
BUSINESS CONTINUITY PLAN

POLICY AND PROCEDURES MANUAL

October 2005



TABLE OF CONTENTS

SECTION

INTRODUCTION AND OVERVIEW

BASIS OF PLAN

OBJECTIVE

I

I.1

PURPOSE

I.2

POLICY STATEMENT

I.3

STRATEGY

I.4

SCOPE OF THE PLAN

I.5

APPROACH, STAGES, ASSESSMENT AND IMPACT

II

BUSINESS CONTINUITY APPROACH

II.1

BUSINESS CONTINUITY STAGES

II.2

BUSINESS RISK ASSESSMENT

II.3

BUSINESS IMPACT ANALYSIS (BIA)

II.4

BUSINESS CONTINUITY AUTHORITY, RESPONSIBILITY AND DECLARATION

III

AUTHORITY AND RESPONSIBILITY

III.1

DISASTER DECLARATION AND ACTIVATION PROCEDURES

IV

BSP SENIOR MANAGEMENT COORDINATOR

IV.1

PLAN ADMINISTRATOR

IV.2

ALTERNATE PLAN ADMINISTRATOR

IV.3

BUSINESS CONTINUITY TEAM

IV.4

MIS TEAM LEADER

IV.5

AES ACTIVATION PROCEDURES

IV.6

CRISIS MANAGEMENT CENTER (CMC) ACTIVATION PROC.

IV.7

DECLARATION OF OUTAGE LEVEL

IV.8

OFFICIAL DECLARATION FORM

IV.9

BUSINESS CONTINUITY TEAM	V
BUSINESS CONTINUITY TEAM MEMBERS	V.1
COMMUNICATION	VI
VOICE DATA COMMUNICATIONS	VI.1
NOTIFICATION/LOCATION POLICY AND PROCEDURES	VII
SENIOR MANAGEMENT CONTACT LIST	VII.1
NOTIFICATION OF MOHELA EMPLOYEES	VII.2
CALLING TREE	VII.2.a
PERSONNEL NOTIFICATION GUIDELINES	VII.2.b
PERSONNEL LOCATION CONTROL FORM	VII.2.c
MASTER LIST OF MOHELA EMPLOYEES - PHONE NUMBERS AND ADDRESSES	VII.2.d
EMPLOYEE COUNSELING	VII.2.e
NEXTEL PHONE LIST	VII.3
AES MASTER CONTACT LIST	VII.4
LENDER CONTACT LIST	VII.5
GUARANTOR CONTACT LIST	VII.6
VENDOR CONTACT LIST	VII.7
HR - INSURANCE CONTACT LIST	VII.8
ACCOUNTING - INSURANCE CONTACT LIST	VII.9
FINANCIAL CONTACT LIST	VII.10
SAFE DEPOSIT COMPANY CONTACT LIST	VII.11

MIS TEAM & HARDWARE & SOFTWARE RECOVERY PROCEDURES	VIII
MIS TEAM	VIII.1
COMPUTER REQUIRED SYSTEM FOR DISASTER RECOVERY	VIII.2
HARDWARE/ NETWORK COMMUNICATIONS	VIII.3
APPLICATIONS	VIII.4
FACILITIES	VIII.5
DATA PROTECTION	VIII.6
BACKUP AND STORAGE PROCEDURES	VIII.6.a
COMPUTER ROOM SECURITY	VIII.6.b
WORK IN PROCESS	VIII.6.c
SOFTWARE APPLICATIONS	VIII.7
SOFTWARE TO BE INSTALLED AT AES	VIII.7.a
OTHER SOFTWARE APPLICATIONS	VIII.7.b
STANDARD MOHELA WORKSTATION	VIII.8
MOHELA NT SERVER AND WORKSTATION SPECS/FUNCTIONS	VIII.9
BUSINESS CONTINUITY CRITICAL FUNCTIONS AND MARC (Minimum Acceptable Recovery Configuration Summary)	VIII.10
MESA RECOVERY	IX
BUSINESS CONTINUITY PROCEDURES PER BUSINESS UNIT	X
ACCOUNTING	X.1
ACCOUNT MAINTENANCE	X.2
CLAIM SUBMISSION AND RELATED FUNCTIONS	X.3
LOAN ORIGINATION	X.4
ASSET ACQUISITION & CONVERSION	X.5
CALL CENTER	X.6
COLLECTIONS	X.7
SKIPTRACING	X.8

