

# Business Continuity Planning

## Creating a Business Continuity Plan

Creating an effective Business Continuity Plan is a long, ever changing process. The plan itself must fit a credit union’s own unique needs (there is no single one size fits all). When developing a business continuity plan, it is always recommended that any credit union follow the process recommended by the FFIEC. The basic framework for this process is:

* **Step 1:** Assess your risks. Should you be preparing for a wildfire? Or a Tornado?
* **Step 2:** Perform a Business Impact Analysis. Identify all of your functions (all the things you do), how long you can be without them, how much data you can afford to lose, and your backup plan you will use until the function is recovered.
* **Step 3:** Build out your Business Continuity Plan (attached is a sample template)
* **Step 4:** Train your staff on the plan. Without training, plans simple become a binder that gathers dust.
* **Step 5:** Test your plan. Perform system tests to confirm your back up process are working. Perform a tabletop test with your team to talk through how you would manage a disaster.
* **Step 6:** Correct issues that come up through testing.

And when those steps are complete, it’s time to move back to step 1

# Risk Assessment Template

Prior to creating a business continuity plan, credit unions should first assess their risk to determine types of threats their plan should address. Below is a sample Risk Assessment Template

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Risk Assessment Worksheet for | Applicability | Probability | Speed of Onset | Forewarning | Duration | Impact | Weighted Risk |
| **Natural Threats** |
| Internal Flooding |  |  |  |  |  |  |  |
| External Flooding |  |  |  |  |  |  |  |
| Internal Fire |  |  |  |  |  |  |  |
| External Fire |  |  |  |  |  |  |  |
| Earthquake |  |  |  |  |  |  |  |
| Thunder / Electrical Storm |  |  |  |  |  |  |  |
| Wind Damage / Tornado |  |  |  |  |  |  |  |
| Snow or Ice Storm |  |  |  |  |  |  |  |
| Hurricane |  |  |  |  |  |  |  |
| Epidemic |  |  |  |  |  |  |  |
| Pandemic |  |  |  |  |  |  |  |
| Major Landslide / Mudslide |  |  |  |  |  |  |  |
| Other |  |  |  |  |  |  |  |
| **Human Threats** |
| Explosion |  |  |  |  |  |  |  |
| Extortion |  |  |  |  |  |  |  |
| Burglary |  |  |  |  |  |  |  |
| Embezzlement |  |  |  |  |  |  |  |
| Vandalism |  |  |  |  |  |  |  |
| Robbery |  |  |  |  |  |  |  |
| Hazardous Waste |  |  |  |  |  |  |  |
| Biological Contamination |  |  |  |  |  |  |  |
| Water Leak / Plumbing Failure |  |  |  |  |  |  |  |
| Work Stoppage |  |  |  |  |  |  |  |
| Aircraft Crash |  |  |  |  |  |  |  |
| Loss of Key Staff |  |  |  |  |  |  |  |
| Data Entry Error |  |  |  |  |  |  |  |
| Improper Handling of Sensitive Data |  |  |  |  |  |  |  |
| Unauthorized Physical Access |  |  |  |  |  |  |  |
| Malicious Damage or Destruction of Software or Data |  |  |  |  |  |  |  |
| Unauthorized Access to or Theft of Data |  |  |  |  |  |  |  |
| Unauthorized Modification of Software or Hardware |  |  |  |  |  |  |  |
| Kidnapping |  |  |  |  |  |  |  |
| **Technical Threats** |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Risk Assessment Worksheet for | Applicability | Probability | Speed of Onset | Forewarning | Duration | Impact | Weighted Risk |
| Power Failure / Fluctuation |  |  |  |  |  |  |  |
| Heating, Ventilating, or Air Conditioning Failure |  |  |  |  |  |  |  |
| Malfunction or Failure of CPU or Hardware |  |  |  |  |  |  |  |
| Failure of Application Software |  |  |  |  |  |  |  |
| Telecommunications Failure |  |  |  |  |  |  |  |
| Media Failure |  |  |  |  |  |  |  |
| Other |  |  |  |  |  |  |  |
|  |
| **Applicability** | Y | Yes |  |
| N | No |
|  |
| **Probability of Occurrence** | 1 | Low |  |
| 5 | Medium |
| 10 | High |
|  |
| **Speed of the Onset** | 0 | Gradual |  |
| 1 | Sudden |
|  |
| **Forewarning** | 0 | Yes |  |
| 1 | No |
|  |
| **Duration of Occurrence** | 0 | 1 hour to 1 day |  |
| 1 | 1 - 2 days |
| 2 | Longer than 2 days |
|  |
| **Impact on the Financial institution** | 0 | No interruption in operations. |
| 1 | Interruption of up to 1 day |
| 2 | Interruption for 1 -2 business days |
| 3 | Interruption in operations for over 2 days |



