BCU-IR05-Data Center Backup & Disaster Recovery Plan

Table of Contents

Introduction

This document is the disaster recovery plan for BCU's data center. The information present in this plan guides BCU's management and technical staff to recover data center operations in either our physical or virtual locations in the event of a business continuity or disaster event.

The recovery plan is composed of document resources and procedures to be used in the event of a disaster affecting data center services. Each supported computing platform has a section containing specific recovery procedures. There are also sections that document the personnel who will perform the recovery tasks and an organizational structure for the recovery process.

This plan is virtually available through the BCU's third party hosted SharePoint site, as well as in BCU's SaaS governance platform, as well as physically available in the Vernon Hills Security Department and physical disaster recovery data center to make it more generally available to BCU staff. This plan will be reviewed annually and updated on a regular basis as changes to the data center are made.

Objectives & Overview

Primary Focus

The primary focus of this document is to provide a plan to respond to a disaster that destroys or severely cripples BCU's virtual environments or physical data centers. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available.

Primary Objectives of the Plan

This disaster recovery plan has the following primary objectives:

- Describe the technology strategies used to achieve disaster recovery.
- Present an orderly course of action for restoring critical computing capability to BCU within as guided by the predetermined recovery objectives.
- Set criteria for making the decision to recover at a cold site or repair the affected site.
- Describe an organizational structure for carrying out the plan.
- Provide information concerning personnel that will be required to carry out the plan and the computing expertise required.
- Identify the equipment, floor plan, procedures, and other items necessary for the recovery.

Assumptions

All disaster recovery plans assume a certain amount of risk, the primary one is how much data is lost or exposed in the event of a disaster. With current resources to duplicate and maintain redundant computer systems, it is impossible to plan for zero down time and zero data loss. Therefore, BCU assumes the risk of having to do without computing resources for a period of time as well as, for the potential of data loss during that interruption period.

Noting that the techniques for backup and recovery used in this plan do NOT guarantee zero data loss. Data recovery efforts in this plan are targeted at getting the systems up and running with the last available off-site backup. Effort will be required after the system operation is restored in order to: (1) restore data integrity to the point of the disaster and (2) to synchronize the data with any new data collected from the point of the disaster forward.

The extent to which this plan will be effective depends on disaster recovery plans by other departments and units within BCU. It is therefore essential that every business unit within BCU develop a plan on how they will conduct business in the event of a disaster for an undetermined period of time. These business units need means to function while the computers and networks are down, plus they need a plan to synchronize data they may have collected while systems were down to restore from backups.

Target audience

This document is intended for the BCU management, Command Team, BCP Committee, disaster recovery teams, and other individuals on a need-to-know basis.

References

Disaster Recovery Plan virtual copy located in BCU's compliance governance system: Preparis

Portal (preparisapp.com)

Virtual copy of the BCP on BCU's SharePoint intranet:
https://baxtercreditunion.sharepoint.com/sites/Policies/Shared Documents/Forms/Public View.aspx?id=%2Fsites%2FPolicies%2FShared Documents%2FBCU-IR03https://baxtercreditunion.sharepoint.com/sites/Policies/Shared Documents/Forms/Public View.aspx?id=/sites/Policies/Shared Documents/BCU-IR03-BCPlan.pdf&parent=/sites/Policies/Shared DocumentsBCPlan%2Epdf&parent=%2Fsites%2FPolicies%2FShared Documents

Disaster Planning

In order to facilitate recovery from a disaster which destroys part or all of the primary data center location, certain preparations have been made in advance. This document describes what has been done to lay the way for a quick and orderly restoration of the data center.

Human Resources

Immediately following the disaster, a planned sequence of events begins. Key employees are notified, and recovery teams are grouped to implement the plan. However, the plan has been designed to be usable even if some employees are unavailable.

Recovery Facility

BCU has a hybrid data center environment containing both physical and virtual production and disaster recovery data centers, or in the case of virtual, regions. If the primary data center or region becomes inoperable, repairing or rebuilding of the primary location may take an extended period. In the interim it will be necessary to restore computer and network services at the secondary site.

