

Business Continuity Plan

SAMPLE
Partial Doc - (c) MM&T, INC 2004
Strictly for demonstration purposes.

1 Introduction	3
1.1 <i>BCP Policy Statement</i>	3
1.2 <i>Special Considerations</i>	3
1.3 <i>Assumptions & Constraints</i>	4
1.4 <i>Minimum Requirements</i>	5
1.5 <i>Responsibilities</i>	5
1.6 <i>CAPlus Documentation, Database, & BCP-CD</i>	5
2 Threat/Risk Assessment (TRA)	7
2.1 <i>TRA Results Overview</i>	7
3 Recovery Process	9
3.1 <i>Emergency Response & Recovery Procedure</i>	9
3.2 <i>Authorities & Emergency Quorum</i>	9
3.3 <i>Plan Activation & Scope</i>	10
3.4 <i>Hotsite/Alternate Locations Overview</i>	11
4 Recovery Teams & Responsibilities	12
4.1 <i>BCP Manager</i>	12
4.2 <i>External Resources</i>	13
5 IT Environment & Recovery	16
5.1 <i>IT Infrastructure & Operations Overview</i>	16
5.2 <i>Networking Overview</i>	16
5.3 <i>Telecommunications Network Overview</i>	16
5.4 <i>Data Backup Summary</i>	16
5.5 <i>DP & Operations Recovery Sequence</i>	17
5.6 <i>Data Processing & Systems Restoration Priority Lists</i>	18
6 Risk Monitoring	19
6.1 <i>BCP Testing</i>	19
6.2 <i>Testing Methodology</i>	19
6.3 <i>Hotsite Requirements & Testing</i>	20
6.4 <i>Test Results Reporting</i>	20
6.5 <i>BCP Maintenance</i>	21
6.6 <i>BCP-CD Update</i>	21
7 Additional Considerations	22
7.1 <i>Systems Development & Life Cycle (SDLC)</i>	22
7.2 <i>Change Control</i>	22
7.3 <i>Insurance Coverage</i>	22
7.4 <i>Data Synchronization</i>	23
7.5 <i>Resource Training</i>	23
7.6 <i>Communications Planning</i>	23
7.7 <i>Government & Community</i>	23

Appendix A | Emergency Response Procedures..... 24

- A.1 | *Main Office Evacuation* 24
- A.2 | *Branch Evacuation* 24
- A.3 | *Medical Response & General Safety* 25
- A.4 | *Severe Weather & Natural Disasters* 25
- A.5 | *Building & Equipment Emergencies* 25
- A.6 | *Environmental Hazards* 26
- A.7 | *Workplace Disruptions* 26
- A.8 | *Loss of Workforce* 26
- A.9 | *Workplace Addiction* 27
- A.10 | *Labor Dispute* 27
- A.11 | *Terrorism* 27
- A.12 | *Computer Virus Attacks* 27
- A.13 | *Systems Intrusion/Abuse* 28
- A.14 | *Power Outage/Blackouts* 28
- A.15 | *Communications Failure* 28
- A.16 | *Equipment/Software Failure* 28
- A.17 | *Delivery Malfunction* 29
- A.18 | *Transportation Disruption* 29
- A.19 | *Run on Financial Institution* 29
- A.20 | *Negative Publicity* 29
- A.21 | *White Collar Crime* 30
- A.22 | *Unauthorized Facilities Access* 30
- A.23 | *Bomb Threat* 30
- A.24 | *Extortion Threat* 30

1 | Introduction

Supporting Documentation & Reports

BIA Documentation
BCP Planning Polic(ies)

The Board of Directors and senior management of Clients Federal Credit Union (hereafter referred to as the “institution”) are fully aware of their responsibility for establishing policies and procedures for comprehensive continuity planning. This business continuity plan (hereafter referred to as the “continuity plan”, “plan”, or “BCP”) has been developed to fulfill this requirement.