CREDIT DISPUTES	X.9
CUSTOMER SERVICE	X.10
CURE REINSURANCE	X.11
SPECIAL PROMOTIONS	X.12
EOM REPORTS	X.13
EOQ ED FORM 799	X.14
PLATINUM REPORT FACILITY (PRF) REPORTS	X.15
SYSTEM SUPPORT AND DEVELOPMENT	X.16
ADJUSTMENTS	X.17
CONTRACT SERVICES	X.18
PURCHASE PROCEDURES FOR STAFFORD LOANS ON COMPASS	X.19
CONSOLIDATIONS	X.20
SUPPORT SERVICES	X.21
POLICY, COMPLIANCE & AUDIT	X.22
AES SYSTEM MANAGEMENT	X.23
BUSINESS CONTINUITY COMPANIES AND SERVICES	XI
GRAMM-LEACH-BLILEY PRIVACY ACT (GLB)	XII
MOHELA USER GROUPS, USER IDS	XIII
MOHELA QUEUES	XIV
MOHELA CLIENT REPORTS	XV
MASTER LIST FOR MOHELA ARC's FOR LOGGING CORRESPONDENCE	XVI
OTHER ITEMS	XVII
FORMS	XVII.1
IDEM LISTING OF CONSOLIDATORS	XVII.2

TESTING AND MAINTENANCE OF THE PLAN	XVIII
TESTING POLICY	XVIII.1
TESTING PROCEDURES	XVIII.2
TESTING SCHEDULE	XVIII.3
MAINTENANCE POLICY	XVIII.4
MAINTENANCE PROCEDURE	XVIII.5
UPDATE LIST OF BUSINESS CONTINUITY PLANS	XVIII.6
PLAN AUTHORIZATION	XIX

BUSINESS CONTINUITY PLAN POLICY & PROCEDURE MANUAL

INTRODUCTION AND OVERVIEW

The Federal Emergency Management Agency (*FEMA*) describes an emergency as any “unplanned event” that can cause deaths or significant injuries to employees, customers or the public; or that can shut down your business, disrupt operations, cause physical or environmental damage, or threaten the facility's financial standing or public image.

MOHELA's Business Continuity plan addresses the framework by which an unplanned event might be managed in order to minimize the loss of vital resources throughout the company. The life of an employee is the most valuable resource at MOHELA because a life cannot be replaced, therefore, the protection of life is at the forefront of all Business Continuity objectives. Other resources critical to MOHELA include financial, data, fixed asset and clientele.

The Business Continuity plan included herein outlines MOHELA's objectives, approach, responsibilities and procedures in carrying out the plan in the case of an unplanned event (see Section II Approach, Stages, Assessment and Impact). This plan is based on the development, documentation, testing and maintenance of the plan on a continuing basis with the central focal point being MOHELA's agreement/contract with AES (American Education Services). In this respect, MOHELA has contracted with AES to act as an off-site facility and entity that will assume the majority of our critical functions (as outlined in this document) in the event that a disaster occurs at MOHELA.

MOHELA's senior management is responsible for the overall management of the MESA System Business Continuity plan with the assistance of the plan administrator. The actual declaration of the disaster and outage level will be determined and made by a member of senior management at the time of the disaster (see Section IV Business Continuity Authority and Declaration). Senior management will coordinate and oversee the transfer of MOHELA's critical business functions to and from AES with the support of a plan administrator and a Business Continuity Team (see Section IV Business Continuity Team (BCT)). MOHELA's communications to employees, customers and vendors about the disaster will be made according to the procedures outlined in this manual (see Section V Communications and Section VI Notification Policy and Procedures).