BCU's physical data or communication locations are:

- Primary physical data center:
  BCU, 340 N. Milwaukee Ave, Vernon Hills, IL 60061
  Badge and biometric access required

- Secondary data center:
  TierPoint 3701 W Burnham St, Milwaukee, WI 53215,
  Phone: (844) 200-8718
  Open 24 hours
  Badge and biometric access required

- Communication Colocation:
  First Communications
  601 West Polk Street Ste. 200, Chicago, IL 60607
  Open 24 hours
  Badge and biometric access required

Access to the primary data center in Vernon Hills, Illinois, requires multi-factor authorization and must be requested through BCU's Service Desk portal. Once the access is requested and approved, the employee's badge is updated to include access to the requested location. In addition to badge access, the employee must have a PIN to turn off the alarm as well as a PIN/Biometric combination to unlock the door. To minimize fire damage, the data center is protected by a multi-phased sprinkler system as well as an instant kill switch. Information

Technology relies on Facilities Dept. for the actual work that needs to be done to renovate the space to be ready to receive and operate the computer equipment. Information Technology has available all power and cooling specifications of equipment to be staged.

The secondary data center is in an area which is physically separated from the primary data center. It has been identified for use as the temporary home for the computer and network systems while the primary data center is being repaired. BCU will use the secondary data center, alternate cloud region, or both as the approach for this disaster recovery plan. The physical location houses systems of critical applications and some available office space for operating and technical personnel. The location has adequate cooling and AC power capacity to support these systems; and provides network connectivity. Those BCU employees who do not have standing approved access, will need to request access from the Director of Infrastructure and Operations and will be monitored by the IAM Team in the Security Division. Access to the secondary colocation needs to be requested from the vendor, background check completed, and biometrics obtained before access can be granted.

BCU's virtual data centers are hosted in Microsoft's Azure cloud environment. Primary processing happens in either the West or North Central regions with the disaster regions being East or South Central, respectively. Microsoft's Azure environment was chosen to host BCU's virtual environment due to their high levels of service commitments, levels of redundancy within an individual region, the ability to utilize both
as a Service as well as Systems/Software as a Service and the disaster recovery integration with alternate regions. Microsoft offers both internal region recovery via zone recovery as well as traditional disaster recovery by having a redundant region. Access to BCU's virtual data centers is controlled by Azure role-based access.

Redundancy

Redundancy is also used in BCU's primary data centers to help recover if there is a failure of critical system, network, telecommunications, or electrical power.

Redundancy is defined as having a secondary peripheral, computer system or network device that takes over when the primary unit fails. Depending upon the technology, some environments fail over to redundant automatically, while others need to be coordinated.

The following redundancies have been setup at BCU's primary data center:

a. Electrical power

Building power coming from the utility company is three-phased power. In the event of a full or partial failure, BCU is protected by a dual UPS system and a diesel generator. BCU's data center, as well as the majority of the desks at BCU's 340 N. Milwaukee Avenue Corporate headquarters, are supported by a dual UPS system providing A and B power. The primary data center located at the 340 building, is protected by both A and B power, with the exception of a handful of servers that are

single honed. In the event that we have an issue with either the A or B UPS unit, either UPS can carry the load of both UPS units.

If the electrical power interruption is outside of BCU's walls, the UPS backup unit will turn on automatically and keep both the data center and those desks that have UPS power up and running during the six second that it takes for the diesel-powered generator to sense the power disruption and automatically turn on. If the power interruption is within the building, the generator would not engage however the UPS system will provide enough power for the production environment within the primary data center to be brought down in a controlled fashion.

BCU's generator is a diesel-powered generator and as previously noted, will automatically turn on when it monitors a break in utility provided power. The generator will continue to run for as long as fuel is provided. The generator is tested on a monthly basis.

b. Network

All network devices in BCU's data center are either dual powered from A and B power or connected to both power supply sides via an electrical transfer switch that will switch supply in the event of a single side power failure.

The majority of our hosts, with the exception of BCU and partner VPN devices, are networked via multiple 10Gbps Ethernet connections to dual Cisco Nexus core switches, utilizing a variety of network protocols or technologies including but not limited to LACP, ECMP, and VPC. to provide resiliency in case of a single link or core switch failure.

This model is repeated at the Colocation center referred to as "Colo" (Polk St., Chicago) and the Milwaukee Data Center.

Branch and remote office connectivity is primarily via MPLS connections to Colo and Vernon Hills Data Center. Additionally, SD-WAN is deployed at most branches providing circuit redundancy, Data Center locations in Vernon Hills, Colo, and Milwaukee are connected via multiple point-to-point circuits and multiple WAN routers utilizing Multiprotocol BGP (mBGP) to provide route redundancy and failover for multiple routing instances.

