Chapter 307

CONTINGENCY PLANNING

Introduction

Corporate credit unions (corporates) have an integral role within the credit union community, serving as a depository for a large portion of credit unions' excess liquidity, and providing numerous correspondent services. A disruption in a corporate's operations for an extended period of time could be disastrous, not only for the corporate, but also its members. Thus, it is imperative contingency plans be developed detailing the alternative site(s) available in the event of service disruptions.

The primary objective in reviewing the contingency plan is to determine it adequately documents management's plans and its implementation has been demonstrated. Contingency plans and arrangements will vary among corporates, as a function of size, complexity, and a multitude of other variables.

Corporate Contingency Planning

The corporate's business continuity planning (BCP) process should reflect the following objectives:

- BCP is about maintaining, resuming, and recovering the business, not just recovery of the technology.
- The planning process should be conducted on an organizational basis.
- A thorough business impact analysis (BIA) and risk assessment is the foundation of an effective BCP.
- The effectiveness of a BCP can only be validated through testing or practical application.
- The BCP and test results should be subjected to an independent audit and reviewed by the board of directors.
- A BCP should be periodically updated to reflect and respond to changes in the financial institution or its service provider(s).

Written Disaster Recovery Plan

The corporate must have a comprehensive written disaster recovery plan. The plan must outline the specific courses of action management and staff will take following an occurrence which interrupts its ability to provide member services. Although it is impossible to anticipate every scenario, an adequate plan will address disruptions of varying severity and duration. The plan should address all critical services and operations provided by both internal departments and external sources. The plan must be a coordinated effort to minimize service disruptions to members, minimize financial losses, and ensure a timely resumption of operations in the event of a disaster.

To develop a reasonable and appropriate plan, management must perform a BIA to determine the criticality of each product or process and a risk assessment to evaluate risk scenarios. This will include a review of each department to assess their criticality in providing member services and their dependence on outside parties for continued performance. Plans must be developed to restore critical operational areas and service affected by a disaster.

The board of directors should review and approve the disaster recovery plan annually. Additionally, the board should be apprised of the scope, frequency, and results of contingency testing. The board should also ensure they are satisfied operating management implemented appropriate corrective action for significant contingency testing concerns.

During short-term disruptions, generally lasting less than one day, it may not be necessary for the corporate to relocate its operations. However, the plan should outline steps to be taken during such situations to ensure timely processing and transaction settlement. The plan must address and prioritize each "critical" operation within the corporate.

For disruptions exceeding one day, the plan needs to provide detailed relocation procedures for the corporate's operations. It would be preferable if the corporate has a dedicated facility which is readily equipped for the corporate to immediately use when a disaster occurs. (See further discussion in the section entitled Disaster Recovery Sites.)

A contingency job description should be developed for each employee outlining that individual's duties during implementation of the plan. This is necessary for two reasons:

1. During a disaster, the duties of some employees who normally perform non-critical functions may change significantly; and
2. During certain types of disasters, some employees may be unable to report to work; therefore, other employees will be required to perform their duties.

The emergency job descriptions should be cross referenced to position desk manuals and/or written operational procedure manuals.

BIA

A Business Impact analysis (BIA) is the first step in developing a BCP. It should include:

- Identification of the potential impact of uncontrolled, non-specific events on the institution's business processes and its members;
- Consideration of all departments and business functions, not just data processing; and
- Estimation of maximum allowable downtime and acceptable levels of data, operations, and financial losses.

Risk Assessment

For a disaster recovery plan to meet its objectives, management must evaluate the types of risk the institution is susceptible to and the impact each risk occurrence could have on financial performance, operations, and member services.

The risk assessment is the second step in developing a BCP. It should include:

- A prioritizing of potential business disruptions based upon severity and likelihood of occurrence;
- A gap analysis comparing the institution's existing BCP, if any, to what is necessary to achieve recovery time and point objectives; and
- An analysis of threats based upon the impact on the institution, its members, and the financial markets, not just the nature of the threat.

There are a number of risks that could potentially impact a corporate. The risks may be different between institutions as a result of geography, local environment, or the services offered. It is imperative management clearly identify and assess the risks associated with their unique operation.

