AnonCo Business Technology Support Continuity Plan

Anonymous Company

Revision 1.0

Last Approved: _____

Table of Contents

1 Introduction

A Business Continuity Plan (BCP) aims to mitigate and prepare for potentially disruptive events. Several key components of a BCP impact the effectiveness of an organization's critical functions and operational resilience. Through the BCP, the organization can identify these key components, formulate responses to help limit a disruptions' negative impact, and develop plans for returning to normal operation promptly when a disruption occurs.

Purpose

The primary purpose of this plan is to provide the Board of Directors, senior leadership, leaders, and team members of Anonymous Company with a set of guidelines. These guidelines serve as a framework for decision-making whenever disruptions occur, which can affect the routine operations and procedures of the organization.

Scope

This document attempts to identify and account for all key business components of Anonymous Company and to address the effects on, as well as proposed solutions for, business continuity. Key business components include the organization's tangible personnel, equipment, and intangible services.

This document includes enterprise-wide, process-oriented approaches that address technology, business operations, exercises and testing, and communication strategies critical to the organization's continuity. This consists of planning for recovery during and after an event and maintaining systems and controls for the resilience of operations. The concept of business continuity is incorporated into the risk management life-cycle of all systems, processes, and operations.

Objectives

The objectives of this continuity plan are listed below:

- Ensure that the department can perform its mission-critical functions, if applicable, under all conditions.
- Reduce the loss of life and minimize property damage and loss.
- Reduce or mitigate disruptions to operations.
- Ensure that the department has a facility where it can continue to perform its mission-critical functions, as appropriate, during a continuity event.
- Protect essential facilities, equipment, records, and other assets, in the event of a disruption.
- Achieve the department's timely and orderly recovery and reconstitution from an emergency.
- Ensure and validate continuity readiness through dynamic and integrated testing, training, exercise program, and operational capability.

Board of Directors and Senior Leadership

Anonymous Company Board of Directors and Senior Leadership ultimately oversee and govern the business continuity process.

The Board of Directors' governance should include the following:

- Assigning business continuity responsibility and accountability.
- Allocating sufficient resources to business continuity management (e.g., personnel, time, budget, training, etc.).
- Aligning business continuity management with the organization's business strategy and risk appetite.
- Understanding business continuity risks and adopting appropriate policies to manage events.
- Reviewing business continuity operating results and performance through management reporting, testing, and auditing.
- Providing a credible challenge to management responsible for the business continuity management process.
- Establishing a provision for management intervention if timeliness for corrective action is not met.

Senior Leadership governance should include the following:

- Defining business continuity roles, responsibilities, and succession plans.
- Allocating knowledgeable personnel and sufficient financial resources.
- Validating personnel understand their business continuity roles and responsibilities.
- Establishing measurable goals for business continuity performance.
- Designing and implementing a business continuity exercise and test program.
- Confirming that exercises, tests, and training are comprehensive and consistent with the organization's business continuity strategy.
- Resolving weaknesses identified in exercises, tests, and training.
- Meeting regularly with designated business continuity personnel to discuss policy changes, exercises, tests, and training plans.
- Assessing and updating business continuity strategies and plans to reflect the current business conditions and operating environment for continuous improvement.
- Coordinating plans and responses with external groups.

2 Management Process

Introduction

Proper planning and understanding the business continuity management process are critical to its success. This section describes the organization's planning, development, and maintenance processes to develop the business continuity plan. The organization uses a multi-step, process-oriented approach to business continuity management. The steps include:

- Business Impact Analysis (BIA)
- Risk Assessment
- Risk Management
- Training, Exercises, and Testing
- Monitoring, Updates, and Reporting

BCP Development and Document Control

Before AnonCo completed this BCP, all regionally based departments participated in a Business Impact Assessment (BIA) and a Risk Evaluation (RE). These were robust engagements that gathered many elements that are included in this plan. Among these are the IT assets, succession plans, communication paths, etc...