Azure regions maintain physical connectivity via dual paths and dual WAN routers in Colo. North Central and South Central regions' connectivity is backed up via VPN to Milwaukee.

c. Internet

Two primary Internet circuits with two providers and separate routers in Vernon Hills provide connectivity to public Internet for on-premises systems. Additionally, Internet services in Colo and redundant Internet paths in Milwaukee provide backup Internet service in case of failure of connectivity in Vernon Hills.

d. Telecommunications

Major Components Roles

- Cloud hosted telephony system provided by Genesys. Cloud hosted SIP services provided by Bandwidth. Bandwidth provides several redundant routing solutions for inbound 8XX numbers through their Call Assure and their "Cloudy Day" solutions. Storage – Legacy call recordings are stored in Azure while new call recordings are stored in the Genesys cloud platform.
- Inbound/Outbound virtual SBC's (Session Board controllers) hosted in Azure– handles the bi-directional fax and analog device traffic.
- Physical phones are now only in limited locations such as conference rooms, services centers, and ELT suites. All other users use soft phones through the Genesys platform.
- Dynamic E911 services hosted in Redsky cloud platform.

e. Fedline Machine

There are four hot, redundant machines: three in the Vernon Hill's corporate headquarters and one in BCU's disaster recovery data center. BCU's IT department keeps one spare formatted Fedline machine ready to be updated with the appropriate certificate and IP configurations in the event one of the machines malfunctions. The Member Operations team who is responsible for electronic transactions, uses the disaster recovery machine quarterly to ensure the system is up, available for log ins, can access the Federal Reserve site and process files.

f. Cluster

Some of BCU critical systems and databases are protected with clustering. This is Microsoft's high-availability solution. In a clustered environment, multiple servers (two or more) operate as a single network server. Failure of one of the network servers in the cluster will go unnoticed because the remaining servers in the cluster assume the work that was being performed by that failed network server.

Back-Ups and SQL Databases

Data is largely held in the following applications: NetApp SAN storage, Azure File Shares, and SQL storage.

BCU's Azure backups are protected against malware and ransomware by utilizing backup copy isolation (cross region long term archiving & near real-time replication) and rely upon Azure technologies which only allow authentication users and the backup service itself to interact with archived data long-term.

The file shares located on the SAN storage are backed up and replicated via the NetApp environment. This is a hot environment in which there is a redundant environment at the disaster recovery data center. The backups and replications are made and stored in the disaster recovery system.

Domain controllers and BCU's Microsoft Active Directory Forrest is protected by Azure Backup (MABS on-prem) and also via BCUS's ADFR product.

If there is a database quality issue, the database will be recovered backups, the majority of which are stored in Azure blob storage.

> Azure File Share: Azure Files Shares offer fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol, Network File System (NFS) protocol, and Azure Files REST API. Azure file shares can be mounted concurrently by cloud or on-premises deployments.
>
> The data contained within Azure Files Shares is protected with native Azure daily backups which are archived and replicated from our primary datacenter region of North Central US to South Central US. Selected critical shares have also been configured for near real-time data replication between regions for high availability.

SQL Protection:

There are two different SQL solutions. First, is a SQL clustered environment with clusters in two different Azure regions. The application talks to a SQL listener and every time there is a change in the database, the DR nodes are updated. If there is a technical issue with the primary node, the secondary node will take the traffic automatically. Other SQL databases have weekly backups with log shipping.

Log shipping is a technique which allows BCU to transfer changes in SQL databases from the primary data center to the secondary data center, allowing for critical databases to be recovered after the primary data center had a disaster. Log shipping involves taking a backup of transaction log of SQL database level on primary server, copying the same on the secondary server and restoring on secondary server at the predefine time interval. Because malware is typically a software and log shipping only copy/restore SQL transaction log, log shipping will not replicate malware to the secondary server. Database full and differential backups are taken at regular intervals so we can recover database from those backups. Log shipping intervals are set by us and can be set to any value to ensure that recovery objectives can be met.

Microsoft O365 Office Protection:

All products withing Microsoft Office 365 are protected by Rubrik. The SaaS based backup solution was purchased in 2023 and has been successfully backing up all aspects of the Office Suite.

