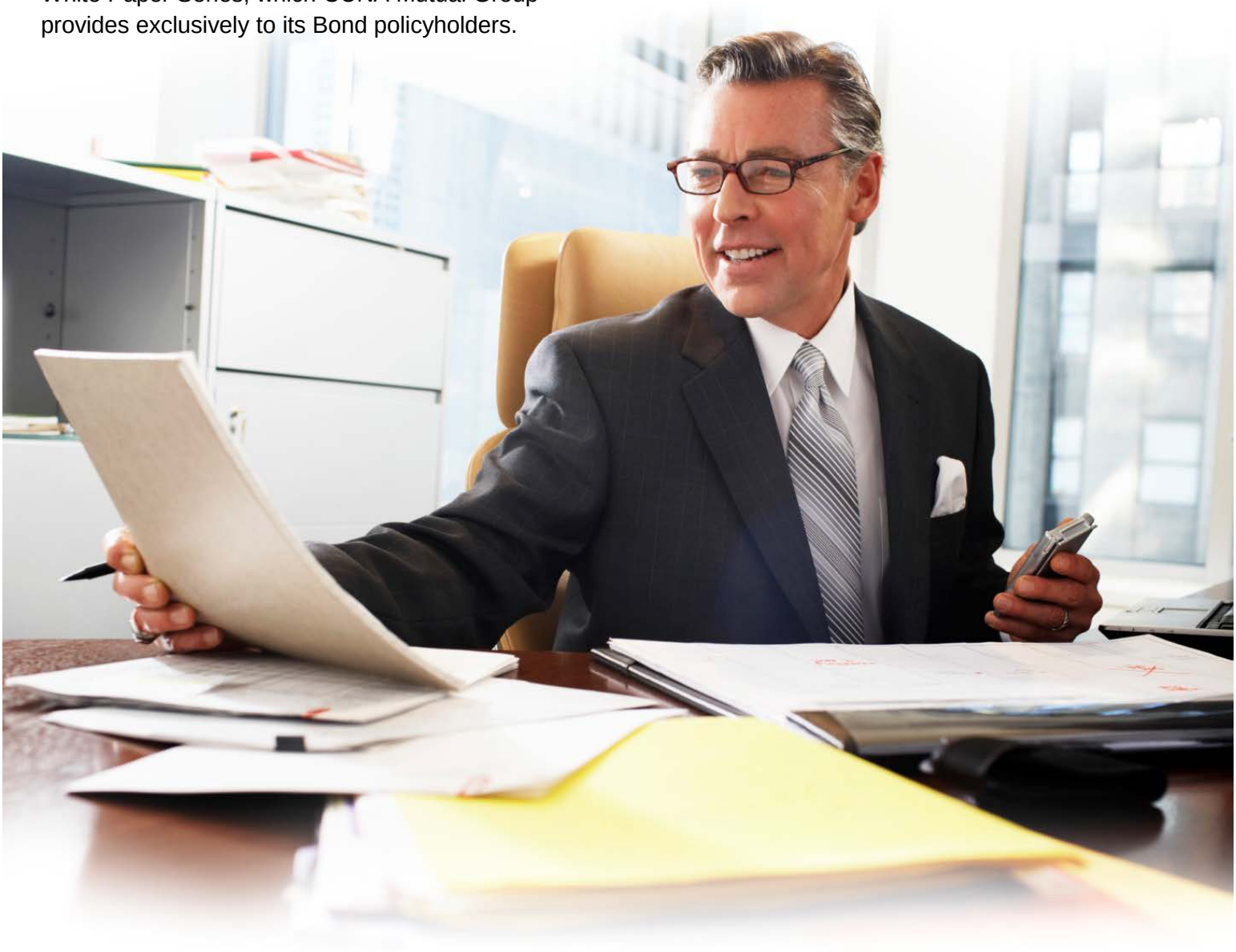
Business Continuity and Disaster Recovery Planning

This white paper is part of the Risk Management White Paper Series, which CUNA Mutual Group provides exclusively to its Bond policyholders.



CUNA MUTUAL GROUP

Table of Contents

Introduction

Business Continuity refers to the activities required to keep your credit union running during a period of displacement or interruption of normal operation. Whereas, Disaster Recovery is the process of rebuilding your credit union's operation or infrastructure after the disaster has passed. It's important to understand the difference in terminology and ensure that your business continuity plan includes a collection of procedures and information which is developed, compiled and maintained in readiness for use in the event of an emergency or a disaster.

Are You Prepared?