The Business Continuity team has been formed to facilitate the Business Continuity plan at each level of activity. Each business function is represented on the Business Continuity Team. The team will implement the Business Continuity plan under the direction of senior management and the plan administrator by ensuring that their respective department procedures are properly discharged during a disaster (see Section IX Business Continuity Procedures Per Business Functions). The team will direct their departments' efforts to the protection of life and to the transfer of their critical functions to and from AES.

In the Business Continuity plan, disasters are categorized in terms of level of outages. Each level of outage is defined as a set number of days in which MOHELA's processes will be disrupted. The level of outages consists of three levels as outlined in Section XII. A level one outage would not require AES to assume MOHELA's critical functions but to assist MOHELA in resuming critical business functions at MOHELA. A level two outage and level three outage would require AES to assume MOHELA critical functions by managing/working MOHELA accounts in the MO region through the procedures set forth in this manual.

MOHELA's overall plan is separated into four stages as follows:

- The first stage consists of the protection, safety and notification of each employee and/or individual.;
- In the second stage, Business Continuity team members will assess the disaster of their business units. The Business Continuity team will then assemble at the Crisis Management Center (CMC) (see subsection IV.7 Crisis Management Center) and report their business unit's assessment to senior management. In this stage, a member of senior management will make a declaration of the disaster with a corresponding outage level;
- The third stage consists of the actual transfer of MOHELA's critical functions to AES. After this transfer, the focus will then turn to the recovery of these critical functions at MOHELA or an alternate location; and
- The fourth and final stage is the review, evaluation and documentation of the previous stages.

For further detail on MOHELA's Business Continuity plan see the plan contents that follow this introduction and overview.

SECTION I – BASIS OF PLAN

I.1. OBJECTIVES

Primary Objective

Protect company assets by minimizing and eliminating, to the point possible, any human, financial, data and customer losses that may occur during a disaster. Enable MOHELA to continue or resume critical business functions immediately following a disaster.

Other Objectives

The plan is designed to:

1. Minimize extent of interruption;
2. Establish and define responsibilities for action during disaster declaration and recovery;
3. Create a recovery team to create, develop, implement and maintain a Business Continuity plan;
4. Establish steps to initiate transition of critical business functions to alternate site(s);
5. Ensure recovery of all MOHELA systems utilizing the plan;
6. Establish plan of action for acquiring necessary equipment and supplies for use during recovery;
7. Establish contact lists to ensure quick and effective implementation of the recovery plan; and
8. Establish procedures for testing and maintenance of plan.

The MOHELA Business Continuity plan is designed to recover business units from any unplanned event that affects normal processing. The plan documents recovery strategies include the necessary technological and human resources required for minimal recovery of our *critical functions*. The plan is also designed around the worst case scenario, which is the complete loss of facility.

The plan's alternate processing site is designated as AES, our business continuity business partner. An agreement/contract has been established with AES, who will provide space and resources to assume the processing of the critical functions on behalf of MOHELA (see agreement/contract excerpt on Business Continuity Plan at Appendix C of this document). Upon notification of a disaster, AES will immediately begin working MOHELA accounts in the MO region. In a level two or three disaster as outlined in this plan, MOHELA critical functions will be transferred to AES for processing.

In the case of the recovery of operations from AES, MOHELA will reestablish operations at its current facilities. If the facility is completely destroyed, then operations will remain at AES until the facility is rebuilt or replaced by a leased or purchased space in the St. Louis metropolitan area. This includes replacement of all hardware, office equipment, furniture and data/phone lines.