Disaster Recovery Team Creation and Notification

Disaster Recovery Team

The decision whether or not to declare a disaster is handled by the Plan Administrator, with aid from the Command Team, as outlined in the Business Continuity Plan (BCP). The BCP also includes the implementation of sub teams lead by the following roles:

- Administrative Business Continuity Plan Coordinator held by the CEO and CHRO
- Communication Business Continuity Plan Coordinator held by the SVP, Marketing/Communications
- Facilities Business Continuity Plan Coordinator held by the VP, Controller
- Technical Business Continuity Plan Coordinator held by the CTO
- Operations Business Continuity Plan Coordinator held by the COO
- Data Business Continuity Plan Coordinator held by the Chief Data Officer
- Security Business Continuity Plan Coordinator held by the CISO

Once a disaster is declared, the Technical Business Continuity Plan Coordinator will implement some or all of the Disaster Recovery Plan. The Technical Business Continuity Plan Coordinator will immense with the creation of a Disaster Recovery Team which will follow this general plan of action:

1) Obtain a current copy of the Disaster Recovery Plan, virtually or a printed copy.
2) Each member of the team is to review the status of their respective areas of responsibility.
3) Review damage assessment.
4) The Technology BCP Coordinator makes the final decision about where to do the recovery.
5) The Technology BCP Coordinator briefly reviews the Disaster Recovery Plan and makes any last-minute adjustments to accommodate special circumstances that are to be discussed and decided upon.
6) If the disaster is related to a cyber event, determine perseveration and forensic requirements by partnering with the CSO and Legal as there are specific actions and vendors need to be enacted and engaged, respectively.

7) Determine which hardware, software, and supplies will be needed to start the restoration of a particular system.
8) Communicate list of components to be purchased and their specifications by submitting a Procurement Request, assuming the M365 environment is up. Then email and call the Sr. Procurement Manager with the procurement request ticket number. If the M365 environment is not up, call the Sr. Procurement Manager for further instructions.
9) When hardware begins to arrive, work with vendor representatives to install the equipment, as necessary. The following vendors have support contracts:
    a. Sentinel Help Hands: NetApp and Cisco
    b. OME/CDW: Nutanix
    c. TierPoint: Helping Hands
10) When all components are assembled, begin the steps to restore the operating system(s) and other data from the Azure backups (cloud and MAB).
11) Attempt to recreate status of all systems up to the point of the disaster if possible. If not, the system is handed off to the Application Recovery Team.
12) Mobile communications will be important during the early phases of the recovery process. This need can be satisfied through the use of cellular telephones and/or two-way radios through BCU's existing mobile deployment procedures. For Puerto Rico emergency communications, 6 satellite phones are available, tested and charged just prior to the start of hurricane season.

Disaster Notification List

These people are to be notified as soon as possible when a technical disaster occurs:

If necessary, contact safety personnel:

Safety Personnel	Dial
Emergency Fire, Ambulance, Rescue, Police	911

Use the IT Emergency Notification List for current contact information.

Person	Title	Cell Phone
Scott Zulpo	CTO	847-527-7302
Pranay Surati	Sr. Director of Infrastructure & Operations	224-207-2769
Salien Manek	Manager, Enterprise Architecture	630-777-8206
Gordon Kenmuir	Director, Service Operations & Support	847-989-6767
Dmitriy Melnick	Sr Director, Development & QA	847-477-6736
Rob Russell	Director, Security Operations & Infrastructure	847-271-6399
Steve Jauregui	Sr Manager, Physical Security	215-498-6858

In addition to those people who will be directly responsible for the disaster recovery process, others in the organization must be notified and updated of the recovery efforts. In addition, some of these people may play a supporting role in the recovery efforts:

Person	Title	Contact
Stephenie Southard	CSO	224-360-4058
Kelli Bartczyszyn	Business Resiliency Director	847-344-8024
Brad Babin	Sr. Manager, Business Resiliency	225-266-8898
Elisa Marshall	Sr. Manager, Procurement	262-455-5025
Lisa Baron	EVP HR	847-977-6464

Person	Title	Contact
CJ Presto	CFO	773-895-4555
Mike Valentine	CEO	847-507-9455
Jim Block	COO	847-522-8817
David Blum	EVP, Relationships & Service Delivery	815-861-7566

Initiation of Emergency Procedures

Establish the Recovery Control Center

The establishment of the Command Center is determined by the Command Team as authorized by the Business Continuity Plan. It might be necessary to also create a Disaster Recovery Control Center from which the disaster recovery process is coordinated. The Technical BCP Coordinator should designate where the Recovery Control Center is to be established.

