CORPORATE CREDIT UNION GUIDANCE LETTER

NO. 2004-05 DATE: November 19, 2004

SUBJ: Business Continuity Planning and Business Critical Processes

TO: The Corporate Credit Union Addressed

The purpose of this letter is to provide corporate credit unions guidance regarding business continuity planning (BCP).

Historically, corporate credit unions have developed disaster recovery plans focusing on catastrophic events which would render their primary data processing center and/or office facilities unusable. While necessary, traditional disaster recovery planning does not address the entire spectrum of non-catastrophic outages of individual computing systems or business processes which may occur from time to time. Such events may not necessitate relocating the entire operation to a hot site. In contrast, BCP aims to develop a series of plans and procedures, useable in whole or in part, that ensure the sustainability of critical business processes at a level acceptable to the business, its partners, and customers. BCP is designed to guide efforts to return to normal processing as soon as practical. Acceptable business continuity options for sustaining critical business processes may include one, two or a mix of the following options:

- Redundant information systems or delivery channels/mechanisms;
- Alternative information systems, processing or delivery options; and/or
- Manual processes and procedures.

Alternative methods or options for sustaining all business processes deemed critical must be addressed in the overall scope of BCP.

The primary foundation for this guidance is the Federal Financial Institutions Examination Council Business Continuity Planning IT Examination Handbook (FFIEC Handbook). The FFIEC Handbook outlines expectations for the following areas:

- Board and Senior Management Responsibilities;
- Business Continuity Planning Process;
- Business Impact Analysis;
- Risk Assessment;
- Risk Management;
- Other Policies, Standards and Process; and
- Risk Monitoring.

Corporate credit unions should review the FFIEC Handbook to ensure they are familiar with financial institution best practices. The FFIEC Handbook is available electronically at http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html#bcp.

Additionally, the Office of Corporate Credit Unions (OCCU) has worked cooperatively with the Association of Corporate Credit Unions (ACCU) to ensure corporate credit unions have a common understanding the BCP process. As a result of this cooperative effort, we have identified the minimum acceptable level of BCP for corporate credit unions.

BCP is a significant undertaking and requires the involvement and commitment of every operational area. The board of directors must establish the proper support and culture for BCP to ensure its effectiveness. Therefore, the board should appoint a senior level committee representing multiple operational areas to oversee BCP development. Ideally, a corporate will have a business continuity manager under the general direction of this committee. The business continuity manager should have direct responsibility for coordinating BCP efforts and overseeing BCP plan development, testing, and capability reporting.

At a minimum, corporate credit unions are expected to complete the following steps in order to meet the minimum requirements for BCP.

1) **Conduct a Business Impact Analysis (BIA)**

   Corporate credit unions must identify the business processes that significantly impact their continued operation. By definition, the scope of the BIA must include all business processes in order to identify elements are new, changed, or previously unrecognized, which once identified may make a business process critical. A critical business process may be physical (building, roads, etc.), human (employees, members, consultants) or technical components (hardware, software, interfaces, external systems, power sources, telecommunications). A critical business process may also be a vendor relationship or dependency. Once the critical business processes have been identified, the next step is to determine how long the organization could continue to function without each process. Factors to consider in performing a business impact analysis are:

   a) The critical system or service;
   b) Identification of single points of failure (hardware component failure, communication or network outage, file or database corruption, local disaster, regional disaster, power outage, software failure, loss of key staff, etc.);
   c) Minimum acceptable service levels or system output; and
   d) The cost, duration, and impact of each failure.

The BIA should be thoroughly documented. The documentation should be sufficient to allow the BCP committee and independent reviewers to follow the process, validate assumptions and scenarios, and should include all systems and business processes. The board of directors will review and approve the comprehensive BIA and approve established business continuity requirements (i.e., acceptable timeframes for recovery of each critical business process) for the organization.

The BIA should be updated whenever a corporate credit union develops a new function or whenever significant changes occur involving existing functions. The board of directors should review the consolidated BIA at least annually.

2) **Conduct a Formal Risk Assessment**

A continuity risk assessment must be completed for each critical business process identified by the BIA. The risk assessment must identify and document:

a) Realistic threat scenarios (local disaster, regional disaster, power outage, software failure, loss of key staff, etc.) across a broad range of possible business disruptions that could potentially disrupt the delivery of products and services to customer and the ability to meet the business expectations of the organization or its partners;
b) Identification and assessment of single points of failure;
c) Known and possible vulnerabilities;
d) The probability of occurrence;
e) Expected business, financial, regulatory or reputation impacts or losses;
f) Impacts on the integrity, availability or privacy of information;
g) Consideration of preventative measures (controls) that deter, detect, and/or reduce impacts to the business process or system;
h) A gap analysis that identifies differences between expectations and the existing plan; and
i) Identification of the frequency and complexity of appropriate recovery plan testing.

The documented results should also include areas reviewed that pose little or no risk to ensure all critical functions have been considered. As with the BIA, the board of directors will review the scope and output of the BCP risk assessment and approve the business continuity risk mitigation requirements for the organization.

3) **Develop the Business Continuity Strategies**

Business continuity strategies for each critical business process must be developed and documented. This is an enterprise-wide undertaking requiring the participation of staff in all operational areas. Senior management and the board must review and approve these strategies.