Assumptions

The Business Continuity plans have been developed based upon the following assumptions:

- Only business unit facilities have been disabled by the disruption; pre-designated alternate sites are unaffected (i.e., AES);
- Off-site storage locations for critical backup files and information are intact and accessible (SDC);

- Qualified personnel in sufficient quantities are available to perform Business Continuity responsibilities;
- Business continuity is performed in accordance with the procedures that have been set forth within this Business Continuity plan;
- The telecommunications and recovery strategies are fully implemented;
- The recovery plan is available, in-place and successfully tested;
- External organizations, such as customers, vendors, government agencies and others, will be reasonably cooperative during the business recovery period;
- Plan review, maintenance, and updates are performed on a regular basis to ensure a viable state of readiness; and
- Business Continuity awareness is prevalent in the company.

I.2. PURPOSE

The primary purpose of the Business Continuity plan is to efficiently and effectively perform the following items if a disaster were to occur:

1. Meet the immediate needs for safeguarding company assets such as the physical safety and mental well being of human life;
2. Establish and resume critical functions as quickly as possible by providing an alternate-processing site that will include sufficient resources and space (AES); and
3. The reestablishment of critical functions by MOHELA either at the current or replacement facilities.

I.3. POLICY STATEMENT

MOHELA's Business Continuity plan has been developed to protect MOHELA resources, specifically human, through an organized response to any unplanned event and to provide methodology for resuming and recovering critical business activities in such an event.

I.4. STRATEGY

The Business Continuity plan does not address specific disaster scenarios. However, this plan addresses immediate, short-term and long-term recovery strategies that encompass any type of event. The MOHELA strategies for a disaster situation are to:

1. Ensure that all human resources are protected and accounted for at the time of an unplanned event;
2. Assess the critical functions of the organization at the business unit level and develop guidelines for resumption of those functions;
3. Ensure that all critical software and data are backed up and stored in an off-site location for access and use during recovery;

4. Publish a plan manual outlining the steps to take during a disaster;
5. Provide a method for testing the plan on an annual basis to better ensure its viability during a real disaster; and
6. Establish a maintenance schedule to update the plan as needed, due to technology, system or business function changes.

Information Systems Strategies

Voice Communications

- Voice communication vendors will be immediately contacted for recovery support;
- Incoming main and toll-free numbers will be re-routed to the vendors' voice messaging system immediately following service interruption; and
- Business units critically dependent upon voice communications (e.g. customer service groups) will be kept informed of the situation.

Computer Systems / External Data Services

- Critical vendors (e.g. recovery facility, off-site storage) will be contacted and placed on alert status;
- Hardware and software vendors will be contacted for recovery support, as necessary; and
- Where applicable, business units will be informed to implement manual processing procedures, until service is restored.

Business Unit Strategies

Ensure the overall well-being of each business units' personnel involved in the disaster.

Outage level I: 5 days

- Manual backup procedures will be implemented until service is restored;
- Hard copy reports and data will be utilized until service is restored;
- Work requiring system data will be back-logged; and
- External and internal entities will be notified of any processing delays, if necessary.

Outage level II & III: 6 – 30 days and greater than 30 days

- All critical activities of each business unit will be transferred to AES;
- Selected business unit personnel may be re-located to an *alternate recovery location*, as directed by the business unit recovery team leader, to resume critical business unit functions;
- Business unit personnel will notify clients, organizational groups and/or vendors, as required, utilizing available resources (e.g. cell phones, e-mail, etc.); and

- Key contacts will be provided status updates, as necessary, and will be informed of any processing changes or delays.

I.5. SCOPE OF THE PLAN

Although no plan can identify all potential disasters, MOHELA's Business Continuity plan has been established using the following potential scenarios:

1. Incidents involving physical damage to our building or specific work areas such as fire, smoke, water damage or bomb threat;
2. Potential or unexpected regional disasters such as tornadoes or flooding;
3. Incidents affecting a local or regional area such as snow storms, closure of major access roads, emergency building evacuation or other threats to the building such as a fire at a nearby building; and
4. Loss of public utilities such as electric, telecommunications or water supply; and loss of computer processing capability due to external or internal (human error or sabotage) failures.

