over processes provides an additional level of redundancy that furthers our efforts to show continual improvement.

Overall, this was an excellent rollover event despite the issues encountered. These rollover exercises continue to show improvement and validate the work being done to streamline the process. With each scheduled rollover event we perform, we ensure that even an unscheduled incident will run smooth and efficient.

Respectfully,

Alan Rog

Alan Rogers | CEO- Site-Four, LLC
arogers@site-four.com

Procedures for the HA Rollover/Rollback

[PROCEDURES CONFIDENTIAL]