

Return To	Kelly L'Heureux 203-598-0883 <a href="mailto:kellyl@mmtonline.com">kellyl@mmtonline.com</a>
Date Issued	March 8, 2004
Return By	March 19, 2004

BIA02 – Business Impact Analysis  
**BIA Worksheet (IT)**

*This worksheet is designed specifically to cover the institution's IT function(s). When completing the IT-BIA, participant(s) should take into consideration specific departmental requirements as well as those of the institution as a whole, as detailed in all completed departmental BIAs.*

In accordance with federal regulations, the institution is conducting a Business Impact Analysis (BIA). As the foundation of any disaster recovery/business continuity strategy, the BIA aims to assess the criticality of the functions, operations, products, and services of each department, including the internal and external resources required to support them. It is also designed to identify all mission critical locations, personnel, vendors, equipment, software, communications, servers, forms/supplies, and reports/documents/files in order to ascertain the potential impact on the institution (financial or otherwise) should any disruption of operations occur. Impact should be thought of in terms of loss of revenue, reduced demand, loss of staff, decreased productivity, financial penalties, loss of opportunities, etc. Additional goals include:

- Identifying the resources and personnel most critical in supporting business processes
- Understanding the possible financial and intangible impacts of an extended disruption of operations
- Defining a recovery window upon which to design priority sequences for systems restoration
- Creating strategies to minimize/mitigate identified risks
- Providing overall direction in defining recovery resource requirements and development of practical business continuity plan

In order to meet the objectives of the BIA, selected personnel have been asked to complete the following questionnaire. As instructed on the following pages, please provide the requested information and refer to mission critical materials/documentation/services that you believe may be a vital to your department's disaster recovery needs (e.g. schematic/configuration diagrams, manual/emergency operating procedures).

**Check the following statement and return completed surveys to the BCP Manager within two (2) weeks of receipt. Direct all questions/comments to contact listed in table at the top of this page.**

<b>"I have read the above statement and exercised due diligence in completing this BIA &amp; providing the requested materials."</b>				<i>Initial &amp; Date</i>	
<i>Department Name</i>	Information Systems	<i>Full Address</i>	123 Main St., Springfield, CT	<i>Floor</i>	1
<i>Completed By (Name/Title)</i>	Joseph Jacobs, CIO			<i>Date of Completion</i>	May 31, 2004
<i>Signature</i>					
<i>Additional Resources Consulted</i>	Brain Brothers, Computer Operator/Programmer Kelly L'Heureux, BCP Consultant (MM&T, INCorporated)				
<i>Recovery Team Name</i>	IT TEAM				
<i>Hotsite Locations (Name/Address)</i>	Town Branch, Floating hotsite support				

## 1. Functions, Products & Services

Define and describe all mission critical functions, products, and services for which your department is involved and/or responsible.

**Table 1**

List the functions, products, and services related to your department.	Describe department's role in processing/operations of the function/product/service.	Criticality/Priority (T) Top (H) High (M) Medium (L) Low	Estimate allowable downtime before loss/disruption of function/product/service creates negative:	
			Operational Impact	Customer Impact
EQISYS Support	Provide 24x7 end-user/vendor support for all EQISYS (core DP system) hardware/software system availability, maintenance, and upgrades.	T	7 days	n/a
Online Systems Support	Monitor, maintain, and provide support for online systems, including: Fiserv ATM, Bill Payment, Voice Response, Home Banking, Liberty, Credit Reporting, Certegy	H	7 days	n/a
Networking Support	Maintain, administer, and provide 24x7 hardware/software support for LAN/WAN	T	7 days	n/a
LAN/WAN Security	Install/maintain security patches and upgrades for all software, maintain server/client PCs using SUS and virus protection	H	30 days	30 days
In-house Applications	Maintain/develop internal programs used for daily operations of EQISYS system	H	1 day	1 day
Third Party Vendors	Develop, maintain, transmit data to 3 <sup>rd</sup> party vendors	M	7 days	7 days
Critical Data Backups	Ensure backups are performed and verified on a regular basis	T	7 days	7 days
Operating Procedures	Maintain and develop IT-related docs/procedures	L	n/a	n/a
User Support	Provide end-user support for all 3 <sup>rd</sup> party software/hardware and any issues arising with end-user functionality	H	7 days	7 days

## 2. General Department Impact Assessment

Provide the requested information for your department and ascertain the impact that a loss/interruption of mission critical functions (listed in "Section 1") may have on the ability to satisfy customer demand as well as internal (board) and external (regulatory compliance) requirements.