Damage Assessment

This damage assessment is a preliminary one which determines the extent of damage to critical hardware and the primary data center and will be performed by the Facilities Manager, Sr Manager of Service Operations and the Sr Manager of Physical. The primary goal of this assessment is to make the decision where primary recovery efforts should be restored as well as what infrastructure needs to be repaired or purchased. This includes building necessities such as electrical, heating and air conditioning and UPS units. The Sr Manger of Physical Security will also determine if there are necessary changes to privileged access.

Team members should be liberal in their estimate of the time required to repair or replace a damaged resource. Take into consideration cases where one repair cannot begin until another step is completed. Estimates of repair time should include ordering, shipping, installation, and testing time.

In considering the hardware items, the equipment lists provided in the recovery sections for each platform are considered first. These lists were constructed primarily for recovery at the secondary data centers, so they consist of the critical components necessary to recovery. You will need to separate items into two groups. One group will be composed of items that are missing or destroyed. The second will be those that are considered salvageable. These "salvageable" items will have to be evaluated by hardware engineers and repaired, as necessary. Based on input from this process, the Recovery Management team can begin the process of acquiring replacements.

Begin Reassembly at Recovery Site

Salvaged and new components are reassembled at the secondary data center according to the instructions contained in this plan, including the deployment of virtual resources in BCU's disaster recovery portion of its cloud. Since all plans of this type are subject to the inherent changes that occur in the computer industry, it may become necessary for recovery personnel to deviate from the plan. If vendors cannot provide a certain piece of equipment on a timely basis, it may be necessary for the recovery personnel to make last-minute substitutions. After the equipment reassembly phase is complete, the work turns to concentrate on the data recovery procedures.

Emergency Procurement

The success or failure of this plan hinges on the ability to purchase goods and services as quickly as possible.

The BCU's Procurement Office will assist in the rapid turnaround of emergency procurements if the disaster affects key purchasing systems. All Disaster Recovery Team members must submit their requests to the Procurement Team via the M365 procurement request form and then contact the Sr. Procurement Manager via cell phone with the request number, who will follow the regulations established for emergency procurement.

Platform Recovery

This portion of the plan documents the detailed procedures for recovering each of the computer and network system components.

Each procedure document will contain the following if applicable:

- A Topology Diagram
- Configuration Specifications
- Administrative Operating Procedures
- Hardware and Software Inventory List
- Service and Support Contact Information
- Specific DR and Business Continuity Procedures
- Backup and Recovery Procedures

Due to the secure nature of the information contained within these documents on-line editing and viewing controlled via rights management on a need-to-know basis.

Platform Recovery Procedures BCU available during a disaster include:

- Linux Servers
- Microsoft Servers
- Other Servers

- Storage (NetApp)
- Network/Infrastructure Components

Restore Data from Backups

BCU has multiple secondary data centers which have standby servers for applications supporting Critical/Tier 1 processes. These processes may also be supported in BCU's disaster recovery portion of its virtual data center. Standby servers are either hot or can be switched on shortly after the disaster plan is activated. In this case, the data of the last hour prior to the disaster may be lost depending on the system, and it should be recovered according to the recovery of application.

Data recovery efforts focus on restoring full servers for each system. Next, the recovery of applications and users' data is carried out from backups. Individual application owners may need to be involved at this point; therefore, teams are assigned for each major application to ensure that data is restored properly.

Applications Recovery

Once the platform system software and subsystems are operating correctly, the task of preparing the remaining end-user applications can begin. Each platform will have a unique recovery road to follow. In some cases, there may be very little to do except for general testing. In other cases, considerable analysis and data synchronization work will likely be required. It is important to note that each application has its own set of detailed recovery procedures documented and maintained by the Applications Development group.

Critical applications are given an extremely high priority in the process. A critical application is one where delaying the recovery of the application could cause much hardship to faculty, staff, and students.

Each application area will require a review. This review should be conducted by an analyst familiar with the application while working closely with the user representative of the application.

Items to be considered should include:

- Review of the user department Disaster Recovery Plan with special attention to any "interim" procedures that have been required in the time period since the disaster event occurred.
- Review of the application documentation concerning file and database recovery.
- Review the status of files and databases after the general platform recovery processing is complete.
- Identify any changes to bring the application to a ready for production status.