- With privileged access, the BIA/Q and RE are retained in a BCP folder on the shared drive.
- Each department should retain both hardcopy and digital copies of their BCP.
- Copies of all department's BCPs are retained, with privileged access, in Audit's BC folder on a shared drive.
- Hard copies of all departments' BCPs are provided to each department's management and corporate leadership.

Business Impact Analysis

To determine the critical business functions and data requirements necessary for the continuing operation of each department during a business interruption or a disaster, each department will be analyzed. Each department will complete a Business Impact Questionnaire (BIQ) to provide information about the potential impact of uncontrolled, non-specific events on that department's business processes.

The BIQs will then be analyzed to determine maximum tolerable downtime (MTD), identify interdependencies, identify resource requirements, and determine the criticality of individual processes to organization operations. The BIA process is discussed in detail in the Business Impact Analysis section.

Risk Assessment

The organization will conduct a risk assessment to enable the organization to achieve its BCP priorities, as determined by the BIA. The purpose of the risk assessment is to evaluate the likelihood and potential impact of reasonably foreseeable internal and external threats that could result in business disruption, including, but not limited to:

- Natural events
- Technical events
- Malicious activity
- International events
- Low-likelihood and high-impact events

The risk assessment is maintained as a separate document from the BCP.

Risk Management

Given the organization's risk assessment, the BIA will be evaluated to determine specific priorities for business processes. During disaster recovery, processes with a higher criticality and corresponding maximum tolerable downtime (MTD) will receive priority attention. As time and resources permit, lower priority will be addressed.

See the "Priority of Processes" section for the organization's business process prioritization and the Business Process Restoration and "Preparedness Controls" sections for additional information regarding the organization's business continuity risk management plans.

Assumptions

There are several assumptions built into each department's BCP. Among these are:

- A complete Disaster Recovery Plan (DRP) has been documented and validated by frequent & successful "failover" exercises. This, along with DR & business continuity (BC) policies, SLA reviews, and incident management plans, provides the backdrop for this BCP.
- This BCP is explicitly developed for the department; however, it can be used as a model and cloned for other departments but cannot be substituted for those departments' BCPs.
- There are dependencies with other departments, both inside and outside departments.
- Those dependencies may or may not be fulfilled during a widespread incident.
- An incident can evolve, broadening its scope and impact beyond its initial manifestation.
- As part of this BCP, time thresholds must be established to automatically escalate the response to a higher level with a broader scope. For example, a roof leak might evolve into a roof collapse, creating the need for transferring business processes to another location.
- An effective response to the incident requires coordination and communication among corporate leadership, other departments, and external entities.

- Depending on the scope and severity of the incident, some processes can or should be suspended, thus enabling staff and asset allocation to focus on more critical functions.
- Expectations must be managed regarding the time needed to resume full operational capabilities.
- Major incident - an event that necessitates suspending all department processes at headquarters and relocating staff to a safe location to execute their tasks. An example would be a hazmat incident on I-25 where the hazmat plume drifted toward the headquarters building.
- This BCP is a "living document" based on the findings when the document was written. Therefore, if processes, IT requirements, asset requirements, or dependencies change during the life cycle of this BCP, those changes should be reflected in the appropriate sections of this document.
- It is anticipated that this plan will be exercised at least annually. That exercise will improve both the plan and its execution. The most cost-effective and least disruptive exercise is a tabletop exercise.
- As AnonCo' resilience matures, it is envisioned that supply chain partners or FICU partners may be invited to execute joint exercises to validate end-to-end BCPs.

Training, Exercises, and Testing

As part of the business continuity management function, training is provided to educate appropriate personnel on the organization's business continuity management goals and objectives, including, but not limited to:

- Significant business continuity concepts, interdependencies, disruption impacts, and operational resilience
- Results of exercises and testing
- Current and future risks facing the organization
- Recent failures to achieve business continuity goals and lessons learned
- New programs and technologies
- Organizational changes

The organization has implemented a comprehensive exercise and testing program for ongoing training and validation of business continuity assumptions. For more information, see the Exercise and Test Program section.