**Table 2**

Question	Y/N	Answer/Description
Does your dept. have established evacuation procedures? (Indicate what and where procedures exist or explain evacuation process)	Y	Staff has been instructed regarding the location of all exits.
Does your dept. have written operating procedures for processing/functions under normal conditions? (Indicate what and where procedures exist or explain why do not exist)	Y	Departmental procedures are kept on the S:// Drive.
Does your dept. have written emergency/manual operating procedures for processing and operating under emergency conditions? (Explain/attach copies or complete <a href="#">WS1-Manual Operations</a> ).	Y	<a href="#">WS1-Manual Operations</a>
Does the dept. or institution have provisions and/or arrangements for emotional support and family care needs in the event of an emergency (Explain/refer to existing documentation)	N	n/a – Handled by BCP Management Team
Use <a href="#">WS2-Financial Analysis</a> to estimate the financial impact on the dept/institution due to reduced capacity during an emergency.	n/a	<a href="#">WS2-Financial Analysis</a>
Is there any potential impact from common recovery sites serving multiple lines of business, departments, or other institutions?	Y	Disruption to member service.

### 3. Personnel Support

List the mission critical internal personnel required to perform the functions/operations of the department in the event of a loss/interruption of normal operations. At a minimum, assign at least one (1) staff member for each of the following resources, using the abbreviations below to complete the Team Function field. If unsure of the designations and responsibilities, leave the field(s) blank and the BCP Manager can help you define these roles.

*Team Functions*

- Team Leader (TL)** Oversees departmental recovery operations and acts a liaison between team and BCP Manager.
- Assistant Team Leader (AL)** Provides support to and will assume role of "Team Leader" in the event of his/her incapacitation or unavailability.
- Team Member (TM)** Provides support to and carries out the directives of the Team and/or Assistant Team Leaders
- Backup/Alternate Member (BM)** Trained to assume any team position/function in the event that required personnel are not available.  
*\*When sufficient resources are available, team members should not double as backup/alternate team members.*

**Table 3**

Resource(Name/Title)	Roles & Responsibilities	Team Function	Is this resource required @ hotsite?
			No = 0   Yes = 1
Joseph Jacobs, CIO	Overall responsibility for previously described functions, products, services	TL	1
Brain Brothers	Backup to Team Leader, Support Team Leader (as required)	BM	1
<b>Total # Required</b>			<b>2</b>

**\*When finished\***  
 Move mouse to "Total" #.  
 Right click.  
 Select "Update Field".

#### 4. Vendors/External Support

List the specific vendors/external resources that are mission critical to the overall operation of both the **IT Department and the institution as a whole**, describing primary services/products provided and criticality in the event of a loss/interruption of normal operations.

**Table 4**

Vendor/External Resource	Primary Service/Product Provided	Criticality/Priority
		(T) Top (H) High (M) Medium (L) Low
TransUnion	Credit reporting	M
Equisys	Core processing	T
Constitution State Corporate Credit Union	Item processing support	T
Magee Company	Coin Counters, Checkwriters	L
Neopost	Postage Meter	L
Jack Henry	Core application/service provider	T
CSCCU	Items processing support	T
Hewlett-Packard	Hardware provider/servicer	M
CT Communications (CTC)	Communications support	M
IBM	Hardware provider/servicer	M
IKON	Copiers	M
Dell	Hardware provider/servicer	M
Americomm	Statement printing, e-Statements	H
CENTURION	DR Remote Recovery Center	T
PageNet	Pagers	M
CISCO Systems	Routers	M
Garrison Technologies	Firewall	H
Microsoft	Software provider/support	M
SBC	Main telecommunications provider	T
CyberGuard	Firewall	H
GFI USA	Email security	H
Sun Microsystems	MCW Software	M
EQISYS	Core application	T
Surf Control	Web security	H
Iron Mountain	Records storage	M
PhoneTel	Communications devices/hardware	M
SecureWorks	Internet security	H
VeriSign	Website encryption	H
Cannon USA	Hardware provider	M
Conversent Communications	Backup phone/Internet lines	M

Online Resources	BillPay provider	M
Carrington Company	Postage meter	L
Fiserv ATM	ATM provider	H

## 5. Equipment

Provide the requested information about the mission critical equipment required to make departmental/institution hotsite locations functional in the event of an interruption/loss of IT capabilities. Ensure that requirements defined in all departmental BIA's are taken into consideration when determining the entire institution's hotsite needs.