SECTION II - APPROACH, STAGES, ASSESSMENT AND IMPACT

II.1. BUSINESS CONTINUITY APPROACH

MOHELA's approach to business continuity is based on our agreement with our major business partner Pennsylvania Higher Education Assistance Authority (AES).

An agreement has been made with the Pennsylvania Higher Education Assistance Agency (AES) to provide an alternate site and resources to assist MOHELA in its business recovery process. The AES site from where MOHELA's critical business functions will operate is located in Harrisburg, Pennsylvania. This site will provide processing capability immediately upon notification of the disaster by the proper MOHELA personnel as outlined in this document.

As AES owns and uses the AES COMPASS system, the AES site will provide student loan employees with expertise to take over the designated business functions. MOHELA Business Continuity Team members will assist AES in the transition of our critical functions to AES. AES will carry out MOHELA's critical functions by working MOHELA accounts in the MO region using user IDs created by AES at the time of the disaster. These user IDs will mimic AES personnel in the various business functions as to access and functionality. Those IDs will be patterned as MOBR for MOHELA Business Recovery. AES will work MOHELA accounts, using these newly created IDs, according to their own operational procedures, MOHELA's Business Continuity procedures (set-forth in this document) and according to MOHELA's direction. If necessary MOHELA will provide employees to assist in performing critical business functions as if they were working in MOHELA's primary facility.

The method implemented to create and maintain the Business Continuity plan utilizes the following steps:

1. Developing ;
2. Writing;
3. Implementing;
4. Testing;
5. Managing ; and
6. Maintaining.

II.2. BUSINESS CONTINUITY STAGES

MOHELA's Business Continuity plan implements the following stages during the occurrence of an unplanned event.

Stage 1: The protection, safety and notification of each employee and/or individual at MOHELA. Note: Business Continuity Team members (see Section V Business Continuity Team) are responsible for this phase of their business function.

Stage 2: The BC team members will assess the damages in their own business unit following the disaster;

The team will assemble at the Crisis Management Center at MOHELA or at a designated off- site location;

The BCT will report their assessment of the damages to the plan administrator and or to the senior management member in charge of disaster;

A senior management member will declare a disaster along with the corresponding outage level per his or her signature on the official disaster declaration form (see Subsection IV.9); and

The BC plan will be activated and managed by senior management with the assistance of the plan administrator, AES liaisons and Business Continuity team members.

Stage 3: MOHELA critical operations will be transferred to AES for processing, if the plan is activated at a level two or three (iv.8. Declaration of Outage Level). Each Business Continuity team member will be responsible for ensuring their business critical functions are properly assumed by AES; and

Once critical operations are assumed by AES, Business Continuity team members' attention will begin to recover critical operations at MOHELA's primary or alternate site.

Stage 4: Review, evaluation and documentation of the previous stages will occur after critical operations have been restored to MOHELA. The evaluation will consist of an examination of resources, cost and the overall effectiveness and efficiency of the plan.

Day Specific Timeline

The goal of the plan is to resume the majority of critical processes, at the minimum, by the beginning of *the third business day* following the incident. This can be achieved by utilizing the AES site in Pennsylvania.

Day One: Protect, locate and notify MOHELA employees.

Day Two: Assess the disaster situation; declare the disaster and outage level. Notify AES and other business continuity partners of the incident and mobilize employees as needed. Begin putting resources in place and transferring critical operations to AES. Communicate the situation to all business associates (i.e. lenders, schools, guarantors, insurance providers).

Day Three: Ensure all critical operating processes are properly in place and functioning.