Accordingly, the institution has conducted a business impact analysis (BIA) in order to identify and prioritize the operations/functions, internal and external human resources, technology resources, documentation, data, records, and materials/supplies critical to its survival and ability to recover from a disaster. It is based on the findings of this BIA that this plan, as well as the institution’s general continuity and strategic planning policies, have been developed.

No plan can address every conceivable situation that could possibly arise. This plan addresses a worst-case scenario and its framework can accommodate emergencies of lesser proportions.

1.1 | BCP Policy Statement

The institution’s management and Board of Directors recognize the need to establish comprehensive business continuity policies to protect employees, customer/members, assets, and information as well as to minimize the time it will take to restore critical operations, functions, products, and services after an emergency is declared. The institution also recognizes that increasing dependency on electronic data processing for operational support results in a corresponding risk, so that a lengthy loss of this resource could negatively impact overall performance and the institution’s ability to continue operations.

Therefore, it is the policy of the institution to develop and maintain a business continuity plan that will provide the institution with every opportunity to withstand a catastrophic event - whether accidental, man-made or natural - and to resume total operations quickly, efficiently and effectively. As such, this plan is designed to minimize the effects of a disaster through pre-planning and contains actions to be taken should an event occur, with or without warning, which causes an emergency to be declared. Its primary purpose is to provide for an orderly, timely resumption of business operations by clearly defining the resources, equipment, supplies, and documentation required to execute the plan as well as their role in the recovery process.

An identification of the risks to which the assets of this institution may be exposed has been made and analyzed. This analysis has indicated that the institution would experience major adverse effects if its ability to perform its intended functions were interrupted for as little as seventy-two (72) hours and therefore, the ultimate goal of this plan is to resume essential business operations and data processing within a 72-hour time frame, followed by the resumption of all operations and processing within one (1) week.

It is expected that, under the guidance of this plan, management will provide swift and decisive leadership and employees will diligently carry out their tasks and fulfill their responsibilities in order to execute a successful and complete recovery. Additional policy goals are listed below:

- Establish authority & responsibility for plan development, implementation, and maintenance.
- Provide emergency response procedures for identified threats.
- Document backup plans for hardware, software, documentation, and data files.
- Comprehensive strategies for emergency planning.
- Establish requirements for testing the adequacy and effectiveness of the plan.

1.2 | Special Considerations

In the context of this plan, the terms “business continuity”, “continuity planning”, “contingency planning”, and “disaster recovery” all refer to the process by which an entire business or small business units re-establish operations and/or service to internal and/or external customer/users, while ensuring that (1) safety and soundness are maintained, (2) assets are protected, and (3) all regulatory requirements are met. These terms do not mean recreating the functional area as it currently exists or getting back to “business as usual”. Rather, they refer to an interim step to resume a functional group’s operational capabilities within a pre-defined timeframe, defined by its criticality and the risks associated with/impact that a delay in its resumption would have on the entire institution.

In addition, the table below details a list of generic terms and resource designations that are used throughout the plan and the specific locations, names, and data that correlate directly to these terms. Additional details about these resources and locations are provided within the BCP-CD reports. These terms are highlighted **IN BOLD** when they appear in this plan.

BCP-Specific Terms & Designations		Table 1.2a
<i>Generic Term</i>	<i>Correlating Resource/Location/Data</i>	
Operations Center	The institution's Main Office, Data Center, or any building where most/all critical units/functions and IT resources are housed. Main Office (123 Main Street, Springfield, CT)	
CEO/BCP Manager	Beth Boroughs, CEO	
Remote DP Hotsite/DR Provider	The vendor with which the institution will work to restore DP capabilities in the event of an emergency. In the case of WFCU, this will be a remote DP Hotsite operated by its Core Provider. CUSA Technologies, Inc. (Fiserv) (986 W. Atherton Drive, Salt Lake City, UT)	
Command Center	The location from which communications to the primary service provider via the Remote DP Hotsite/DR Provider will be restored. Springfield Food Center (234 West Main Street, Springfield, CT)	
Secondary Command Center	The location to be used in the event that the Command Center is not available and/or in addition to the Command Center. Springdale Memorial Town Hall (789 East Main Street, Springfield, CT)	
Core Provider	CUSA Technologies, Inc. (Fiserv) HEADQUARTERS (986 W. Atherton Drive, Salt Lake City, UT) LOCAL/REGIONAL OFFICE (Mansfield, MA)	
Items Processing Provider	Constitution State Corporate Credit Union (CSCCU) (47 Barnes Industrial Park Road South, Wallingford, CT)	
Telecommunications Provider	Cox Communications (9 J.P. Murphy Highway, West Warwick, RI)	
BCP Provider	The vendor used by the institution to develop/maintain its business continuity planning requirements, strategies, and documentation. MM&T, INCorporated (PO Box 1322, Middlebury, CT)	