# Business Continuity Plan Template

## Incident Command Structure

Identify the key roles you will need to fill during a crisis and who will fill those roles. Below is a sample structure

|  |  |
| --- | --- |
|  | **INCIDENT COMMANDER** |
| **Lead** |  | A. (Set by CEO) |  |
| B. (Set by CEO) |
| **Key Respon- sibilities** | * Pick leads for each team
* Set objectives, priorities
* Establish decision making process
* Establish single system for ordering resources
 |
|  | **MEMBER COMMUNICATIONS TEAM** | **EMPLOYEE SUPPORT TEAM** | **MEMBER OPS TEAM** | **IT TEAM** | **SECURITY TEAM** |
| **Lead** |  | A. (set by IC) |  |  |  | A. (set by IC) |  |  |  | A. (set by IC) |  |  |  | A. (set by IC) |  |  |  | A. (set by IC) |  |  |
| B. (set by IC) | B. (set by IC) | B. (set by IC) | B. (set by IC) | B. (set by IC) |
| **Support Team** | (Set by Team Lead) | (Set by Team Lead) | (Set by Team Lead) | (Set by Team Lead) | (Set by Team Lead) |
| **Key Respon- sibilities** | * PR
* Member Communication
* Social Media
* Public website
 | * Staff support
* Staff shelter
* Staff communication
* Staff safety
 | * Member support
* Develop & implement Member strategies
 | IT Support | * Facility security
* Liaison with government agency
 |
|  | **BCP MANAGEMENT TEAM** | **FACILITIES/ LOGISTICS TEAM** | **FINANCE & ADMIN TEAM** | **IC LIAISON** |  |
| **Lead** |  | A. (set by IC) |  |  |  | A. (set by IC) |  |  |  | A. (set by IC) |  |  |  | A. (set by IC) |  |  |  |
| B. (set by IC) | B. (set by IC) | B. (set by IC) | B. (set by IC) |
| **Support Team** | (Set by Team Lead) | (Set by Team Lead) | (Set by Team Lead) | (Set by Team Lead) |  |
| **Key Respon- sibilities** | * Monitor & communicate situation
* Manage BCP Dashboard & assignments
* Capture lessons learned & incident records
 | * Ordering & managing all resources (supplies, equipment, fuel, food)
* Managing facilities
 | * Tracking costs, recording personnel time
* Negotiating leases and vendor contracts
* Managing data analytics
 | IC's Point of contact for anyone outside response team |  |



## Key Response Strategies

Include a basic checklist of your key, immediate tasks that must be completed after a crisis has hit. Each team should have their own checklist. Below is a sample checklist for the Incident Commander