- Identify any areas where the application must be synchronized with other applications and coordinate with those application areas.
- Identify and review application outputs to certify the application ready for production use.

Restore Applications Data

It is at this point that the disaster recovery plans for users and departments (e.g., the application owners) must merge with the completion of the Information Technology plan. BCU uses both shipping change logs to the secondary data center as well as storing backups off-site. In either case there is still a gap between the time the last data was recorded and the time of the disaster; therefore, application owners must have means for restoring each running application database to the point of the disaster. They must also take all new data collected since that point and input it into the application databases. When this process is complete, the BCU computer systems can be reopened for business. Some applications may be available only to a few key personnel, while others may be available to anyone who can access the computer systems.

Recovery Objectives

The following sections describe the key terms in BCU's recovery objectives. These terms and processes are employed during BCU's BIA conversation which determine the order in which systems are recovered.

Maximum Tolerable Downtime

The Federal Financial Institution Examination Counsel (FFIEC) defines Maximum Tolerable Downtime (MTD) as "The total amount of time the system owner or authorizing official is willing to accept for a business process disruption, including all impact considerations."[1] BCU conducts interviews with Management to understand the business need and the capability of the business to return a particular function to normal operation and capacity after an interruption event.

A business function may be required to comply with service level agreements or regulatory requirements which dictate the MTD. In cases where MTD is mandated, Management should evaluate the financial and/or reputation damage that service delays may cause. Combinations of all of these factors will determine MTD. MTD is recorded in the BIA worksheet and represented using the unit hours.

Recovery Point Objective

Recovery Point Objective (RPO) is defined by FFEIC as "The point in time to which data used by an activity is restored to enable the resumption of business functions. The RPO is expressed backward in time from the point of disruption and can be specified in increments of time (e.g., minutes, hours, or days)."[2]

[1] (FFIEC, 2019)
[2] (FFIEC, 2019)

RPO is determined by or determines theamount of time between the interruption event and the last good backup which could be restored. This is equal to the time between backup completions as the worst possible time for an interruption to occur would be the moment before a backup completes. The time between backups may be determined by the ability of the business unit to recreate lost data. In the event that the business unit is not able to recreate data, or it is not necessary to recreate data, the business may elect to accept RPO as defined by the backup frequency but must put in place procedures to continue the business function without recreating the data.

If data can be recreated, rekeyed, or recovered by other means, the amount of time it takes to perform this work should be understood and considered when determining the Recovery Time Objective.

Work Recovery Time

BCU defines Work Recovery Time (WRT) as the amount of time a business unit requires to test a system after it is restored, recreate any data that was lost, if needed, and return the business function to an acceptable minimum capacity. WRT is typically expressed in hours.

Recovery Time Objective

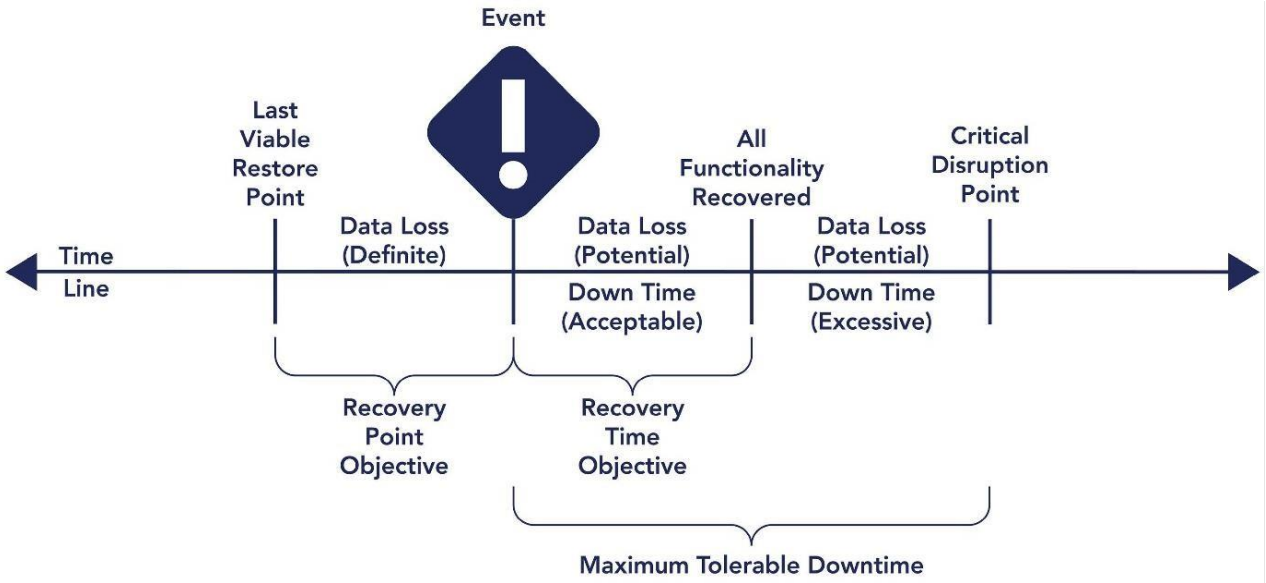
FFIEC defines Recovery Time Objective (RTO) as "The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes."[3] BCU calculates RTO by subtracting WRT from MTD and the result is expressed in hours.