1.3 | Assumptions & Constraints

The institution has carefully considered the following assumptions, on which this plan has been developed, based on the findings of the institution's business impact analysis (BIA) and risk assessment. Although the basic framework of the plan is built upon them, provisions for exceptions to these assumptions have been made and are addressed in various sections of the plan.

- The disaster will render all or part of the Operations Center unusable or inaccessible;
- The disaster will occur at the worst possible time;
- Current copies of the business continuity plan and all supporting documentation/data (e.g. BCP-CD) are readily available from offsite storage locations;
- Pre-determined hotsite locations will be available;
- The **Remote DP Hotsite/DR Provider** will perform according to its "Disaster Recovery Agreement";
- Required personnel are available and understand their role in the execution of the plan;
- Current file backups are stored and readily accessible from offsite locations;
- Critical documentation is stored and readily accessible from offsite locations;
- Communication lines are available or can be purchased/installed within 48 hours;
- Additional PCs and communications equipment/software can be purchased within 48 hours;
- Required supplies are stored and readily accessible from offsite locations and/or vendors;
- The basic priorities for restoration of essential service to the community will take precedence over the recovery of an individual organization;
- A general disaster will affect similar organizations and lessen the net effect on the institution, and;
- Vehicular transportation in the local area is possible.

1.4 | Minimum Requirements

In order to fulfill the goals and objectives and ensure the successful execution of this plan, the institution has made provisions for and will maintain the following requirements.

- Establishing a pre-arranged **Command Center** from which senior/executive management and BCP Management Team can conduct business.
- Establishing a pre-arranged **Data Processing (DP) Hotsite** to house critical operations/functions of the institution as well as any additional hotsite locations required for other critical functions/operations (e.g. Lending, Customer/Member Services) and/or displaced personnel.
- Ensuring availability of equipment and materials required to re-establish operations at the hotsite.
- Pre-assigning required personnel to their appropriate hotsite locations and pre-defining emergency notification procedures.
- Pre-defining the tasks required to be executed after the disaster and assign them to personnel adequately trained and knowledgeable of his/her responsibilities in regards to task completion.
- Ensuring that up-to-date, backup copies of critical data, files, programs, and documentation are stored and readily accessible at offsite/Hotsite locations.
- At a minimum, making current copies of this plan and BCP-CD available at all hotsite locations and providing all Team Leaders with a copy of the BCP-CD.
- Implementing adequate training programs to ensure that all involved internal and external resources understand their role and are prepared to complete their assigned recovery/reconstruction tasks in the event of an emergency.
- Ensuring provisions for secure transportation of personnel and materials.
- Ensuring that adequate, necessary funds are available to support the recovery.

1.5 | Responsibilities

In order to ensure that this plan remains current and viable, the institution's **BCP Manager** is responsible for ensuring that the following tasks are completed on an ongoing basis.