\*\*Immediate Priorities\*\*

|  |  |
| --- | --- |
| **Step 1** | Make sure 911 has been called if needed |
| **Step 2** | Pick Incident Commander:  |
| **Step 3** | Set Executive Team meeting place (the “Command Center”). Good options:1. [list locations]Exec team works together using standard Incident Management protocol. |
| **Step 4** | Get your critical team together. Minimum recommended:* Member communications team
* Employee Support team
* Member Ops Team
* IT Team
* Security Team
* BCP Management Team
* Facilities/Logistics Team
* Finance & Admin Team
* IC Liaison
 |
| **Step 5** | Notify staff with Emergency Notification System. Recommendations:* Assigned to:
* Content:
	+ All Staff: Situation status, ETA for update, instructions to confirm status
	+ Senior Staff: Any follow up instructions for senior staff
 |
| **Step 6** | Set Command Center protocol for tracking status during crisis. Recommendations:* Check-ins: Every 1-2 hours
* Issue reporting: Response team reports all issues & updates to Incident Commander & BCP coordinator
* Reporting method: email, in person, or cell phone
* Items to track: BCP Coordinator tracks:
	+ Issues/Assigned tasks
	+ Related decisions
	+ Who it was assigned to
	+ Resolution ETA

 o When and how issue was resolved.  |

|  |  |
| --- | --- |
|  | *Note: If internet is available, use “Command Center Tracking” in SmartSheet.***\*\*Continue for Duration of Crisis\*\*** |
| **Step 6** | IC sets direction for Staff Communication. Recommendations:* Frequency: Initial – within 30 minutes, updates - As situation evolves, generally every 2 hours until situation stabilizes
* Assigned to: Drafted by Member support with help from Communications, Sent by IC.
* Minimum content:
	+ Branches & ATM Status: Who’s closed & ETA for reopening, Who’s re-opened.
	+ System Status: Major systems down & ETA, System issues resolved.
	+ Operational status: Status of core operational areas – Issues impacting Members & ETA, issues that have been resolved. Core focus areas: Payments, Lending,

MSC & Branches* + Employee Issues: Any major employee issues (safety, lodging, child care, pay, etc.)
	+ Any talking points for the above
* Channel: Options for sending out status updates:
	+ Email
	+ Alert Media
	+ In person/phone call

**\*\*Continue for Duration of Crisis\*\*** |
| **Step 7** | IC sets direction for Member communication. Recommendations:* Frequency: Initial: Within 30 minutes, Updates: As situation evolves, generally every 2 hours until situation stabilizes
* Assigned to: Communications to draft language with help from Member support, recommend channel, and implement. Incident Commander or designee to approve language and channel
* Channels: Public Website, OLB/Mobile, Social Media, 800 # message

**\*\*Continue for Duration of Crisis\*\*** |
| **Step 7** | Work with your teams. Figure out status & make critical decisions:* IT:
	+ Are we going to DR? If so – authorize IT to activate DR.
	+ Confirm highest priority for system recovery.
* People: Take action needed to ensure safety of employees
* Communication: Confirm immediate communication needs & protocol
* Facilities:
	+ Secure buildings
	+ Confirm highest priority for building repairs
	+ Decide work site to use for critical staff.
* Members: ID & report critical Member Needs
* Security: Secure buildings
 |
| **Step 9** | Update Board |



\*\*Next Steps After Immediate Priorities\*\*

|  |  |
| --- | --- |
| **Step 10** | Set protocol for receiving status reports from all areas. Recommendations:* Frequency: twice daily, emergencies immediately
* Process: Send to IC and copy BCP coordinator for tracking
* Recommended Content:
	+ Status of staff – who can work, who can’t work, special needs
	+ Status of functions: what is not working or impacting Member service.

**\*\*Continue for duration of crisis\*\*** |
| **Step 11** | Review status reports from all teams, prioritize issues, make critical decisions. Likely issues to address:**IT Team:** Provide direction as needed on strategy for restoration.**Employee Relations Team:*** Hotel or other lodging, child care, meals
* Special pay or time off needs
* Assist impacted staff

**Communications Team:** Provide direction for ongoing Member communication, including communication methods, content, and timing.**Facilities Team:** Provide direction as needed on strategy to repair buildings or move staff to alternate worksite.**Member Experience Team:*** Monitor cash levels, authorize special shipments, or movement of cash as needed
* Adjust hours of operation as needed
* Provide direction as needed on special exceptions to reduce Member impact.