A disaster, whether natural or man-made, and although infrequent, may require credit unions to implement their business continuity plans and to improvise creative solutions to address unforeseen difficulties quickly and sometimes, on the fly. Regular reassessment as to how well your credit union is prepared for reasonably foreseeable threats across all levels of the organization and not just from the perspective of recovering the information technology operations is critical to being prepared. Natural disasters such as hurricanes, tornadoes and earthquakes; technological failures such as power outages and brown-outs; and social threats such as riots, strikes and personal acts of violence top the list of threats requiring immediate attention. This paper outlines procedures and guidelines your credit union could follow in developing its own business continuity plan.

How Much Planning and Preparation is Enough?

Oftentimes, disasters cannot be prevented or anticipated, so preparation and practice for them is necessary. Knowing where to go and what critical functions need to be restored can provide confidence to all employees when responding to a disaster. Identifying potential threats, assessing their potential impact, assigning priorities and developing planned responses are the basic principles of sound business continuity planning. Such reviews often categorize threats on a scale from high to low, according to both their probability of occurrence and the severity of the impact each threat could have on the credit union.

The impact rather than the source of the threat should guide the development of the business continuity plan. For example, a threat that presents a low probability of occurrence and a low severity of impact may not warrant further review or major action. However, a threat that could pose a high severity impact generally warrants further consideration regardless of its probability of occurrence.

Reasonable safeguards should be implemented to mitigate the range of risks that realistically may confront your credit union. Developing, implementing and regularly testing business continuity plans to ensure their continued effectiveness for responding to changing business and operational needs takes time, resources and money. Consideration should be given to striking a balance between the threats your credit union faces with the cost-effective measures to mitigate those risks and recognizing areas where it may be either cost-prohibitive or impossible to alleviate your credit union's exposure.

Background

In preparation for the Year 2000 (Y2K), many credit unions developed business contingency plans for their critical information systems. However, in order to continue to offer their member services and the operations that go along to support these services, credit unions should have gone beyond their data information systems and developed comprehensive contingency plans for all critical resources.

Following the tragic events of September 11, 2001, the National Credit Union Administration (NCUA) issued NCUA Letter to Credit Unions #01-CU-21, dealing with Disaster Recovery and Business Resumption Contingency Plans. As an attachment to this Letter was a Contingency Plan Best Practices, which was intended to provide high-level guidance for credit unions developing and/or revising their business contingency plans.

In 2005 and after the Hurricane Katrina had struck the Gulf Coast, the Federal Financial Institutions Examination Council (FFIEC), the member regulatory agencies (including the NCUA) and the Conference of State Bank Supervisors compiled their comments collected from affected financial institutions regarding the lessons they learned from the effects of Hurricane Katrina. These comments were published as part of the FFIEC white paper entitled, "Lessons Learned From Hurricane Katrina: Preparing Your Financial Institution for a Catastrophic Event" and is available at the www.FFIEC.gov website.

In 2006, following the outbreak of avian flu in Asia, the NCUA issued NCUA Letter to Credit Unions #06-CU-06, Influenza Pandemic Preparedness, intending to raise the awareness regarding the threat of a pandemic influenza outbreak and its potential impact on the delivery of critical financial services. Later that same year, the FFIEC issued its "Interagency Statement on Pandemic Planning", which is available at the www.FFIEC.gov website, intending to remind financial institutions that business continuity plans should address the threat of a pandemic influenza outbreak and its potential impact on the delivery of critical financial services.

In 2010, the NCUA issued Letter to Credit Unions #10-CU-10, to urge all federally insured credit unions to perform a review of their business continuity plans in preparation for the 2010 hurricane season and for the ongoing readiness to respond to other similar incidents. This Letter stated that management's plans should be commensurate with the complexity of their credit union's operations. Plans should focus on minimizing interruptions of service to the members and maintaining member confidence in times of emergency. Depending on the nature of the event, the NCUA also encouraged an extra level of credit union assistance to impacted members, such as special loan terms and reduced documentation requirements. Finally, federally insured credit unions were encouraged to periodically review their pandemic preparedness and response plans to ensure they are current and appropriate for the credit union's operation.

Importance of the Plan

Disasters and threats can occur at anytime; therefore, being prepared is highly critical. A business continuity plan is necessary to minimize disruption of the business. Business continuity planning is a more complex approach to making sure credit union operations continue, not only after a natural calamity but also in the event of smaller disruptions including illness or departure of key employees, vendor problems or other challenges credit unions face from time to time.

Without a business continuity plan, the credit union might face a reduced chance of delivering its critical financial services to its members on a continued basis. This inability to provide these critical services could also put the credit union's ability to operate as a viable financial entity at severe risk and possibly, eventually put it out of business.