Monitoring, Updates, and Reporting

As changes in risks, technology, and organization processes are identified through ongoing monitoring, the business continuity plan is reviewed and updated to reflect the current environment. Areas to be considered in regular updates include:

- Operational, security, and alternate-facility requirements
- Technical procedures and vital records
- Hardware, software, and other equipment

- Contact information for team members and third parties

Reports are delivered to senior management and the board of directors over the status of the plan, including the BIA, risk assessment, business continuity risk management plans, exercise, test results, and identified issues. See the Revision/Approval Log for additional information.

Plan Maintenance

The plan owner will regularly update their business continuity plan(s), going through a formal review annually. All contact details documented in the business continuity plan will be updated annually or as they change by the Plan Owner. Employee contact information stored by departments for Business Continuity must comply with data protection policies.

Annual Review

The department will review this Business Continuity Plan, components, and supporting elements annually and make any required updates or changes. Any modifications to this plan will be documented on the title page of this document.

Plan Approval

The Plan Owner and Business Continuity Manager review the BCP (Business Continuity Plan) annually. The Plan Owner is responsible for maintaining and updating the plan as information or processes change. Each change will be reviewed with the Plan Approver and Business Continuity Manager for an in-depth understanding of this document.

Decision Process Matrix

Based on the type and severity of the emergency, the BCP may be activated by one of the following methods:

- Chief Technical Officer (CTO) or Chief Information Security Officer (CISO) initiates the activation of this plan.
- The Chief Executive Officer (CEO) or designated successor initiates this plan's activation for the entire organization based on an emergency or threat directed at the organization.
- The designee appointed by the Chief Executive Officer (CEO) initiates the activation of this plan.

BCP activation is a scenario-driven process that allows flexible and scalable responses to the full spectrum of emergencies and other events that could disrupt operations with or without warning during regular operation hours and after-hours. BCP activation is not required for all emergencies and disruptive situations since other actions may be deemed appropriate. The decision to activate this plan and related activities are tailored for the situation based upon projected or actual impact and severity that may occur with or without warning.

Assessing for Activation

In the lead-up to a disruptive event, or as a disruptive event begins, the Chief Executive Officer (CEO) and Chief Technical Officer (CTO) should monitor the situation. Leadership should assess their operational readiness and make necessary preparations for BCP activation. Triggers for activation should be based on a risk assessment. Considerations should include the following:

- Location of the disruption and potential impacts (e.g., organization disruption vs. targeted disruption).
- The business area's capacity to manage the disruption (i.e., could be controlled using existing management action).
- Stakeholder, political, media, or reputational implications.
- Time of year:
- End of Fiscal Year
- End of Fiscal Quarter
- Holidays
- Weather Events (Snow, Wind, Rain, Hail, etc...)
- Natural Disasters (Earthquake, Wildfire, etc...)
- Timing related to monthly department processes.
- Timing related to Annual Tax preparation.

Activation of a BCP may also be triggered by:

- An interdependent BCP is being activated.
- Advice from a resource recovery support area that an outage is likely to occur.
- The Business Continuity Coordinator if:
- Multiple critical business functions are impacted; senior management has information warrants activation.
- The department operates under disaster and emergency management arrangements (at the local, regional, departmental, or state level).

Activating the BCP

To activate a BCP, the BCP owner must escalate their assessment of the event and seek approval from the BCP approver. Following activation of a BCP, the BCP owner should immediately notify the following:

- Their immediate BCP escalation point. The BCP owner will notify the staff involved in implementing the BCP.
- IT, Facilities, HR − any interdependent functions (to ensure functions can adapt as needed and any related BCP(s) are activated).
- The BC/DR Coordinator has indicated that Executive leadership has invoked the organization's DR plan.