- Notes:** Use generic terms in the Type/Name field (e.g. Standard PC, Network Printer, Copier).  
 Use specific descriptions in the Model field (e.g. Dell 4500, HP 4600 LaserJet, Xerox CopyCentre C35 Digital Copier).  
Vendor indicates the vendor from which the item was purchased (e.g. Staples, CompUSA, Dell).  
Serviced By indicates the vendor which services the item (e.g. In-house, Dell [under warranty], CT Computer Repairs).

**Table 5**

Type/Name	Model	Vendor (If Known)	Serviced By (If different from "Vendor")	Criticality/Priority
				(T) Top (H) High (M) Medium (L) Low
Tape Drive	IBM 7207			H
Tape Drive	IBM 8mm			H
Dial-up Modems				T
T1 Circuits				M
Cisco Router		Fiserv		H
Corporate Laptop	Dell – Used to establish connectivity to CENTURION Remote Recovery Center, stored offsite at CIO's home	Dell	Dell	T

## 6. Software/Applications

Provide the requested information about the mission critical software/applications required to make departmental/institution hot site locations functional in the event of an interruption/loss of IT capabilities. Ensure that requirements defined in all departmental BIA's are taken into consideration when determining the entire institution's hot site needs.

**Notes:** Use generic terms in the Title field (e.g. Microsoft Office, Acrobat Reader, WinZip).

Use specific descriptions in the Version field (e.g. XP-SP3, 6.0, 9.0-6028).

Vendor indicates the vendor from which the item was purchased (e.g. Microsoft, CompUSA, In-house).

Serviced By indicates the vendor which services/supports the item (e.g. Microsoft [under license], CT Software, In-house).

**Table 6**

Title	Version	Vendor (If Known)	Serviced By (If different from "Vendor")	Criticality/Priority
				(T) Top (H) High (M) Medium (L) Low
PGP encryption	Current			H
Veritas Software (Backups)	Current			H
EQISYS	Current			T
MS Windows/Office	Current			T
Internet connection software	Current			T

## 7. Communications Support (Networking)

Provide the requested information about the mission critical networking and communications lines/devices required to make departmental/institution hot-site locations functional in the event of an interruption/loss of IT capabilities. Ensure that requirements defined in all departmental BIA's are taken into consideration when determining the entire institution's hot-site needs.

**Notes:** If the institution has an outsourced hot-site provider, the information provided and the provider's contract must correspond with one another. This section should also include requirements for additional hot-site locations (e.g. branch locations, leased office space) that will require network/communications support in order to be functional.

**Table 7**

Question	Y/N	Answer/Description	Criticality/Priority
			(T) Top (H) High (M) Medium (L) Low
Do IT and other required institution functions require LAN/WAN (or other) connections?	Y	All end-users connect to the core DP systems through the LAN/WAN	H
<i>If you answered "NO" above, proceed to the next page. If you answered "YES", complete the following.</i>			
If applicable, list required connections (e.g. voice, data, mobile).	Y	Access to EQISYS connecting first to MUFUS1 and then to the RISC 6000	T
If applicable, indicate communications device/lines required to support connections.	Y	TCP/IP protocol for both LAN/WAN w/ remote locations using T1 digital circuits	H
Are any PC/CRTs connected to LAN/WAN? List and describe method(s) of connection.	Y	Approximately 50 PCs using TCP/IP 10/100	M/H
Are any printers connected to LAN/WAN? List and describe method(s) of connection.	Y	Approximately 25 using TCP/IP 10/100	M/H
Is there any additional hardware required to connect/interface with LAN/WAN?	Y	CISCO 1720 Router and AdTran CSU/DSU's	H
Is there any specialized software required to connect/interface with LAN/WAN?	N		n/a
Describe department role in the backup of specific LAN/WAN resources (if any).	N/A	IT handles all monitoring and maintenance on a daily basis	n/a
Are there any operational/security controls to be implemented prior to restoration of LAN/WAN connection?	N	With possible exception to work with SBC who provides support for physical circuits.	n/a