Responsibility for the Plan

Primary responsibility for creating the credit union's business continuity plan lies with the credit union's board of directors. Working with management, the board should ensure that a comprehensive plan is in place and that it is tested, reviewed, updated and approved at least annually. The board should also record each review in the board's meeting minutes.

Credit unions that use service bureaus or other vendor arrangements to handle their business continuity needs should also evaluate the vendor's business continuity plan to ensure that the adequacy and compatibility of that plan with that of the credit union's plan. Such evaluations should be completed regularly and reported to the credit union's board of directors and recorded in the board's meeting minutes.

Plan Components

Since the business continuity plan contains confidential information, the document should be labeled "confidential" in bold type at the beginning of the plan to emphasize that the plan is strictly confidential. When training employees, emphasize that the plan is confidential and should not be discussed with family and friends or anyone outside of the credit union.

Business continuity planning should include the following planning phases:

- Establish Organizational Planning Guidelines – Appoint a work group and identify critical systems and services.
- Complete a Business Impact Analysis – Consider each critical system or service, the types of failure events that could occur, the minimum acceptable service levels or system output desired, the probability of occurrence, the probable timing of the occurrence and the cost, duration and impact of each failure.
- Develop Detailed Contingency Plans – Develop appropriately detailed and prioritized plans for the identified failure scenarios.
- Design a Validation Method – The methods selected should determine if the credit union could recover to an acceptable level of business within the timeframe indicated in the contingency plans.
- Communicate the Plans – 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.
- Testing – Develop a systematic testing plan to be utilized throughout the year. Consistent testing will ensure the plan is working well and that all employees, tenured and new, are aware of their roles and responsibilities.

The remainder of this document provides additional guidance for each key element of the plan.

Key Elements of the Plan

The following key elements should be considered with all business continuity plans:

- **P**lanning – Ensuring Financial Services to Members.
- **R**esources – Allocation of Equipment, Facilities and Supplies.
- **E**valuation – Testing of Contingencies for All Critical Systems.
- **P**eople – Maintaining Readiness of Staff and Officials.
- **A**lliances – Establishing Relationships with Other Organizations.
- **R**eview – Updating Internal Plans for Effectiveness.
- **E**xperience – Incorporate Lessons Learned from Others.

Planning – Ensuring Financial Services to Members

The ultimate goal of the plan is to ensure continued financial services to the credit union members. To accomplish that goal, several key elements need to be included in the business continuity plan.

Business continuity planning can take many forms. It is preparing for disasters and other threats that require credit union officials to implement contingencies to ensure uninterrupted services to their members. These plans are often labeled "business continuity" or "disaster recovery." It is important that this type of planning involves the institution as a whole and focuses on providing vital financial services to the members as its primary goal.

Schedule testing, followed by updates to the plan, at least on an annual basis to ensure the plan is updated and readily available to everyone involved in the process. Work papers to support the testing work that was performed should be maintained and archived. These work papers should include copies of the test scenarios and results obtained. The FFIEC IT Handbook - Business Continuity Planning contains helpful information on risk monitoring and testing. This handbook is available at the www.FFIEC.gov website.

Participation in planning and testing by the board of directors reinforces that the plan is deserving of a high priority. Any discussions about the plan or the planning process should be documented in the board's meeting minutes. Although support for this plan begins at the top of the organization, support throughout the organization is necessary for this plan to succeed.

Identify threats to delivering financial services helps plan for the unexpected. Critical systems and their role in providing vital financial services must be identified to ensure continued financial services to the members. The credit union should focus their planning on threats that are most likely to affect their operations. Examples of such threats are fires, flooding, hurricanes, tornadoes, sabotage, riots, nuclear attacks, power failures, fraud, theft, equipment failures, pandemics and others.

Some credit unions will find their most likely threats are small in scope, but still have a high probability of causing service disruptions. For example, computer malfunctions, temporary telecommunication interruptions, delayed coin and currency deliveries or ATM malfunctions are some examples of these threats.

There are different methods of determining which systems are critical, such as performing a business impact analysis or a flow chart diagram to determine which elements are needed to ensure vital financial services can be provided to the members. Regardless of the method used to determine which systems are critical, there is a direct link between critical systems and providing vital financial services to the members. Once the critical systems are selected, they should be further prioritized to ensure systems are restored in the sequence of greatest priority and to address any interdependencies among them. The plan should contain a timeline for the restoration of critical systems. This will ensure systems are restored in priority order and perhaps, on schedule.