Some potential risks management should consider are:

1. Natural - fire, flood, earthquake, hurricane;
2. Technical - hardware/software failure, power disruption, communications interference;
3. Human - riots, strikes, disgruntled employees and terrorist acts; and
4. Pandemic Infectious Disease Outbreak – a threat with the ability to spread rapidly over large areas, possibly worldwide.

Disaster Recovery Sites

Each corporate must have an alternate facility equipped and ready for immediate use in the event of a disaster. The facility, referred to as a recovery site, must be located far enough from the corporate to minimize the possibility of both locations being affected by a regional disaster. The recovery site should be located in a separate power grid and be served by a separate telephone central office than the corporate. The recovery site should be accessible to employees within a reasonable period of time.

The recovery site facility must be large enough and sufficiently supplied and equipped to accommodate the corporate's entire operation with a minimum number of employees needed for day-to-day operations. The contingency site contract must indicate the location will be available for a sufficient amount of time to allow the corporate to locate a new permanent facility, if necessary.

In some cases a corporate may establish its own alternative site, while in other cases the corporate shares a location with other entities. Cost is a major factor. Various companies market memberships in recovery sites at a set annual fee.

It is in the best interest of the corporate to have a written agreement with the management of the recovery site, or other parties with which they share the facility. The agreement should detail the conditions under which the site may be used. It is imperative should a disastrous event occur, the recovery site location is available and has the capability to handle the critical operations.

All of the corporate's essential personnel should have an understanding of the disaster recovery plan. Employees should know what to do if an emergency occurs and where and when to report to the recovery site location. The use of periodic tabletop walk-through exercises will enhance that knowledge. The facility should be tested, at least annually, to ensure it meets minimum requirements to continue essential services.

Reciprocal Agreements

Many corporates enter into agreements with their members or other corporates with compatible hardware/software capabilities. These arrangements usually are made on a "best efforts" basis whereby Corporate A agrees to backup Corporate B provided Corporate A has time available. There is a mutual agreement to share office facilities, data processing capacity, or other services in a disaster. This type of arrangement is less desirable than one where dedicated facilities are available, because it relies on the excess capacity of the reciprocal institution. Since the needs of parties are continually evolving, it is difficult for management to determine whether the available excess capacity is adequate to meet present or future demands. Presumably,

the reciprocal institution would take care of its own needs first. Many reciprocal agreements contain written limitations to that effect.

Reciprocal agreements can play an important role in providing a secondary backup site in the event of a regional catastrophe rendering both the primary and recovery site locations inoperable. These agreements outlining both parties' responsibilities should be in a written contact.

Disaster Recovery Testing

The most comprehensive disaster recovery plan may be of little value if, under actual conditions, it fails to perform adequately. It is incumbent upon management to ensure to the best of their ability the plan will perform as proposed. Each corporate must perform at least a full scale test of its disaster recovery plan on an annual basis. Additionally, larger corporates may need to independently test various aspects of the plan more frequently (i.e., information systems, funds transfer, ACH, and item processing). A full scale test is one which covers all aspects of the corporate's operation and includes a full day's business volume. Item processing operations may be tested independently.

Periodic review should be performed to ensure, when a full-scale test is performed, all employees are familiar with their duties and responsibilities. Where practical, surprise tests could also be included to ensure employees maintain ongoing familiarity with the plan. In an actual emergency, the plan is more likely to be effective if all employees remain calm and are familiar with their responsibilities. Walk-through exercises will help keep staff familiar with the plans.

Corporates must maintain detailed documentation of each disaster recovery test. The results should be subjected to an independent audit and reviewed by the board of directors and senior management. Officials should utilize test results to make any necessary revisions to the plan to address weakness identified during testing.