II.3. BUSINESS RISK ASSESSMENT

Disasters have been classified into five groups: Natural, Neighborhood Human, Environmental, Business & Political risks. Listed in these groups are potential risks for MOHELA and its employees:

Natural Risks

Earthquake – Madrid Fault
Floods - Flood Plain, Missouri River
Tornadoes
Snow & Ice Storms
Lightning
Heavy Winds

Neighborhood Risks

Airport – Next to Spirit of St. Louis Airport
Major Freeway - Freeway – I60

Human Risks

Violence in the workplace
Sabotage
Bomb Threats
Embezzlement/Fraud

Environmental Risks

Hazardous material spill – Freeway
Mold Environment
Community Health Risks

Business Risks

PHEAA and PHEAA COMPASS System Failure
Loss of Key Employees and of Senior Management Personnel

Political Risks

Reputation
Goodwill
Legislative Environment

These risks could result in the loss of human life, financial loss or increment (including lost productivity), the loss of critical data and the loss or impairment of our relationship with customers. The primary concern and risk involved with any disaster is the loss of human life. No individual should risk injury to themselves in an attempt to recover or guard against other business assets.

The primary losses or operational issues by department if a disaster were to occur are as follows:

Account Maintenance & Claims: Potential loss of loan guarantees, inability to communicate with customers, guarantors, etc.;

Customer Service: Inability to receive or make calls and perform the necessary due diligence requirements;

Conversions: Inability to purchase from or service loans for MOHELA lenders;

Loan Origination: Inability to disburse loans to schools and borrowers;

Consolidation: Inability to originate and process loans;

Accounting Inability to process payments, pay bills and the potential loss of accounting records;

MIS: Loss of critical loan, accounting and management data and document images;

HR: Payroll and benefit administration delay or error; the loss of employment records;

Cash Loans: Loss of guarantee; due diligence and servicing issues;

Contract Services: Inability to communicate and meet lender demands and requirements; and

Support Services: Loss of critical mail; inability to process critical correspondence.

The failure of PHEAA and/or of its COMPASS system could cause major data loss and an incapability to continue on as an entity if the PHEAA Company or COMPASS system does not continue on as viable corporation or system. MOHELA has thus required per its contract with PHEAA to provide automated systems and procedural controls to maintain integrity of MOHELA data. PHEAA is required to have a business continuity plan that can regenerate any lost, erased or destroyed data within 72 hours of the disaster. The contract also requires physical security of computer and record systems. If a disaster were to occur that would require PHEAA to relocate to a hot site they must be able to resume operations and services to MOHELA as stipulated in the contract within 72 hours. The contract excerpt that speaks to Disaster Recovery and Backup in the contract with PHEAA is as follows:

Disaster Recovery and Backup. PHEAA shall provide automated system and procedural controls to verify and maintain the integrity of MOHELA data. PHEAA shall promptly regenerate any lost, erased or destroyed data within seventy-two (72) hours. PHEAA shall provide for the physical security of its computer processing and record retention systems and shall maintain a comprehensive disaster recovery plan. The plan shall provide for the computer processing and record retention systems used to provide services hereunder and standards for the resumption of services set forth in this Agreement in the event of a disruption in service. In the event of a declared

emergency where PHEAA's computer operations must be relocated to the PHEAA disaster recovery hot site, operations shall be resumed within seventy-two (72) hours.

II.4. BUSINESS IMPACT ANALYSIS – (BIA)

The following steps were used to conduct the analysis:

1. All business units participated in the BIA;
2. Standard questions were developed to ask each department (allowing room for specific business unit issues). Questions focused on the critical functions of their business units, the impact the lack of resources would have on those functions and the MARC (Minimum Acceptable Recovery Configuration) items and timelines for recovery;
3. BIA surveys were conducted in person with each department;
4. A business function priority list was produced identifying all business units, critical business functions, and the associated recovery timelines; and
5. A MARC summary report was produced identifying all business unit resources needed to perform the above business functions during a recovery situation.

Measurement Categories

Both tangible and intangible impacts from a disaster were gathered. Where actual impacts could not be quantified, subjective terms were used to represent the severity of the impact. Intangible impacts, such as customer service impacts, were also identified in subjective terms.