Communication efforts should begin with the members, staff, officials and regulators to ensure readiness. Be sure to include multiple forms of communication between key employees, vendors, leagues, corporate credit unions, news media, the NCUA and/or the state regulators. Various methods for disseminating information to the members must be established to ensure every member gets the message on how to reach the credit union. Specifically for key and secondary employees, establish guidelines for evacuation and/or shelter in place. Member communication needs to play a major role for dealing with threatening situations. Plans should include communicating with the members through a variety of sources such as internet postings, radio, newspapers, newsletters, lobby handouts and signs displayed at each office location.

A significant lesson learned from previous disasters is that focusing on communication is key to successfully preparing for and operating in disaster conditions. Business continuity plans need to give communication a high priority to ensure member confidence and service levels are maintained.

Business continuity plans should also recognize the role of outside parties, such as vendors, leagues and regulators in working through a threat or disaster. Ideally, within the first 24 hours following a threat or disaster, all significant outside parties should be contacted, including the NCUA and/or the state regulators.

Pre-event preparations should be established, such as supplies at a safe location, as well as data back-ups with accessibility plans from a safe location. The plan should address "shelter-in-place" or evacuation routines which are appropriate, based on the various types of threats or disasters that could be facing the credit union.

If advance notice is available concerning the possibility of a threat or disaster, the plan needs to be activated early on. Time before the disaster can be utilized to ensure alternate systems are ready, facilities secure and staff is adequately prepared. Taking steps such as covering equipment and files or moving critical equipment to safety can greatly improve the expected recovery time following these events.

NCUA Rules and Regulations Section 749 (3) requires a credit union to establish a vital records center to store back-ups of vital records at locations far enough away from the credit union's main offices to avoid the simultaneous loss of both sets of records in the event of a threat or disaster. The plan should reflect this requirement and the credit union's experience in their local area to identify a place to store back-up records.

Social Media

Just some quick facts—According to a study by the Red Cross, 76% of respondents said they have used social media to determine whether or not a loved one was safe after a disaster, and an additional 25% had gone on to download a disaster-related app. 24% of respondents had actually been in a disaster and had used social media to let loved ones know they were safe.

What this tells you is—whether or not you're using social media to communicate during a crisis, your audience is looking to the speed and convenience of social media updates to get the most current information in times of disaster. If you're not there, you could run the risk of being irrelevant.

The audience is there—the culture and regular behavior pattern to use social medial is there… but it is critical to have your audience already connected to you BEFORE you use these channels to communicate important details related to any disaster, or you will be speaking but no one will be hearing you.

Think about not just members, but are your employees connected? Do you want them to be? If you plan to use social media to communicate necessary info in a disaster situation, then you will.

Establishing your audience is something you will want to have part of your regular communications strategy in the midst of a disaster.

As far as sharing info—share what you know, what you can verify is true, and if you don't have much info, let people know it's your priority to find that info and get back to you on it. Give approximate timeframe for when you expect more info and give an update at that time whether you have the info, or need to tell them you still are finding things out but don't leave them hanging.

Be prepared that if you open this line of two-way communication at all, you will have to have the time/resources to respond to and answer questions, post updates and resolutions/conclusions. It's worse to start using social media channels and abandon it after just one or two posts with no follow-up, than to not use it at all. Not every CU has the capacity to use it, and if your audience isn't there yet, there's little benefit in using it. Make sure your employees know your social media policy in advance of any disasters occurring, so in that time, they will know what they can or can't do or say on behalf of the Credit Union.

Lastly, BE CONSISTENT! Not only with yourself and what other information is coming from non-social media channels, but also other news sources. Keep a pulse on what's happening holistically and not just at your organization if it's a larger situation. Also, be

sure you understand the impact of what you're communicating about. It might not be the best channel to communicate about something such as a data breach or hack if it only impacts a handful of people. In that situation, follow up directly with those impacted and don't worry those who wouldn't otherwise be affected. Communicating via social media can do more damage than good in some situations.

Social Media Checklist:

- Integrate social media into your disaster crisis communications plan but don't forget about other communication channels.
- Assemble a team that understands each social media platform.
- Practice using social media before you need it in a crisis.
- Consider all audiences: employees; volunteers; clients, partners/vendors; community; and media.
- Work in advance – establish connections with people, groups, local and national organizations to share information.
- Monitor social media, keywords and #hashtags.
- Collect intelligence, link to others, and share insights.
- Be brief, pertinent, consistent, and timely.
- Set the cadence of your timeline and frequency of posts.

Resources – Allocation of Sufficient Equipment, Facilities and Supplies

Resources play an important part in being able to deliver financial services to the credit union's members. The credit union should make arrangements to have sufficient equipment, facilities and supplies to work through a threat or disaster. These resources can range from small items, such as back-up power supplies, to alternate operating locations. Establishing a safe location such as an alternate facility and stocking it with the proper equipment and supplies can greatly reduce the stress of any type of threat or disaster. Include a checklist of supplies that would be needed at the alternate facilities within the plan.

