NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA 22314

DATE: **December 2001** **LETTER NO.: 01-CU-21**

TO: **All Federally Insured Credit Unions**

SUBJ: **Disaster Recovery and Business Resumption Contingency Plans**

ENCL: **Appendix 1, Contingency Plan Best Practices**

The purpose of this letter is to provide guidance to credit unions in developing comprehensive, written, updated and tested Disaster Recovery (DRP) and Business Resumption Contingency Plans (BRCP) referred to collectively as "contingency plans." In preparation for the Year 2000, many credit unions developed contingency plans for their critical information systems. Credit unions should review their plans and update them. However, credit unions must go beyond their information systems and develop comprehensive contingency plans for **all** critical resources.

After the tragic events of September 11th, NCUA initiated a review of its own internal contingency plans. Various news sources indicate that financial service providers affected by the terrorist attack, who had tested contingency plans, were up and running, at least at a minimal level, very quickly. As primary financial institutions for millions of members, credit unions must ensure they can rapidly provide a minimally acceptable level of critical member services during a disaster.

Appendix 1 titled, *Contingency Plan Best Practices*, provides high-level guidance for credit unions developing and/or revising their contingency plans.

If you have any questions or concerns, please contact your NCUA Regional Office or State Supervisory Authority.

Sincerely,

/s/
Dennis Dollar
Chairman

Enclosure

Contingency Plan Best Practices

As we have seen from recent events, credit unions can experience a sudden disruption of their operations. The disruption can be minimal, with a power outage for an hour or two, or the building and its contents destroyed through a sudden explosion or fire. The threats can be natural, human, or technical. Credit union's contingency plans should consider a **worst-case scenario**. To be effective, the plans should assume that the credit union could not continue operating at its physical location, due to a natural disaster or some other unforeseen event, for an extended period.

Contingency planning includes the following phases:

1. Establish *Organizational Planning Guidelines*;
2. Complete a *Business Impact Analysis*;
3. Develop detailed *Contingency Plans*;
4. Design a *Validation* method; and
5. *Communicate* the plans.

The remainder of this document provides additional guidance for each phase.

1. Organizational Planning Guidelines

The board of directors and senior management can either develop appropriate contingency plans or designate the task to a work group. In either case, the board and senior management retain the responsibility for the plan's development and approval along with sufficient resources to ensure the plan's success.

Appoint a Work Group

Depending on the credit union's size and complexity, the work group can consist of a single individual or be composed of credit union management and staff, appropriate third party vendors and/or consultants. Work group members should represent all areas of the credit union. Group members should understand that their objective is to initially develop and then ensure updated, viable contingency plans.

Identify Critical Systems and Services

A critical system or service is any internal or external credit union system or service that would have a material negative impact on operations or financial condition. It is important to note that specific critical systems may be components of a number of core business processes and may serve as an interface between and among the operations of core business processes. In identifying criticality, management should consider their membership and member use. For example, if a credit union has a significant number of members that extensively rely on an electronic system, all of the components that constitute this process would likely be critical.

2. Business Impact Analysis

Credit unions must ask themselves, "What system or service would significantly impact the continued operation of this credit union?" "If this system or service were non-operational, how long could we continue to function without it?" Questions such as these and more would assist management in assessing the credit union's business risk. In performing a business impact analysis, credit unions should consider:

- The critical system or service;
- Type of failure events;
- Minimum acceptable service levels or system output;
- The probability of occurrence;
- The probable timing of the occurrence; and
- The cost, duration, and impact of each failure.

Credit unions should prioritize these risks and develop appropriate contingency plans.

It is equally important for a small, one location credit union to evaluate its risk as it is for a large, multi-branch, complex credit union. In the event of a catastrophic event, the small, one-location credit union may take on more risk because it has have fewer financial and human resources available.

Critical System or Service

A critical system or service can be physical (building, roads, parking lot), human (employees, members, consultants) or technical (hardware, software, interfaces, external systems, power sources, telecommunications). The work group should involve department staff to determine critical activities. For example, when determining critical information systems, staff would review the network diagram, a picture of all the internal and external systems and how they interface, and include each process or interface associated with the critical service.

Other possible critical systems could be applications and the associated files stored on an employee's hard drive to document board minutes or reconcile general ledger accounts or bank statements.