Business impacts were assessed by time. These time categories are important because of the possible recovery strategies that it may require. Impacts were categorized into the eight timelines as follows:

- **Day 1 (Immediate)**
- **Day 2**
- **Day 3**
- **Day 3 - 5**
- **Day 5**
- **Day 5 - 10**
- **Day 10**
- **Day 30**

Impacts - Preparedness

MOHELA's ability to mitigate the impacts of a disaster will be dependent upon the effective response of its people at the time of the disaster, the survival of essential information resources, and the availability of alternate physical resources (e.g., equipment and facilities) required to sustain critical business operations.

The following summarizes the level of preparedness information gathered from the business impact surveys:

1. The level of awareness and preparedness was fairly low throughout all MOHELA business units. The MIS area has taken steps to document, maintain and provide back up resources for recovery of data and computer systems. This analysis indicates that resumption of critical business functions (operations) has been neglected in the area of disaster recovery planning;
2. A service interruption to critical computer systems and voice communications would cause serious delays to most departments, rendering MOHELA services inadequate to meet regulatory and contractual obligations; and
 - a) Every business unit stated it depends on telephone services and computer data application services for approximately 90% of its daily operations. These services are critical to business resumption and to successful, long-term recovery.
 - b) Most departments could operate without computing services, or cease operations for up to 2-5 days. However, interruptions beyond 5 days will likely cause workflow to be unmanageable, resulting in idle staff and significant impacts to production and regulatory compliance.
3. Most business units felt confident in MOHELA's ability to turn many of the critical functions over to AES for processing until the recovery process was stabilized. More detail regarding this can be found later in this recovery plan document.

Analysis and Recommendations

Recovery Timing Requirements

Each department was asked to identify whether or not serious business impacts would occur during a disaster, necessitating the rapid resumption of critical business functions. Most departments identified one or more business functions that are classified as needing restoration within five (5) days of a service interruption. Many departments expect serious financial, regulatory or contractual impacts to occur if restoration is not accomplished within this time frame. A few areas did not report any short-term urgent recovery requirements. However, several of these areas indicated their services would be required in a recovery support role to assist other, more time sensitive areas.

Responses to the Business Impact Analysis were analyzed and summarized into critical business functions. These critical business functions and the resources required to accomplish them were classified into one of these timelines for resumption:

- **Day 1 (Immediate)**
- **Day 2**
- **Day 3**
- **Day 3 - 5**
- **Day 5**
- **Day 5 - 10**
- **Day 10**
- **Day 30**

The deciding criteria for categorizing the critical business functions was related to revenue loss, regulatory compliance or customer service issues.

The critical business function priority list shows the reported business recovery timings and the recommended restoration priority. Departments that identified immediate recovery requirements are:

Department	Function
MIS	Data Restoration
MIS	Data Center (Hardware) Restoration
MIS	Phone line restoration and/or disaster notification message

Minimum Acceptable Recovery Configuration (MARC)

Departments were asked to provide an estimate of the level of resources required for them to resume essential business operations following a disaster declaration. Refer to the MARC summary report at Subsection VIII.10 for a comprehensive listing of all MARC resources required by each business unit over each resumption timeline.

Conclusions and Recommendations

Detailed Business Continuity Plans should be designed, documented, and implemented for each MOHELA business unit (see IX – Business Continuity Procedures per Business Function.).

The resulting plans will need to:

1. Identify corporate resumption priorities by department and function;
2. Identify recovery strategies, including telecommunications and record re-creation;
3. Identify recovery response participation;
4. Identify alternate operating facilities;
5. Identify tasks and activities necessary to resume business functions;
6. Validate recovery strategies which call for the transfer of responsibilities from the affected location to an alternate operating location;
7. Document minimum recovery resources such as terminals, personal computers, data lines, staffing requirements, facility requirements, and vital records; and
8. Include a business recovery testing methodology and maintenance program.

A documented and tested Business Continuity plan will reduce the duration and severity of a service interruption, and consequently, reduce the magnitude of the business impacts. It will also enhance coordination among the various business units. The analysis findings indicate that an immediate and efficient restoration operation would minimize these impacts.