Resources should take into account all critical systems needed to provide vital financial services to the members. Critical systems can be hardware, software and items needed for manual procedures. Examples range from hardcopy checks to computer servers. A list of critical systems and a list of emergency contact names and phone numbers for vendors/suppliers should be maintained in the plan, as well as at the alternate facility location.

What if the alternate facility location is unavailable, does the plan include a back-up site, just in case? This information should be included in the plan as well as at the back-up facility to your alternate safe location and how problems will be resolved.

Agreements should be in place with provisions for anytime access to the alternate location(s) is needed. The alternate worksite(s) should have back-up copies of data processing information, the business continuity plan and hard copies of communication information for key staff and external parties.

Plans requiring hot sites or alternate back up facilities for resuming operations do not account for demands on the backup providers that would overwhelm their ability to meet their contractual obligations. Contracts for use of back facilities typically assumed

a need of relatively short duration, not an event that would displace clients for months. Plans assumed that electronic backup files would provide the information necessary to resume operations quickly, but many credit unions discover they were more dependent on paper than they realized, and document reconstruction became an additional task.

It's important to understand how prepared your partners, key service providers, and vendors are. Can they withstand the impact? Information outsourcing and transaction processing involve operational risks similar to those that arise when those functions are performed internally. These risks include threats to the availability of systems used to support transactions, threats to the integrity of member information security and threats to the integrity of risk management systems.

The off-site location should be a reasonable distance away to insure protection of the back-up data. Having multiple sites permits a greater probability that a back-up site will be available in different threat or disaster scenarios.

The plan should provide a reliable means for meeting the emergency withdrawal needs of its members. If applicable, the plan should specify off-line limits for ATMs and debit cards. The plan should include the necessary steps to activate these off-line limits.

The plan should contain essential information needed to submit insurance policy claims. Also, it should include contact information for the insurance companies' business continuity teams.

Another resource often overlooked is adequate insurance coverage. An annual review of your insurance policies should be included as part of your business continuity plan.

Evaluation – Testing of Contingencies for All Critical Systems

Business continuity plans should be tested at least annually. This regular testing will help ensure the plan adequately addresses all essential functions. Evaluation and testing of the business continuity plan includes various phases of testing. Table-top testing can be effective for an overall review of the plan. Practical testing which includes going off-site and working for a full day from the alternate location is critical to include in the plan to ensure the location is ready at a moment's notice. Practical testing should be conducted annually. Document the date of the test and include an after-testing report that indicates what worked well, what didn't work well and what areas could be improved.

Agreements and/or leases for alternate locations should also be evaluated and reviewed annually. Communication testing with key employees, vendors, leagues, corporate credit unions, news media, the NCUA and/or the state regulators should be conducted annually. All test results should be integrated into the updated business continuity plan, which should then be reviewed and approved by the board of directors and documented in the board's meeting minutes.

The test should be documented and workpapers maintained, demonstrating that all critical functions and areas were tested.

Disaster drills should be created that realistically address threats to the credit union and involve staff members from a cross-section of the organization. In the event that a third party is used to perform or facilitate these tests, they must be knowledgeable in the credit union's critical functions and disaster response goals.

Shared service branches should be advised of your plan and included in the testing. They need to be prepared on how to handle the increased traffic and transactions in the event of a threat or disaster.

The credit union should ensure their vendor agreements keep pace with changes in the credit union's asset size, complexity of services and membership levels.

Vendor agreements should be evaluated and tested annually to ensure they can provide the resources, services and/or supplies needed to provide financial services to the members.

Disaster support agreements with vendors that provide services to minimize damage, such as the placement of sand bags, boarding up of windows, fuel for generators and restoration after the disaster has passed, should be considered.

The plan should contain emergency contact information for all disaster support vendors and include alternate sources for the critical services.

Evaluations should include review of back-up sites for readiness. These sites should have working equipment and should be stocked with supplies as specified within the plan.

The test should include using all of the various means of communication to ensure there are no technical problems or additional necessary training requirements.

The credit union should prepare a template or script for this type of communication in advance and have established contacts for disseminating important information.

Testing may include periodic contacts with the various media outlets to ensure contacts remain valid and procedures for sharing information are accurate.

After completing a test of the plan, the credit union should update it to correct for any shortfalls.

For many business continuity practitioners, one of the most challenging assignments is the development of realistic but stimulating test exercises that prove a suitable plot line that can be adapted and embellished for your operations. The delivery of, and the feedback from, any test exercise is one of the most interesting and valuable parts of any disaster plan. Again, good solid preparation can ensure a sound delivery and help ensure that everyone benefits from the testing exercise.