Type of Failures

Credit unions can survive interruptions if they evaluate their exposure and prepare for a full range of disasters. Part of the process is to identify events that can impede operations. These include:

Local Events – (your location only)

- Water leaks, fire, robbery, bomb threat, building damage, employee strike, threats against employees, simultaneous temporary or permanent loss of several key employees, vendor failure, computer viruses, sabotage, hardware damage, biological threat

Neighborhood Events – (locations in your immediate area)

- Power outage, communication disruptions, tornado, earthquake, floods, road closure, explosion, striking employees at an adjoining business, chemical spills, protests, riots

Community Events – (the city or approximately a 50-mile radius)

- Hurricane, power outage, earthquake, flood, transportation interruption

Regional Events – (several adjacent cities or approximately a 100-mile radius)

- Hurricane, earthquake, snowstorm, ice storm

Statewide Events – (the entire state or approximately a 250-mile radius)

- Hurricane

Remote Events – (another location)

- You use an online service provider or third party who is affected by a local, neighborhood, community, regional, or statewide event.

Minimum Acceptable Service Levels or System Output

The work group should establish minimum acceptable service levels based on the duration of failure events. Practical categories can include: immediate (one day or less), short-term (one to three days), intermediate (three to ten days), and long-term (greater than ten days). In evaluating minimum levels, credit unions should consider:

- Minimum number of employees required;
- Ability to bring in outside human resources;
- Amount of service or system down time before it will affect membership or reputation;
- Regulatory requirements;
- Affect on other businesses (business checking accounts, line of credit

advances, cash needs, etc.);
- Vendor and outside source list including their address, phone number, and contact person (service bureau, online banking provider, security company, power company, etc.);
- List of current systems and equipment including model number, version and manufacturer with address, phone number, and contact person;
- Other resources - credit union or personal cell phones, pagers, etc.;
- Legal and liability issues;
- Security; and,
- Costs vs. benefits – cost, however, should not be the overriding factor in developing a good plan

Likelihood of Occurrence

Evaluate the likelihood of a specific event occurring. If the credit union operates in a southern state, the likelihood of a snow or ice storm would be remote compared to one that operates in a northern state. The same theory applies to other natural disasters. Location would not factor in for human or technical failures.

Failure Scenarios

Once management determines their critical systems or services, identifies failure events, establishes duration categories, and determines minimum acceptable service levels, management should rank event probability and criticality in developing failure scenarios.

The "Dependency" is the critical system or service; "Event" is the type of disaster; "Duration" is the defined timeframe the critical system would be out of service; "Probability" is the likelihood of occurrence; "Criticality" is how much of an impact the failure would have on credit union operations over the duration period.

"Probability" and "Criticality" are placed on a scale of 1 to 5, with 5 being the most likely event to occur or most critical system and 1 being the least likely to occur or least critical system.

The following table illustrates three scenarios – water supply outage (failure 1 – A to 1 – D), power outage (failure 2 – A to 2 – D), and employees not able to report for work (failure 3 – A to 3 – D). For example, failure scenario 3 considers the same failure event, employees unable to report for work, over four different timeframes, 3 – A, immediate, to 3 – D, long-term. The probability that no employees are available to report for work for more than ten days, failure scenario 3 – D (identified as long-term) is very low (1), while the impact of having no employees for more than ten days would be very high (5).

Failure Scenarios	Dependency	Failure Event	Duration	Prob-ability	Cricti-cality
1 – A	Infrastructure Supplier	Local Water Supply Outage	Immediate	2	2
1 – B	Infrastructure Supplier	Local Water Supply Outage	Short-term	2	3
1 – C	Infrastructure Supplier	Local Water Supply Outage	Intermediate	1	4
1 – D	Infrastructure Supplier	Local Water Supply Outage	Long-term	1	5
2 – A	Infrastructure Supplier	Remote Power Outage – Regional	Immediate	5	3
2 – B	Infrastructure Supplier	Remote Power Outage – Regional	Short-term	4	5
2 – C	Infrastructure Supplier	Remote Power Outage – Regional	Intermediate	3	5
2 – D	Infrastructure Supplier	Remote Power Outage – Regional	Long-term	2	5
3 – A	Employee	Employees Cannot Get to Work	Immediate	3	3
3 – B	Employee	Employees Cannot Get to Work	Short-term	2	4
3 – C	Employee	Employees Cannot Get to Work	Intermediate	1	5
3 – D	Employee	Employees Cannot Get to Work	Long-term	1	5

At this point, senior management should approve of the critical system or service, failures, duration, probability and criticality levels.