VIII.10. BUSINESS CONTINUITY CRITICAL FUNCTIONS AND MARC (Minimum Acceptable Recovery Configuration Summary)

This section identifies MOHELA’s critical department functions, the resumption timeline for each function, the recovery location and the anticipated number of people needed to assist in the recovery efforts. The level of recovery will be dependent upon the disaster situation itself and a timeline for such recovery will be assessed following the incident. 100% recovery is completely dependent on the specifics of the disaster. In the event of a disaster, the following functions and resources will be restored following the procedures established in this Business Continuity Plan.

Business Unit	Critical Function	Resumption Timeline	Recovery Location	Potential People Needed at Recovery Location	Comments
Accounting	Loan Origination	Day 3	AES	1	Bring check stock to AES
Accounting	Payment Processing	Day 5	AES	1	
Accounting	General Ledger	Day 3-5	AES	3	AES
Accounting	Accounts Payable	Day 10	AES	1	
CASH Loans	Phone Servicing	Day 3	To be determined		See IX MESA Recovery below.
CASH Loans	Origination/Disbursemen	Day 5	To be determined		See IX MESA Recovery below.
CASH Loans	Due Diligence	Day 10	To be determined		See IX MESA Recovery below.
Claims/Cures	Claims Review and Filing	Day 3	AES	1	
Claims/Cures	Due Diligence	Day 5	AES	1	
Contract Services	Cancellations & Refunds	Day 3	AES	2	AES
Contract Services	Lender Reconciliation's	Day 3-5	AES	above	AES
Contract Services	Lender Reporting	Day 3-5	AES	above	AES
Contract Services	Loan Sales	Day 30	AES	above	AES
Conversions & Acquisitions	Imaging & Indexing	Day 3	To be determined	2	Critical documents to scan: LO applications, CASH Loan Applications and correspondence, LO and LM correspondence. Copy and send copies to AES to be worked.
Conversions & Acquisitions	Loan Input/Rosters/Collateral	Day 10	AES	2	AES
Customer Service	Phone Servicing	Day 3	AES		
Customer Service	Bank of America Servicing	Day 3	BOA take back		
Customer Service	Collection Campaigns	Day 3	AES	1	
Account Maintenance	Status and EGD Chgs	Day 3-5	AES	1	AES
GAR	Account Research	Day 30	AES		AES
Human Resources	Professional Counseling	Immediate	Provident Counseling	1	

Business Unit	Critical Function	Resumption Timeline	Recovery Location	Potential of People Needed at Recovery Location	Comments
Human Resources	Retrieve pertinent employee data	Immediate	AES	1	Access to ADP/Report Smith at AES
Human Resources	Payroll	Day 3-5	ADP	1	Depends on date in payroll cycle
Human Resources	Benefits Administration	Day 5	AES	1	Access to ADP/Report Smith at AES
Human Resources	Recruitment/Temp Employees	Day 10	AES		Coordinate staffing level needs
Loan Consolidation	Application Processing	Day 30	To be determined		
Loan Maintenance	OSD, Deferment & Forbearance Processing	Day 3-5	AES	1	AES
Loan Origination	Disbursements & Request for Funds	Day 3	AES	2	Need all guarantor and Request for Funds software.
Loan Origination and Others	GLB	Day 3	AES		See LO business unit procedures in Section X.
PCA	System & Regs Support for Recovery Staff	Day 5-10	To be determined		Staff will go where needed in support role.
Skiptracing/Credit	Log Return Mail Data	Day 3-5	AES	1	AES
Skiptracing/Credit	Skiptracing	Day 5-10	AES	1	
Skiptracing/Credit	Credit	Day 5-10	AES	1	
Support Services	Open & Sort Incoming Mail	Day 2	AES		Overnight payments to AES.
Support Services	Print & Mail Delinquency Letters	Day 3	AES	1	
Support Services	Print & Mail Bills	Day 5-10	AES	1	