**10. Reports/Documents/Files**

Provide the requested information about the IT-related reports, documents, and files required to perform the specific function(s) of the department and/or institution, including all specialized, mission critical items. Items that are not-specific to the department but used throughout the organization (e.g. absentee log spreadsheets, employee manuals, benefits booklet) are not required below and will be covered in a separate BIA for "Support Services".

- Notes:** Include all mission critical core and ancillary applications required at the hot site.  
 Use the abbreviations included in the Type field to indicate the primary format of the item (e.g. electronic, imaged, hardcopy).  
 Use the Source field to indicate the storage location of the item (e.g. Network Server – G://Accounting, Main Branch Vault, @ Hotsite).  
 You may group items by type of file (e.g. Accounting Files, Marketing Files, Nightly Backups, Monthly/Quarterly Backups)

**Table 10**

<i>Report/Document/File Name</i>	<i>Type</i>	<i>Source/Location</i>	<i>Criticality/Priority</i>
	(H) Hardcopy (E) Electronic (M) Microfilm (C) CD-ROM (T) Tape (O) Other		(T) Top (H) High (M) Medium (L) Low
IT Docs (ALL)	E	Stored and maintained on network server	T

## 11. File Backup & Restoration

Provide the requested information about the methods and materials used to backup up the mission critical systems, applications, files/data, reports, and documentation, including those related specifically to the IT department (e.g. network usage, systems performance, user password/account data) as well as those covering backup of data for multiple user departments (e.g. departmental file servers, proprietary systems data, institution applications data, software programs for restoration). Be as detailed as possible.

Table 11

Question	Answer/Description	Criticality/Priority
		(T) Top (H) High (M) Medium (L) Low
What systems/files/data required backup?	EQISYS, Network Server, OTG, ERMserver, Jukebox, Voice Response, MCW	T
What specific hardware/software is used to perform backup (if any)?	Veritas, IBM 7207 tape drive, IBM 8mm tape drive	T
How often are backups performed?	Daily	n/a
What type(s) of electronic storage media are used to for backups?	HP C5141F ½", Imation 1.2 SLR, HP C5718A, Sony 170ME 8mm, HP C7983A	n/a
Where are copies of the backups stored?	Offsite in a fireproof box located at CIO home	n/a
How often are the backups rotated at the storage site(s)?	Daily	n/a
What resource(s) are involved in/responsible for the execution and storage of backups?	Software programs are scheduled on a daily basis to automatically backup required data	n/a
If using backups to restore systems, would files need to be brought current? If yes, how long would it take?	No	n/a

## **12. Cross-Training Programs**

If applicable, describe employee cross-training programs provided by the department, including training for back-up personnel in the event that key personnel are inaccessible/unavailable.

---

None.

## **13. Additional Information**

Use the space below to provide any additional/pertinent details regarding the operations and resource requirements of your department/function.

---

None.

**WS1-Manual Operations**

*\*If your department has already developed and maintains “manual” or “emergency operating procedures” in a separate document, you should have already indicated this in “Section II” and DO NOT need to complete this worksheet.*

In the event that systems/connectivity support for required functions/products/service is inaccessible/unavailable, manual processing may be required until systems and/or connectivity are restored. Use the following table to provide the information about manual workarounds/tasks and the amount of time they can be used before downtime begins to negatively impact institution operations.

**Worksheet 1**

<i>Describe Manual Workarounds/Procedure (Include any supporting documentation for manual operations)</i>	<i>Maximum Allowable Time w/o Systems Support</i>
If the EQISYS (core processing system) were unavailable, the credit union would be forced to log transactions manually until system availability returned. A trial balance is created on a daily basis and the output is stored on the Optical system. This report can then be transferred to individual locations and staff would have hardcopies available to check on availability of funds prior to transaction processing.	3 DAYS

<< [BACK TO “2. General Department Impact Analysis”](#)