- Training employees/required resources in BCP strategies and responsibilities.
- Receiving required BCP data updates and forwarding to **BCP Provider** in a timely manner.
- In cooperation with **BCP Provider**, maintaining the CAPlus database to a current status.
- In cooperation with **BCP Provider**, ensuring the plan is in a current state at all times.
- Testing the plan as well as reviewing and approving the test plan prior to its execution.
- Periodically reviewing the backup file creation, rotation procedures, and logs to ensure its viability.
- At least annually, working with **BCP Provider** to execute the CAPlus BCP maintenance ("Continuity/Monitoring/RM02-BCPMaintenance.doc") procedure, which includes a review of the "Data Processing & Systems Restoration Priority Lists", "Recovery Tasks", "Recovery Procedures", and "Emergency Operating Procedures" as well as all additional, supporting documentation and data, to ensure the accuracy of all CAPlus and BCP information.
- At least annually, updating the Board regarding the status of the plan, testing results, and maintenance routines.

1.6 | CAPlus Documentation, Database, & BCP-CD

The institution's CAPlus database ("Data.mdb") and documentation ("Continuity" directory) is installed and maintained internally by the institution on the **CPO Server @ MM&T, INCorporated** (Middlebury, CT).

This plan contains the minimum information to illustrate the institution's disaster recovery/business continuity strategy, and is supported by reports, generated from the CAPlus database, that provide detailed information on the specific resource, equipment, and supply requirements of the institution. It is also supported by the following BCP-related documentation and data.

- BIA** Contains all business impact analysis (BIA) documentation, including the suggested procedure and worksheet for conducting the BIA. This folder should also be used to store completed BIA interview forms.

- Documentation** Contains the core BCP document (“ContinuityPlan.doc”) and all supporting documentation (see below), such as hotsite/service provider contracts, BCPs, and test results and insurance coverage documentation.
- Monitoring** Contains policies, procedures, and forms required for risk monitoring, including annual BCP testing, review, and maintenance procedures and supporting forms.
- Procedures** Contains “Recovery Procedures” (from the CAPlus database) as well as the institution’s emergency/manual operating and related internal procedures.
- Threats** Contains threat/risk assessment (TRA) related documentation, including a procedure and worksheet to conduct the TRA, in order to identify threats and determine their probability of occurrence and potential impact.

All required/standard documentation and data is provided on the accompanying Business Continuity Plan CD (“BCP-CD”) and can be viewed/printed from any PC with a standard CD-ROM drive and printer connection. At a minimum, the BCP-CD includes the following required/standard elements (unless otherwise noted in “Table 1.6a” below).

- | | |
|--------------------------------------|---|
| Business Continuity Plan Document | Communications (@ Hotsite/By Shift) |
| Threat/Risk Assessment Documentation | Servers (@ Hotsite/By Shift) |
| BIA Documentation | Workstations (@ Hotsite/By Shift) |
| Recall Roster | Forms/Supplies (@ Hotsite) |
| Locations & Hotsites | Reports/Documents/Files (@ Hotsite) |
| Personnel & Team Members | Recovery Tasks (By Team/By Category) |
| Team Leaders | Recovery Procedures |
| Vendors & External Teams | Risk Monitoring Procedures |
| Equipment (@ Hotsite/By Shift) | Telephone Books (Locations/Personnel/Vendors) |

Requirements, as designated in the above-mentioned reports on the BCP-CD, are specific to the event that the institution moves operations to a hotsite/temporary location for LESS THAN TWO WEEKS. Should the need to support operations at the hotsite be longer, the institution will review requirements and recall the necessary personnel/acquire the necessary equipment, communications, and supplies, as deemed necessary.

Additional supporting elements are available as indicated in “Table 1.6a” below. This documentation (e.g. IT compliance reviews, strategic plans, general policies and procedures, flowcharts, regulatory information, testing results) may be required/desired to support the institution’s plan and copies may be stored internally by the institution or externally by vendors/service providers. The following table lists and indicates storage location/backup information for all supporting BCP-elements included with this plan, which are referred to (as applicable) in a textbox at the beginning of each plan.