**Payments:** As needed, adjust offline processing limits if needed**Community Team:** If disaster is affecting community, determine if RCU Community Fund is to be activated. Is so, instruct Community Team to activate their plan.**Lending:** As needed, authorize special lending products for impacted Members (e.g. 0% loans).**All Teams:** as needed, authorize any special exceptions to reduce Member Impact (e.g. skip payments, late fee waivers) |
| **Step 12** | As needed, contact any local officials and regulators. |

## Staff Contacts

Name and contact information for all staff

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Cell Phone | Email Address | Address |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Call Tree

List a call tree establishing responsibility for contacting various staff. Alternative, purchase an emergency notification system to be used to push out automated messages to staff.

* CEO calls:
	+ Chief Operation Officer calls
		- Branch manager calls
			* Branch staff
	+ Chief Financial Officer
		- Department managers call
			* Department staff

## 3rd Party Contact

Listing of the name and contact information of all your critical 3rd parties (vendors, regulators, government officials).

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Cell Phone | Email Address | Address |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Resources

List critical resources you will need to operate your credit union

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Resource | Normal Qty. | Minimum Qty. | Day 1 | Day 2 | Day 3 | Week 2 | Week 3 |
| Workstations |  |  |  |  |  |  |  |
| Printers |  |  |  |  |  |  |  |
| Laptops |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

## Locations

List back up locations you have identified that you could use if you cannot use your main location

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Location | Type | Address | Phone | Priority |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Required Functions:

List all of your credit union’s normal functions (example: take deposits, clear checks, fund loans) and identify its priority for recovery, your backup plan for handling it until you’ve recovered, how long you can go without it, and how much data is acceptable to lose.

|  |  |  |  |
| --- | --- | --- | --- |
| Function | Maximum Allowable Downtime (MAD) | Recovery Time Objective (RTO) | Recovery Point Objective (RPO) |
| [Describe function}**Impact of Loss:**[How will it impact you?]**Work Around**[back up plan until recovery] |  |  |  |
| [Describe function}**Impact of Loss:**[How will it impact you?]**Work Around**[back up plan until recovery] |  |  |  |
| [Describe function}**Impact of Loss:**[How will it impact you?]**Work Around**[back up plan until recovery] |  |  |  |
| [Describe function}**Impact of Loss:**[How will it impact you?]**Work Around**[back up plan until recovery] |  |  |  |

## Recovery Templates:

Include templates for communication and tracking which could help you manage the crisis. Attached are example templates.



**DAMAGE ASSESSMENT WORKSHEET**

**Location Name:** \_

**Prepared by: Report Date:** \_ \_ **Report Time:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ITEM TO BE** |  | **STATUS** | **ACTION NEEDED** | **NOTES** |
| **CHECKED Good** | **Bad** |
| **1. Assess Building Access** |  |  |
| A. Is building accessible? | * Yes
 | * Limited

-OR-* Access denied
* Time:
* By:
* Until:
 |  |  |
| B. Are there safety concerns? | * No
 | * Yes – There are safety concerns
 |  |  |
| C. Are there other building access issues? | * No
 | * Yes
 |  |  |
| **2. Assess Structure** |  |  |
| A. Are walls damaged? | * No
 | * Yes – Visible damage
 |  |  |
| B. Are floors damaged? | * No
 | * Yes – Visible damage
 |  |  |
| C. Are ceilings damaged? | * No
 | * Yes – Visible damage
 |  |  |
| **3. Assess Utility status** |  |
| A. Is there a potential gas leak? | * No
 | * Yes – potential gas leak
 | * Turn off gas valve
* Contact Gas company
 |  |
| B. Is the electrical system intact? | * Yes
 | * No
 | * Turn off electricity at main breaker.
* Avoid water on the ground – if exists call utility company to shut off
 |  |
| C. Is lighting working? | * Yes
 | * No – No lighting
 |  |  |