People – Maintaining Readiness of Staff and Officials

The plan should specifically state the succession of authority and establish clear responsibilities for all parties involved, as well as key people to initiate the plan, direct others in implementation and lead communications throughout the threat or disaster. To avoid confusion in the face of a threat or disaster, this list provides information about who is responsible for what activities or actions.

Key people should each have a copy of the plan and know the procedures to notify employees that the plan has been activated and when it is deactivated. A chart of emergency contact information (e.g., cell phone, home phone and contact numbers) for all employees and officials should be included.

The plan should specify who is granted the authority to declare an emergency and have the ability to invoke the plan. This person may be the CEO, Board Chairman or another key person, such as a branch manager. It should also contain the steps necessary for the specified individual to initiate and terminate emergency status. An alternate should be appointed for this position and be prepared to act as the primary contact, if needed.

A key employee should be designated to communicate with external sources, such as the media or any outside agency.

All officials and staff members should be involved in the process. The special skills of each individual should be inventoried to ensure coverage for all critical functions. Duties should be clearly defined for all personnel involved. Each person should have primary and secondary responsibilities.

The plan should take into account that, during a disaster, various staff members may need to attend to their personal situations and may not be available for work.

Depending on the size of the credit union, it may be feasible to establish a Disaster Recovery Team (DRT). The team would be made up of key people who have the management and technical skills to implement the business continuity plan. An effective DRT includes people who represent a cross-section of the organization to ensure all areas are represented and covered.

The DRT needs to have a primary meeting place location in case of a threat or disaster. There also needs to be a listing of alternate assembly sites, in case the primary site is not accessible.

Awareness by officials and staff is an important element of success. Quick reference information, such as wallet cards, can serve to supplement periodic training.

Alliances – Establishing Relationships with Other Organizations

Essential alliances are outside entities that can aid in the operations during a time of emergency. For example, vendors, trade groups and regulators are key alliances to include in the business continuity plan to ensure there is agreement when disaster strikes. The credit union should have established relationships with other credit unions and/or key vendors with enough geographic separation to help ensure the same threat or disaster will not affect the credit union and its alliances. Examples of an alliance that some credit unions use to reduce the likelihood of disruptions in member service are shared service center agreements.

Current business partners and alliances must have the credit union’s emergency contact information and vice versa. Applicable portions of the plan should be shared with the business alliances to ensure that they are aware of the credit union's operating strategy.

Ensure that key vendors understand the credit union's needs in the event of an emergency and are able to meet the expected demand. The plan should have a listing of all major vendors, emergency contact information and secondary sources for critical products and services.

To the extent possible, the credit union needs to involve its major vendors in testing or walk-throughs of the plan to ensure their plans are practical and functional.

Review – Updating Internal Plans for Effectiveness

The business continuity plan is a living document and should be reviewed periodically for any necessary updates and changes. As new procedures, software, etc. are implemented, consider how these changes might affect the business continuity plan.

Post-incident response reviews should be performed after the credit union has been affected by a threat, disaster or service disruption. What worked well, what didn't work and what changes or improvements are needed? Deficiencies found during testing and causes for the service disruption should be documented and appropriate changes made to the plan.

These reviews are valuable learning experiences that could be the difference between one hour without services to the members or twenty-four hours or longer without these same services.

Experience – Incorporate Lessons Learned from Others

Experience is the best teacher. Learn from other credit unions and other financial institutions. Chapter and League meetings are great places to network and learn from others. Learning from the credit union's vendors is also valuable source of information. Ask for a copy of their business continuity plan and implement some of the best practices utilized by these vendors that may be appropriate to your plan. There have been many lessons learned from the major threats or disasters that have affected other credit unions and other financial institutions. Sharing ideas for disaster preparedness will lend itself to discovering items that may not have been initially considered by the credit union.

Pandemic Planning

Pandemic planning presents unique challenges to credit unions unlike most natural or technical disasters and malicious acts. The impact of a pandemic event is much more difficult to determine because of the potential difference in the scale and duration of a pandemic event. As a result of these differences, credit unions need to plan for the potential adverse effects of a pandemic event. Experts believe the most significant challenge may be the severe staffing shortages that are likely to result from a pandemic outbreak.

To assist in credit unions' pandemic planning efforts, the NCUA and other Federal Financial Institutions Examination Council (FFIEC) member agencies have developed the pandemic planning guidance section which was incorporated into the FFIEC Information Technology Handbook – Business Continuity Planning. This handbook is available at the www.FFIEC.gov website.