Supporting Documentation & Materials		Table 1.6a
<i>Document/Material Name</i>	<i>Storage Location/Backup Information</i>	
Departmental/Organizational Charts	BCP-CD “Supporting Documentation”	
IT/Communications Schematics	BCP-CD “Supporting Documentation”	
Emergency/Manual Operating Procedures	BCP-CD “Recovery Tasks”	
IT Policies & Procedures	BCP-CD “IT Policies & Procedures” Hardcopy Stored onsite in CEO’s office Electronic Stored onsite on standalone PC in CEO’s office	
Annual BCP Testing Results (Most Current)	BCP-CD “Risk Monitoring” (Most recent certificate of completion of CUSA DR test & “Update01” spreadsheets	
Regulatory Examination Results/Reports	BCP-CD “Risk Monitoring” section, Exam2001/Updates folder(s).	
Core Provider Contract/BCP/Testing Results	Hardcopy stored onsite in CEO’s office	
Remote DP Hotsite/DR Service Provider Contract/BCP/Testing Results	Hardcopy stored onsite in CEO’s office	
Command Center Hotsite Contracts	BCP-CD “Supporting Documentation/Contracts” Hardcopy stored onsite in CEO’s office.	

Each year, the **BCP Manager** should oversee the review and update the institution’s CAPlus database, continuity plan, and supporting documentation to reflect changes that have occurred at the institution as described in 6.5 | BCP Maintenance.

2 | Threat/Risk Assessment (TRA)

Supporting Documentation & Reports

Threat Assessment Documentation
 Team Leaders Report
 Emergency Manual Ops. Procedures

The institution has conducted a threat/risk assessment to identify potential threats to the stability and security of its facilities, data and information, IT/communications infrastructure, employees, assets, and critical operations/functions. This section of the plan is based upon the findings of that risk assessment, providing a list of the threats that have been determined the most-likely to affect the institution (see below). In support of the findings, Appendix A | Emergency Response Procedures contains emergency procedures developed to help the institution respond to identified threats/situations in an attempt to minimize loss of human life and internal resources/assets.

2.1 | TRA Results Overview

Many events could expose the **Operations Center** to physical damage so severe that it would render the building inaccessible or unusable. In addition to physical disasters, a variety of threats to the institution's technology and data exist for which the cause can be either accidental (e.g. power outage, equipment failure) or intentional/malicious (e.g. fraud/theft, sabotage, terrorism).

Based on its most recent assessment/review, the institution has determined that the following threats pose the greatest risk to the institution based on factors such as its organization, mode of operations, asset size, services and products offered, technology infrastructure, facilities, and geographic location. Risks are categorized as belonging to one of the following threat types and are assigned both a probability of occurrence and impact rating of high, medium, or low.

Technical Disasters			Table 2.1a
Probability Rating	Impact Rating	Threat	Corresponding Emergency Procedure
M	M	Loss of Workforce	A.8 Loss of Workforce
M	M	Workplace Addictions	A.9 Workplace Addiction
M	L	Loss of Critical Records/Documentation	A.13 Systems Intrusion/Abuse
M	L	Data Corruption/Loss (Accidental)	A.13 Systems Intrusion/Abuse
H	L	Power Outage/Blackouts	A.14 Power Outage/Blackouts
M	H	Communications Failure	A.15 Communications Failure
M	H	Service Provider Outage	A.15 Communications Failure
M	M	Hardware Failure	A.16 Equipment/Software Failure
M	M	Software/Applications Failure	A.16 Equipment/Software Failure
M	M	Delivery Malfunction	A.17 Delivery Malfunction
M	M	Transportation Disruption	A.18 Transportation Disruption
L	H	Run on Financial Institution	A.19 Run on Financial Institution
L	M	Negative Publicity	A.20 Negative Publicity
M	M	Human Error	Depends on situation.