4) **Develop the Business Continuity Plan**

The board-designated committee or business continuity manager must ensure the business continuity strategies are consolidated and documented in a centralized plan. The comprehensive enterprise-wide plan should address a wide range of contingency scenarios from minor disruptions to loss of total capability. Potential disruptions should be addressed by flexible scenario-based response strategies. These strategies must be sufficiently detailed to provide step-by-step execution of problem management, situation assessment and business impact guidance and escalation timetables. The following issues should be also be addressed:

a) Emergency response;
b) Command and control;
c) Crisis management and communication;
d) Human resources;
e) Information systems;
f) Telecommunications and data recovery;
g) Facilities management and restoration; and
h) Production areas and operations.

Documented departmental or business process-specific recovery procedures are required for all critical business processes. Procedures will include a prioritized sequence of immediate steps to be taken during an event including:

- Notification of appropriate parties;
- Assembling required expertise;
- Accurate diagnosis of the situation;
- Damage containment and control;
- Immediate actions to facilitate recovery;
- Test steps necessary to verify complete data recovery to an expected result at a known point in time; and
- Address interdependencies between processes and systems and third-parties.

5) **Exercise and Maintain the Plan**

Corporate credit unions must test all business processes identified and classified as critical annually and within a reasonable time period (e.g., 3 months) after significant changes in business processes, technology or the plan. Ideally, this occurs during an integrated test. When that is not feasible, separate tests of critical processes should occur using realistic test assumptions that simulate integrated testing to the degree possible.

A clearly defined test plan must be prepared for each critical business process, including the scope, assumptions, and objectives of the test. The assumptions and objectives of the test should be documented and validated in advance of the test.

A structured process must be developed to capture and report test results and any corrective actions. The results and corrective actions must provide linkage back to baseline requirements to maximize their usefulness. Accurately summarized results must be presented to executive management and the board for review.

Procedures must be in place to ensure the plan is kept current as changes in potential threats, the business environment, critical business processes or systems occur.

The BCP, including the test results reporting process, must be reviewed by internal audit or an independent third party to validate its scope and effectiveness.

BCP is a process with a definable life cycle. It is understood all corporate credit unions are not currently at the same level of preparedness. Due to the diversity of their operations, those not currently meeting the minimum BCP requirements will not reach the minimum level of BCP simultaneously. Additionally, some corporate credit unions may elect to exceed these requirements, in whole or in part, based on perceived business needs. Corporate credit unions that have not achieved the minimum BCP requirements are expected to have completed the following:

a) Assess the corporate's current position relative to the minimum BCP requirements;
b) Develop an appropriately detailed action plan (i.e., task(s), milestones, and status) and a timeline for completing the minimum BCP requirements; and
c) Report progress toward completion of the action plan to the board of directors at least quarterly.

OCCU examiners will evaluate corporate credit unions on a best efforts basis to comply with the minimum required level of BCP. Those not at the minimum required level will be evaluated on the thoroughness and reasonableness of their action plans as well as their sustained, timely progress in meeting defined milestones.

The OCCU plans to continue working cooperatively with the ACCU to ensure common understanding of the expectations regarding BCP. If you have any questions or concerns, please contact my office.

Sincerely,

/S/

Kent Buckham
Director
Office of Corporate Credit Unions

FFIEC Information Technology Examination Handbook

Booklets

Audit

- Printable version of booklet
- On-line version of booklet
- Workprogram - Generic word-processing version
- Workprogram - Microsoft Word 2000 version
- Presentations

Business Continuity Planning

- Printable version of booklet
- On-line version of booklet
- Workprogram - Generic word-processing version
- Workprogram - Microsoft Word 2000 version
- Presentations
- Non-regulatory Resources

Development and Acquisition

- Printable version of booklet
- On-line version of booklet
- Workprogram - Generic word-processing version
- Workprogram - Microsoft Word 2000 version
- Presentations

E-Banking

- Printable version of booklet
- On-line version of booklet
- Workprogram - Generic word-processing version
- Workprogram - Microsoft Word 2000 version
- E-Banking Request Letter Items - Generic word-processing version
- E-Banking Request Letter Items - Microsoft Word 2000 version
- Presentations

FedLine

- Printable version of booklet
- On-line version of booklet
- Workprogram - Generic word-processing version
- Workprogram - Microsoft Word 2000 version
- Presentations

Information Security

- Printable version of booklet
- Low resolution version of booklet
- On-line version of booklet
- Workprogram - Generic word-processing version
- Workprogram - Microsoft Word 2000 version
- Presentations

Management

- Printable version of booklet
- On-line version of booklet
- Workprogram - Generic word-processing version
- Workprogram - Microsoft Word 2000 version
- Presentations

Operations

- Printable version of booklet
- On-line version of booklet
- Workprogram - Generic word-processing version
- Workprogram - Microsoft Word 2000 version
- Presentations

Outsourcing Technology Services

- Printable version of booklet
- On-line version of booklet
- Workprogram - Generic word-processing version
- Workprogram - Microsoft Word 2000 version
- Presentations

Retail Payment Systems

- Printable version of booklet
- On-line version of booklet
- Workprogram - Generic word-processing version
- Workprogram - Microsoft Word 2000 version
- Presentations
- Non-regulatory Resources

Supervision of Technology Service Providers

- Printable version of booklet
- On-line version of booklet
- Workprogram - Generic word-processing version
- Workprogram - Microsoft Word 2000 version
- Presentations

Wholesale Payment Systems

- Printable version of booklet
- On-line version of booklet
- Workprogram - Generic word-processing version
- Workprogram - Microsoft Word 2000 version
- Presentations