In cases where a system is hosted by a third-party the business owner must understand what contractual obligation the third-party has to restore systems in the event of a disaster and ensure that time does not exceed RTO. If the third-party provider is not obligated to return the system to service quickly enough to meet RTO, the business owner should evaluate the business function and make changes to the business function or the third-party service to meet BCU's needs.

Dependencies

Critical business functions have dependencies. Those dependencies are things like electrical power, network connectivity, or system/application functionality. If the RTO for a dependency exceeds the RTO for a critical function on which it depends BCU must resolve or reconcile the difference by reducing RTO for the dependency or increasing MTD for the critical function.

[3] (FFIEC, 2019)



Criticality Definitions

Criticality	Description	RTO
Non-essential	This function or process is not essential to the success of the business. It may be provided as a convenience for customers or employees or may be an efficiency enhancing function. Without this function or process the business would survive but might be impaired.	4 weeks
Normal	The business relies on this function or process to accomplish routine tasks related to the successful delivery of services to customers or other parts of the business. Some workarounds are available, and the business can cope with an interruption in this process for up to one week.	7 days
Important	This function is important to the continued and smooth operation of the business. Interruptions to this function may disrupt other functions or there may be unacceptable consequences to working around it. If this process is not restored within 72 hours irreparable damage to the business will occur.	72 hours
Urgent	The business cannot function effectively during interruptions to this process. Workarounds are too cumbersome to be effective and other processes are significantly affected by the loss of this one. Interruptions of longer than one day may cause irreparable damage to the business.	24 hours
Critical	A failure to return this function to an operational state within four hours will cause the business to fail. It is likely other functions, or the business as a whole depend on it.	4 hours

Move Back to Restored Permanent Facility

If the recovery process has taken place at the secondary data center, physical restoration of the primary computing locations (or an alternate facility) will have begun. When that facility is ready for occupancy, the systems assembled at the secondary data center are to be moved back to the primary data center. This plan does not attempt to address the logistics of this move, which should be vastly less complicated than the work done to do the recovery at the secondary data center.

Maintaining the Plan

Having a disaster recovery plan is critical. But the plan will rapidly become obsolete if a workable procedure for maintaining the plan is not also developed and implemented. This document provides information about the document itself, standards used in its construction, and maintenance procedures necessary to keep it up to date.

Web Server Accessible

This disaster recovery plan has been designed to be accessible via SharePoint. This makes it easy to access the plan for periodic review and provides a convenient means for structuring the plan in an online fashion.

Document Owner

This document is owned by the Security Team, which is responsible for its content and maintenance.

Document Review

This document is subject to be reviewed on an annual (or more frequent) basis to validate that its content remains relevant and up to date. Significant or material changes to this document must be reviewed and approved by the Member Data Security Committee as described BCU-S01Security Policy, in Section 3, Roles and Responsibilities.

Change History

Version	Change	Author	Date
1.0	Initial version	Robin Burns	1/11/2021
2.0	Annual update (network, internet, SQL backup and procurement clarifications. Team updates)	Kelli Bartczyszyn	7/8/2022
2.1	Updates to backup, phone system and branch connectivity explanations	Brad Babin	9/15/2023
2.2	Updates to some processes and terminology Added M365 back-up explanation	Brad Babin	3/28/24

Approval History

Version	Name	Title	Date
1.0	Stephenie Southard	CISO	6/13/21
2.0	Stephenie Southard	CISO	7/29/22
2.1	Stephenie Southard	CSO	9/29/23
2.2	Stephenie Southard	CSO	7/15/2024