Natural Disasters			Table 2.1b
Probability Rating	Impact Rating	Threat	Corresponding Emergency Procedure
L	H	Earthquake	A.4 Severe Weather & Natural Disasters
L	H	Hurricane	A.4 Severe Weather & Natural Disasters
L	H	Tornado	A.4 Severe Weather & Natural Disasters
M	L	Flood	A.4 Severe Weather & Natural Disasters
M	L	Winter Weather/Blizzard	A.4 Severe Weather & Natural Disasters
M	L	Water Damage	A.5 Building & Equipment Emergencies
M	M	Electrical Storms/Lightening	A.5 Building & Equipment Emergencies
L	H	Fire	A.5 Building & Equipment Emergencies
L	H	Explosion (Accidental)	A.5 Building & Equipment Emergencies
L	H	Air Contamination	A.6 Environmental Hazards
L	H	Hazardous Spill	A.6 Environmental Hazards

Malicious Activity			Table 2.1c
<i>Probability Rating</i>	<i>Impact Rating</i>	<i>Threat</i>	<i>Corresponding Emergency Procedure</i>
L	H	Explosion (Malicious)	A.5 Building & Equipment Emergencies
L	M	Civil Unrest/Riot	A.7 Workplace Disruptions
L	M	Workplace Violence	A.7 Workplace Disruptions
L	M	Labor Dispute/Strike	A.10 Labor Dispute
L	H	Terrorism (General)	A.11 Terrorism
L	H	Bio-Chemical Terrorism	A.11 Terrorism
L	H	Cyber-Terrorism	A.13 Systems Intrusion/Abuse
L	H	Computer Hacking	A.13 Systems Intrusion/Abuse
L	H	Denial of Service Attack	A.13 Systems Intrusion/Abuse
L	H	Data Corruption Loss (Malicious)	A.13 Systems Intrusion/Abuse
L	H	Virus Attack	A.12 Computer Virus Attacks
L	M	White Collar Crime	A.21 White Collar Crime
L	M	Unauthorized Facilities Access	A.22 Unauthorized Facilities Access
L	H	Bomb Threat	A.23 Bomb Threat
L	M	Extortion Threat	A.24 Extortion Threat

3 | Recovery Process

This section of the plan contains an overview of the entire recovery process from the events/circumstances that will lead to declaration of a disaster (and either partial or full execution of the plan) to the renovation of the old/reconstruction of a new, permanent location.

This plan has been specifically developed to address disasters and emergencies affecting the institution's **Operations Center**. Disasters occurring at branch locations and external processing/operating locations, (e.g. service provider locations) are also addressed.

Supporting Documentation & Reports

Locations/Hotsites
 Team Leaders
 Personnel/Team Members
 External Teams
 Telephone Tree/Recall Roster
 Emergency Response Procedure
 Recovery Tasks & Procedures
 Hotsite Contract/BCP/Test Results
 Provider Contract/BCP/Test Results

3.1 | Emergency Response & Recovery Procedure

The officer-in-charge and **BCP Manager** will ensure safe and secure emergency management, using all applicable procedures and resources in order to protect human life and property. Once the situation is under control, the officer-in-charge and **BCP Manager** will work together to implement the "Emergency Response" recovery procedure, which contains a detailed sequence of events for managing and directing the entire recovery process and a summary of which is provided below.

Immediately upon notification that an emergency has occurred, the **BCP Manager** will assemble the BCP Management Team and relocate to the Command Center, from which the following sequence of events will occur under the joint direction of the BCP Manager and officer(s)-in-charge.

1. *Disaster Declaration* | Evaluate situation and determine need to conduct damage assessment.
2. *Damage Assessment* | As deemed necessary and once the area is determined to be safe, conduct a damage assessment according to the "Damage Assessment" procedure. Estimate the length of time the service/facility will remain inaccessible and recommend for a course of action.
3. *Hotsite & Team Activation* | As deemed necessary, hotsite location(s) will be activated and Team Leaders will be notified. Upon notification, Team Leaders will retrieve all required recovery materials/equipment from offsite storage locations, meet at the Command Center where they will be briefed on the emergency/course of action to be taken. Team Leaders will then notify and assemble recovery teams at the pre-assigned hotsite, from which Team Leaders will ensure the timely, accurate completion of assigned tasks. Each department will use existing operational procedures to assist them in carrying out their responsibilities under this plan.
4. *Recovery Management* | Oversee data processing and business recovery from the assigned hotsite location(s), including the execution/delegation of tasks for establishing appropriate security and/or medical attention at damaged location(s), conducting team status report meetings, and communicating with media, customer/members, and employees.
5. *Reconstruction & Relocation* | Coordinate reconstruction of/return to the permanent site, ensuring a smooth, timely transition from recovery (hotsite) to normal (final recovery site) operations.
6. *Post-Disaster Critique & Plan Update* | Develop a plan and conduct a post-disaster critique to evaluate the effectiveness of existing BCP strategies and recovery policies/procedures, updating BCP strategies and documentation, (as deemed necessary), in order to correct problem areas. Replenish/Redistribute updated materials/documentation to all applicable locations/resources.