Credit unions should realize that they may face simultaneous multiple failure scenarios depending on the disaster. The development of failure scenarios allows credit unions to prioritize and develop appropriately detailed contingency plans. For instance, a failure scenario with a probability and criticality rating of 5 would likely have more resources devoted to developing and implementing related contingency plans than would a failure scenario with a probability and criticality rating of 1.

Credit unions should periodically review the failure scenarios to ensure that probability and criticality ratings are still appropriate given the changing environment and member expectations.

3. Contingency Plans

The credit union is now ready to develop appropriately detailed and prioritized plans for the identified failure scenarios.

Contingency Strategies
Evaluate the options and select the most cost-effective, practical, and appropriate strategy for the size and complexity of the credit union. The primary goal should be to maximize the functionality and speed of recovery and minimize cost.

When considering critical information systems, any credit union that uses an on-line service provider or other third parties should evaluate the adequacy of the provider's contingency plans and ensure the credit union's plans are compatible with the on-line service provider's plans or third party's plans.

Plan Detail
The plans should focus on the impact of the disruption. It should include the steps to take to recover critical activities in the event staff is unavailable, electronic and/or paper information is gone, and the building or other tangible assets are either destroyed or unreachable. Each section should stand alone. The plans should incorporate:

- Approximate cost of implementation in terms of personnel and financial resources;
- Staffing requirements such as replacement personnel, extraordinary staff expenses and safety and health factors; and,
- Sufficient detail so that employees can implement the contingency plans effectively.

The work group would assemble the individual plans to form comprehensive contingency plans. By doing this, as services or systems change, management could easily update the individual plans.

4. Validation

To ensure the contingency plans actually work, a credit union should test the plan at least annually or when a significant change takes place. The test should determine if the credit union could recover to an acceptable level of business within the timeframe stated in the contingency plans. Examples of validation methods include, but are not limited to, simulations, role-play, walk-throughs, and alternate site reviews.

Credit unions can utilize any qualified, independent party, such as an internal auditor, external auditor, consultant, or an employee who was not directly involved in developing the contingency plans. The independent party's responsibilities include:

- Assessing the planning process;
- Reviewing the resulting plans;
- Testing the contingency plans scope and evaluating the test results;
- Determining if management had appropriate follow-up and corrective actions;
- Evaluating the adequacy of management reporting and oversight; and,
- Verifying the credit union's disaster recovery site has the current hardware, software, and environmental systems available.

Management should retain the necessary documentation that includes the scope and type of tests performed and a sufficient audit trail to determine the success of each test with appropriate follow-up.

5. Communication

Contingency plans should outline a program to notify employees, members, business partners, third party vendors, bonding companies, news media, law enforcement, regulators, and other outside parties about the disruption and the impact on operations. Notification can involve television, radio, newspapers, mail or a combination of these.

Notification to NCUA

According to NCUA Rules and Regulations, Part 748 (1) (b), "Each federally-insured credit union will notify the regional director within 5 business days of any catastrophic act that occurs at its office(s)." Part 748 (1) (b) further states documentation requirements. Please refer to the appropriate regulation for full details.

Employees

Since the credit union cannot know in advance which employees will be available during a disaster, it should communicate the plans and the procedures for responding to failure events to all employees. All employees should receive a copy of the plans or, at least those responsible for implementation. In addition, the credit union should store plan copies at a secure back-up location or other site in the event the copies at the primary site are not available.

Operations Manual

Management should have each staff member develop detailed operating instructions. This will assist staff, not familiar with the duties, to continue critical functions. Operating instructions can also help the credit union hire temporary staff not familiar with financial institutions.

Training

Employees should receive annual contingency plan training. Management may wish to simulate a disruption by suddenly changing employee duties to be certain the operations manual provides satisfactory instructions.

Summary

In order to be prepared for a disaster, credit unions must have plans so they know what to do when disaster strikes. This document provides the framework for credit unions to develop detailed contingency plans, test the plans, and communicate them. Each credit union must assess its own risks and develop strategies accordingly.

Credit unions should seek guidance from a wide range of sources when developing the details of their plans, including other credit unions, trade associations, industry periodicals, bonding companies, resources on the Internet, consultants, seminars, etc. There is no time like the present to prepare for the unknown.