The guidance section addresses the need for credit unions to establish plans to manage a pandemic event. Therefore, the business continuity plan should include:

- A preventative program to reduce the likelihood the operations will be significantly affected by a pandemic event.
- A documented strategy which provides for scaling pandemic efforts.
- A comprehensive framework of facilities, systems or procedures to continue critical operations if a large number of staff are unavailable for prolonged periods of time.

- A testing program to ensure the pandemic planning practices and capabilities are effective.
- An oversight program to ensure ongoing review and updates are made to the pandemic plan.

Appendix B to the NCUA Regulation Part 749 indicates that the credit union's written plan should address the annual testing of this plan and to revise the plan as circumstances warrant. In March 2006, the NCUA issued the Letter to Credit Unions #06-CU-06, addressing Influenza Pandemic Preparedness. The purpose of this Letter was to raise the awareness of credit unions regarding the threat of a pandemic influenza outbreak and its potential impact on the delivery of critical financial services. In this Letter, the NCUA outlines the responsibilities of the U.S. private sector and critical infrastructure entities to include the following:

- Establish an ethic of infection control in the workplace that is reinforced during the annual influenza season, to include, if possible, options for working offsite while ill and systems to reduce infection transmission and worker education.
- Establish contingency systems to maintain delivery of essential goods and services during times of significant and sustained worker absenteeism.
- Where possible, establish mechanisms to allow workers to provide services from home, if public health officials advise against non-essential travel outside the home.
- Establish partnerships with other members of the sector to provide mutual support and maintenance of essential services during a pandemic event.

Credit unions and their service providers should review the National Strategy for Pandemic Influenza to consider what actions may be appropriate for their particular situation and whether such actions should be included in their event response and contingency strategies. A copy of the National Strategy for Pandemic Influenza is available at the www.FEMA.gov website.

Key points to consider. Does the pandemic plan address all of the following:

- A preventative program to reduce the likelihood the operations will be significantly affected by a pandemic event?
- A documented strategy which provides for scaling pandemic events, including provisions for a possible second and third wave of a pandemic?
- A comprehensive listing of facilities, systems or procedures to continue critical operations, if a large number of staff is unavailable for prolonged periods of time?
- A testing program to ensure the pandemic planning practices and capabilities are effective?
- An evaluation of critical service provider plans for operating during a pandemic?
- An oversight program to ensure ongoing review and updates are made to the pandemic plan?

Hurricane Planning

In June 2006, the NCUA issued its Letter to Credit Unions #06-CU-11, Interagency Guidance Lessons Learned By Institutions Affected By Hurricane Katrina, with a copy of the FFIEC whitepaper entitled "Lessons Learned From Hurricane Katrina: Preparing Your Institution for a Catastrophic Event". This Letter underscores the importance in which the NCUA placed in having a viable hurricane emergency plan in place at the time. This point was re-emphasized over time in other Letters issued, specifically the NCUA Letters to Credit Unions #07-CU-02, Interagency Reminder of Supervisory Guidance for Financial Institutions Affected by Hurricane Katrina, #09-CU-13, Hurricane Preparedness and Pandemic Planning and #10-CU-10, Resources for Hurricane, Disaster, Emergency and Pandemic Planning and Preparedness.

The 2006 FFIEC whitepaper entitled "Lessons Learned from Hurricane Katrina: Preparing Your Institution for a Catastrophic Event" provides certain specific details, lessons learned and recommendations to address as part of a financial institution's hurricane planning. Numerous related references were also provided as part of this whitepaper. This whitepaper is available at the www.FFIEC.gov website.

This whitepaper recommends that the hurricane portion of the business continuity plan should address the following:

- A preventative program to reduce the likelihood the operations will be significantly affected by a hurricane event.
- Does this program include disaster drills, their frequency and who should participate in these drills?
- Does this program address alternate methods of communication with employees and members after a hurricane?
- Does this program address prolonged disruptions in the mail or other delivery services and possible delivery alternatives after a hurricane?
- Does this program address primary and alternative gathering or work places for employees after a hurricane?
- Does this program address alternate transportation methods for employees after a hurricane?
- Does this program address the needs of employees and their family members to basic essential services, such as food, medical services and child care after a hurricane?
- Does this program address the credit union's access to replenish its supplies to continue operations after a hurricane?
- Does this program address sources of back-up power?
- Does this program address the possible processing of manual transactions and the need for large amounts of available cash?
- Does this program address communication with local, state and federal authorities and media that could provide assistance after a hurricane?

Insurance Review

Business continuity planning can help reduce your exposure to loss. Insurance is a vital part of this plan. Property coverages should be in place for all buildings, business personal property, extra expense and data processing equipment.