3.2 | Authorities & Emergency Quorum

Specific actions to be taken following the declaration of a disaster will be at the direction of the **CEO**. In her absence/incapacitation, the officers designated below, in the order-listed and dependent upon availability, will assume leadership until the designated officer or an officer higher on the list is available.

Emergency Chain of Command			Table 3.2a
	Name	Title	Emergency Phone #
01	Annie Arnold	Assistant Manager, Operations	
02	Stephanie Soares	Administrative Assistant	
03	Mark Mathers	Vice Chairperson/Board of Directors	

*Any available officer/senior manager.

In the event of an emergency/disaster of such proportion that the duly-constituted officers of the institution are unable to function, the applicable provisions of the by-laws shall be suspended and the affairs of the institution shall be conducted as herein provided, so far as permitted by law.

- *Assignment of Duties* | The Board may temporarily assign the duties of an officer to another officer and delegate such duties to that person, as it deems necessary.
- *Quorum* | Available members of the Board shall constitute a quorum that has absolute authority during the emergency, according to the provisions in the institution's By-Laws.
- *Quarters* | If the institution's quarters are so damaged as to render them unusable, the Board shall procure temporary offices out of which to conduct the business of the institution until permanent quarters can be obtained and made ready for occupancy.

3.3 | Plan Activation & Scope

Internal Disasters/Emergencies | The following scenario/response pairs address plan activation procedures for emergencies affecting the institution's **Operations Center**.

- Scenario A:* If the entire main building/facility is destroyed and/or inaccessible;
→ **BCP WILL BE INVOKED TO THE FULLEST** | Executive and senior managers will report to the Command Center and operations will be moved to the **Command Center** with the support of the **Remote DP Hotsite/DR Provider**. All **Operations Center** staff and branch personnel will report to their hotsite locations. Currency and negotiable papers will be transferred by armored car from the damaged branch to the **Command Center**. Other branch files that are still intact will be removed and stored at available locations at the discretion of the officer-in-charge. The branch's teller operation will be move to the **Command Center**. Assignments will be made at the discretion of the officer-in-charge.
- Scenario B:* If the **Operations Center** is destroyed and/or inaccessible (DP Hotsite is Available);
→ **MOST OF THE BCP WILL BE INVOKED** | Operations will be moved to the **Command Center** with the support of the **Remote DP Hotsite/DR Provider**. Staff working in affected areas will report to their hotsite locations. Staff working in safe, non-damaged areas will report to their normal work locations.
- Scenario C:* If the **Operations Center** is destroyed and/or inaccessible (DP Hotsite is Unavailable);
→ **PARTS OF THE BCP WILL BE INVOKED** | Components of the plan will be invoked for data processing purposes.

External Disasters/Emergencies | The following scenario/response pairs address plan activation procedures for emergencies affecting external locations and/or resources critical to the institution's functions and operations (e.g. providers of outsourced function/processes, correspondent institutions).

- Scenario A:* If a disaster occurs at the **Core Provider's** facilities,
→ The provider has a viable business continuity plan that will be executed and the service provider will fulfill all legal obligations to the institution according to the provisions set forth in the service contract between the two organizations.
- Scenario B:* If a disaster occurs at the **Items Processing Provider's** facilities,
→ The provider has a viable business continuity plan that will be executed and the service provider will fulfill all legal obligations to the institution according to the provisions set forth in the service contract between the two organizations.