Protective Measures Against Disasters and Disruptions

Physical disasters can be created by man or result from natural phenomena. Regardless of the cause, the best plan to prevent severe loss is effective backup procedures covering equipment, data, operating systems, application software, communication resources and documentation. These provisions enable reconstruction with minimal confusion and delay. Following are the basic security measures for major physical risks:

Fire

Computer center personnel must know what to do in a fire emergency. Instructions should be posted in prominent locations. Fire alarm boxes and emergency power switches should be clearly visible and unobstructed. Fire drills should periodically be held. Personnel should know how to respond to automatic extinguisher systems, as well as the location and operation of power and shut-off valves. Data centers should have industry standard chemical based fire suppressant systems. Where only water based systems are available, waterproof covers should be located near equipment in the event the sprinklers are activated. Hand extinguishers should be placed in readily accessible locations. All computer installations should be equipped with heat or smoke detectors. Detectors should be located away from air conditioning or intake ducts as they may hinder the build up of smoke required to trigger the alarm. Walls, doors, and partitions should be fire-resistant. The degree of fire protection in the data center should be consistent with the ability to easily restore information.

Flooding

A corporate should not locate its computer installation in or near a flood plain. If the computer equipment is placed below ground level or a sprinkler system is used, precautions to limit water damage should be taken. If there is a floor above the computer room, the computer room ceiling should be sealed to prevent water seepage.

Sabotage and Riot

Computer center personnel should know how to handle intruders, bomb threats, and other disturbances. Since attacks on computer installations have occurred, their locations should be inconspicuous. Sabotage could be caused by a disgruntled employee. Therefore, personnel policies should address the process for the immediate termination and removal from the premises of any employee considered a threat. Locked doors, intrusion detection devices, guard and other controls that restrict physical access are important preventative measures.

Power Failure

Voltage coming into the data center is often monitored by a recording voltmeter and regulated to prevent power fluctuations. In the event of power failure, an alternative power source should be provided. Independent power supply units consist of gas or diesel generators or a battery arrangement**,** providing electricity for a limited period to allow an orderly system shutdown. Most corporates use an uninterruptible power supply (UPS) system to allow an orderly critical function shut down.

Fraud or Theft

Physical measures to safeguard against loss from fraud or theft are comparable to those outlined for sabotage and riot. Exposure is reduced by restricting access to information that may be altered or stolen. Since fraud or theft may be perpetrated easily by insiders, personnel policies should be designed to minimize that possibility. Procedures to safeguard information are essential to ensure member confidence. This is supported by a strong system of internal controls and audit function. Additionally, there may be legal implications for the corporate if sensitive or confidential information pertaining to a member is released.

Equipment Failure

Equipment failure may result in extended processing delays. Performance of preventive maintenance enhances system reliability

and should be extended to all supporting equipment, such as temperature and humidity control systems and alarm or detection devices.

Pandemic Planning

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

Continuity plans to manage a pandemic event 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;
- A testing program to ensure the pandemic planning practices and capabilities are effective; and
- An oversight program to ensure ongoing review and updates are made to the pandemic plan.

Hardware Backup

Hardware backup is a critical step in contingency planning. The corporate needs to consider alternate processing capabilities for each of its computer installations in the event the work environment becomes disabled. These plans can take several forms and involve the use of another financial institution, data center, or installation.

In addition, hardware manufacturers and software vendors can be helpful in locating an alternate processing site and in some cases will be able to provide backup equipment under emergency conditions. In

planning the recovery site facility, the corporate should consider the adequacy of hardware at the location, the ability to quickly relocate hardware, or an agreement to share compatible hardware at another facility.

Program or Software Backup

Software backup is another important phase of contingency planning. The program backup for all hardware platforms consists of three basic areas:

1. Operating system software;
2. Application software; and
3. Documentation.

All software and related documentation must have adequate off-premise storage. Even when using a "standard" software package from one vendor, the software will likely vary from one location to another based on options chosen by the institution during or subsequent to system implementation.

The operating system must be backed-up with at least two copies of the current version. Without it, even the most sophisticated computer hardware is useless. One copy should be stored in the tape and disk library for immediate availability in the event the original is impaired. The second copy should be stored in a secure, off-premise location. Duplicate copies should be tested periodically and recreated whenever there is a change in the original.

Application software, which includes both source and object versions of all application programs must be maintained in the same manner as the operating system software. Backup copies of programs must be updated as program changes are made. Minor updates to backup copies can be made on a group basis, but major revisions or enhancements to application programs should be updated immediately. Storing, testing, and updating such software should be addressed in the contingency plan.

Software vendors can usually supply institutions with copies of standard application software products if the originals are destroyed.