Have you reviewed or updated at least the following coverages with your insurer in the last 12 months:

- Building replacement cost?
- Data processing equipment coverage?
- Data processing extra expense coverage?
- Business personal property coverage?
- Extra expense coverage?
- Valuable information coverage?
- Flood insurance? (If applicable)
- Earthquake coverage? (If applicable)

One of the six techniques of risk control is to transfer the risk of an emergency event to another party. Insurance is one example of a risk transfer tool available to a credit union. It's recommended that the appropriate insurance coverages that could be affected in the event of a credit union disaster be reviewed at least annually by either management and/or the credit union's Board of Directors. This review should be documented in the Board's meeting minutes.

The coverage most often under-estimated is extra expense. Forgotten extra expenses include relocating telephones, terminals and workstations, renting space for storage and record reconstruction; or the cost of finding, renting, shipping and setting up portable generators, toilets and fresh water supplies at the disaster site.

Appendix B to the NCUA Regulation Part 749 indicates that the credit union's written business continuity plan address the annual testing of this plan and to revise the plan as circumstances warrant. This review and testing of the plan elements certainly applies to and should include a review of the appropriate insurance coverages.

Business continuity planning can help to minimize your credit union's losses in the event of a threat or disaster, but this planning can't guarantee that a loss won't occur. Insurance is a vital part of any business continuity program. Basic coverages should include property coverage on buildings, business personal property coverage and extra expense and EDP coverage that includes data processing equipment, media and extra expense coverages.

It's important to keep an up-to-date inventory of all credit union assets that reflects replacement costs. This asset inventory not only helps ensure that your credit union has adequate insurance limits in force, but also helps determine losses in the event a threat or disaster occurs.

Your credit union may not be able to predict or avoid a disaster, but a carefully prepared and tested business continuity plan, along with adequate insurance will make the recovery process easier and more effective.

At least annually, review the complete package of insurance coverages with your CUNA Mutual Sales Executive. This review will help determine your credit union's exposure to loss, identify any gaps in coverage and guide you in choosing the most appropriate coverages and limits for your credit union.

Management's Role in the Planning Process

The primary responsibility for creating and maintaining a business continuity plan lies with the credit union's board of directors. Working with management, the board should ensure that a comprehensive business continuity plan is in place and that it is tested, reviewed, updated and approved at least annually, with each review and approval recorded in the board's meeting minutes.

Credit unions that use service bureaus as part of their major operations should also evaluate the service bureaus' continuity plans to ensure the adequacy and compatibility of the bureaus' plans with the credit union's plan. Such evaluations should be reported to the credit union's board of directors and noted in the board's meeting minutes.

Involving the board of directors in business continuity planning sets the tone from the top that this planning is important. Reviews and participation in the testing by the board helps to reinforce their support and ensure that the plans won't be forgotten and fall in disuse.

References

1.) Federal Emergency Management Agency, www.FEMA.gov website. a.) Search for "National Strategy for Pandemic Influenza". b.) Search for "National Disaster Recovery Framework".

2.) Federal Financial Institutions Examination Council, www.FFIEC.gov website. a.) Search for "IT Examination Handbook", then Business Continuity Planning. b.) Search for "Interagency Statement on Pandemic Planning". c.) Search for "Lessons Learned From Hurricane Katrina".

3.) National Credit Union Administration, www.NCUA.gov website. Search for "Rules and Regulations", and then locate Section 749.3.

4.) National Credit Union Administration, Letter to Credit Unions No. 01-CU-21, "Disaster Recovery and Business Resumption Contingency Plans". This Letter contains the Contingency Plan Best Practices.

5.) National Credit Union Administration, Letter to Credit Unions No. 06-CU-06, "Influenza Pandemic Preparedness".

6.) National Credit Union Administration, Letter to Credit Unions No. 06-CU-11, "Interagency Guidance Lessons Learned By Institutions Affected By Hurricane Katrina".

7.) National Credit Union Administration, Letter to Credit Unions No. 06-CU-12, "Disaster Preparedness and Response Examination Procedures". The link to the AIRES Disaster Preparedness and Response Questionnaire is in this Letter.

8.) National Credit Union Administration, Letter to Credit Unions No. 07-CU-02, "Interagency Reminder of Supervisory Guidance for Financial Institutions Affected by Hurricane Katrina".

9.) National Credit Union Administration, Letter to Credit Unions No. 08-CU-01, "Guidance on Pandemic Planning".
10.) National Credit Union Administration, Letter to Credit Unions No. 09-CU-13, "Hurricane Preparedness and Pandemic Planning".
11.) National Credit Union Administration, Letter to Credit Unions No. 10-CU-10, "Resources for Hurricane, Disaster, Emergency and Pandemic Planning and Preparedness"