|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM TO BE CHECKED** | **STATUS** | **ACTION NEEDED** | **NOTES** |
| **Good** | **Bad** |
| D. Is HVAC working? | * Yes
 | * No – heating, cooling, or ventilation not working
 |  |  |
| G. Is plumbing intact? | * Yes
 | * No – ruptures/leaks
 | * Avoid using toilets
* Contact a plumber
* Contac the water company
 |  |
| H. Are there other Utility issues? | * No
 | * Yes
 |  |  |
| **4. Assess Equipment** |  |
| A. Was equipment moved in disaster? | * No
 | * Yes – Equipment moved
 |  |  |
| B. Receiving water from overhead leaks? | * No
 | * Yes – overhead leaks
 |  |  |
| C. Contaminated by smoke or soot? | * No
 | * Yes – contaminated
 |  |  |
| D. Showing signs of electrical problems? | * No
 | * Yes – electrical problems
 |  |  |
| E. What is overall status of equipment? | * Un- damaged
 | * Damaged but repairable

-OR-* Destroyed
 |  |  |
| F. Are there other equipment issues | * No
 | * Yes
 |  |  |
| **5. Assess Services** |  |
| A. Is access control working? | * Yes
 | * No – access control is not working
 |  |  |
| B. Have sprinklers been activated | * No
 | * Yes – sprinklers have been activated
 |  |  |
| C. Is power supply working? | * Yes
 | * Yes – generator only

-OR-* No – no power to facility
 |  |  |
| D. Are circuit breakers/power | * No
 | * Yes - Damaged
 |  |  |



|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM TO BE CHECKED** | **STATUS** | **ACTION NEEDED** | **NOTES** |
| **Good** | **Bad** |
| cables damaged? |  |  |  |  |
| E. Are there other services issues? | * No
 | * Yes
 |  |  |
| **6. Supplies** |  |
| A. Have supplies been damaged? | * No
 | * Damaged but usable

-OR-* Destroyed
 |  |  |
|  |  |  |  |  |
| **7. Security** |  |
| A. General safety and security in the neighborhood? (i.e riots/looting) | * Yes
 | * No
 |  |  |
| B. Is Member information Security at risk? | * No
 | * Yes
 |  |  |
| C. Is security guard needed? | * No
 | * Yes
 |  |  |
| D. Alarm and Camera systems functioning? | * Yes
 | * No
 |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |



### INCIDENT LOG

NAME: DEPARTMENT/TITLE:

|  |  |  |  |
| --- | --- | --- | --- |
| DATE | TIME | INCIDENT/ACTION/REQUEST EXPENDITURE | CLOSE OUT (TYPE X) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# System Restoration Priorities

Below are the recommended priorities for restoration of [CREDIT UNION] systems following a disaster. Actual priorities will depend on the specifics of the disaster and the impact to (CREDIT UNION). The IT Team Lead is responsible for reviewing and confirming system priorities with the Incident Commander as part of the recovery process.

|  |  |
| --- | --- |
| **FULLY FUNCTIONAL AT ALL TIMES**IT Team will validate systems remain fully functional | **MANUALLY CONTROLLED FAILOVER SYSTEMS**(by Priority)IT Team will manually restore systems |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

### STAFF COMMUNICATION TEMPLATE

|  |
| --- |
| Redwood Credit Union |
| Topic | **[TOPIC]** |
| Who | Everyone |
| Additional Information | To assist you in responding to questions regarding the current situation, below is an overview of our operational status. We will continue to provide updates as the situation evolves.**Overall Power Outages:**[any changes to power status]**Branch Status**[current status of branches]**ATM Status**[Current status of ATM] **Special Instructions** Any special instructions |
| Action | [expectations for staff actions] |
| Closing/ Contact: | **In Closing:**We will continue to keep staff updated as pertinent events unfold.Thank you everyone for your dedication to our Members, communities, and each other! Because of each of you, we have made a significant positive impact to our Members’ lives when they have needed us. |
| cid:image003.jpg@01D13C16.94EE0930 |