However, even assuming the vendor accurately maintained the institution's parameters, selections, and modifications, there will probably be additional expenses and some delay in making the software operational. Under these circumstances, the institution is placing responsibility for storing software with vendors. Most vendors are reluctant to guarantee software availability, because they may not have current sets of the institution's software. Thus, the corporate should maintain its own software backup at an off-site location to ensure minimal processing interruption during an emergency.

Documentation for the operating system and the application programs should also be backed up. A minimum level of documentation should be maintained at an off-site location. This should include current copies of:

1. Operating system options and modifications;
2. Application flowcharts;
3. Descriptive narrative for all systems and programs;
4. File layouts and transaction codes;
5. Operator run instructions; and
6. User manuals.

Procedure manuals are also necessary during disaster recovery. Duplicate copies of all critical procedures should be stored at the off-site location. Most importantly, a copy of the procedures outlining operations during emergencies must be maintained off-site.

Data File Backup

The most important area of backup involves the institution's data files, regardless of the platform in which the data is located. Financial institutions must always be able to generate a current master file. Data files must be backed up both on and off site to provide recovery capability. Retention of current data files, or older master files and the transaction files necessary to bring them current, is important so processing can continue after disasters occur. The creation and rotation of data file backups is a daily activity in most institutions.

Telecommunications Backup

A data center must develop an effective backup plan, including an agreement for alternative site processing. For telecommunications, that plan also must address the communications media and equipment. The contingency plan should establish priorities and identify critical components of the network. Rerouting and redundancy may permit the use of alternate equipment, facilities, lines and circuits, but may still be limited by other considerations. Considerations include risk versus economics, the practicality of the selected backup components, and the security and data integrity provided by the backup plan.

Risks may be addressed by assessing individual components in the network, the dependence on each component, and the probability of it going down or becoming unavailable or unreliable. The costs of various backup alternatives must be weighed against the extent of risk protection each provides. This assessment also should address costs associated with testing, since all components of a plan should be periodically tested.

Financial institutions should have a file identifying all circuits by circuit number and a matrix outlining their location, priorities and uses. A duplicate of this file should be maintained at a different location in case of any problems.

The backup plan must address the practicality of each component. Selected alternatives must be able to accommodate the anticipated volumes or capacities at the necessary speeds to meet the established priorities. Reliability, flexibility, and compatibility - all components of the original planning process - also must be considered in formulation of the backup plan. Additionally, the telecommunications backup plan must be compatible with other contingency plans in the corporate, since it will affect users, data processing, and members.

Security and the data integrity of alternate components used must be considered in the contingency plan. Different components provide different quality and possess different risks. Alternate equipment selected should be checked to determine if it permits encryption.

The relative importance of applications processed and the extent a corporate depends on its telecommunications system will determine the degree of backup required. Management should make a careful appraisal of its backup requirements, decide on an effective plan, detail the procedures, and periodically test its effectiveness.

Examination Objectives

The examiner is to determine if the board of directors and operating management have taken necessary steps to ensure an appropriate contingency plan is in place to maintain the institution's critical operations and services in the event of a disaster. The examiner will need to determine:

1. The board of directors has adopted a written disaster recovery plan;
2. Appropriate review and analysis, in the form of a BIA and Risk Assessment have been performed by management to assess the potential risks and establish operational priorities during disaster occurrences;
3. The corporate has a recovery site location that will be available and fully functional in an emergency situation;
4. The corporate has in place written agreements, as necessary, with recovery site management, vendors, etc. If applicable, a reciprocal agreement is in place with the other institution that agree**s** to share facilities and capacity;
5. Disaster recovery plan testing is performed at least annually. Documentation of the tests is maintained and reviewed by the officials;
6. The disaster recovery plan is revised, as necessary, to address changes in operations, and to resolve problems arising during testing; and
7. The officials have taken steps to address protective measures against disasters and/or disruptions.

Examination Procedures

See Corporate Examination Procedures - Contingency Planning (OCCU 307P).

Examination Questionnaire

See Corporate Examination Questionnaire - Contingency Planning (OCCU 307Q).

References

1. FFIEC Information Systems Examination Handbook
2. NCUA Letter to Credit Unions (08-CU-01) Guidance on Pandemic Planning