- Staff is not required in the BCP response (outlining what they need while managing the disruptive event).
- Customers and stakeholders (advising them how they might be affected)
- Communications Department for broader communication requirements.

Escalating Issues

Any issues identified should be escalated to the BCP Owner. They should notify the BCP approver of any escalated issues for it to:

- Maintain situational awareness.
- Recommend activating disaster and emergency management arrangements, if necessary and appropriate. Escalation may be required for several reasons, for example:
- The maximum acceptable outage is at risk of being exceeded.
- Minimum performance standards are at risk of not being achieved.
- There is insufficient capacity to implement the BCP with existing resources.
- Disruption's impact has increased in size, severity, and complexity.

The BCP Owner may decide the event requires a disaster and emergency management response. However, they must escalate this decision to Executive leadership. If Executive Leadership determines the event does require a disaster and emergency management response, they will activate the department's disaster and emergency management arrangements.

Deactivating BCP

The process for deactivating a Business Continuity Plan is broadly defined below. One or more of the following can start deactivating the plan. The plan owner and plan approver have the final authority on whether the plan or parts of the plan can and should be deactivated.

- No new or developing situations or outages.
- People, Processes, Buildings, or Technology have stabilized and are reporting as stable.
- Determine how any backlog of work and transition carried out under alternative arrangements will be actioned.
- Deactivating the plan is acceptable to Stakeholders.
- Interested parties have been communicated with and updated on the status.
- The BCP Owner should conduct a welfare check of staff impacted by the event and monitor staff wellbeing during the transition back to business as usual.
- Don't hesitate to contact the Employee Assistance Program (EAP) for assistance if there are welfare concerns.
- Prioritize which BCP activities can be stopped and transitioned back to business-as-usual and when.

- Post-mortem/ Continuous improvement has been scheduled, ideally within 24-48 hours after the deactivation of the BCP.
- Formal communication/ notification has been made to Stakeholders and Interested Parties.

When it has been determined that deactivating the plan is warranted, the plan owner will communicate formally via email to all interested parties and stakeholders that operations have been normalized.

Return to New or Renovated Work Site (Recovery)

Return to a new or renovated work site is a term used to cover the various tasks involved in recovering the work site and assets, which provide one of the foundations for the department's capability and capacity. Whether it is back to a refurbished headquarters facility or elsewhere, outlining the many tasks is outside the domain of this plan. However, this plan does outline those steps which involve the department. These include validating that the work site and assets are available and in satisfactory order before the services can resume at that renovated or new facility. In addition, as AnonCo' resilience capabilities continue to evolve, this section may be updated with who or what committee is responsible for renovation efforts and how they intend to engage the department.

Return to New or Renovated Work Site Overview

When a disruption occurs, the Crisis Management Team (CMT) manages the response to the incident. Part of the CMT's job is identifying and executing the return to a new or renovated work site. Site staff whose primary responsibility will be coordinating with the department to obtain concurrence on the extent of damage and how the workspace and assets will be made whole. The planning and coordination of repairs or acquisition of new space are coordinated with the IMT's return to new or renovated work site team. Still, they must engage the department and obtain agreement on the efforts.

Work Site Inspection

As the return to the new or renovated work site progresses, it is anticipated the department will walk through their work facility and use the facility and asset checklists below to validate that the work is satisfactory.

Facility Checklist

Department Workspace Checklist	Done	
Does the workspace meet the required amount of space?		
Are there changes of which the department was not aware?		

Will the change impact the operation's capability or capacity, and is management aware of that change?		
IF THE DEPARTMENT MOVES TO A NEW LOCATION - Are the other departments with which the business unit interacts aware of the new location, and are there any changes in how those departments interact with the department?		

3 Call Trees

In the event of an emergency situation, the personnel will be contacted in order of their appearance on each applicable list.

3.1 Business Tech Call Tree

Team Member 20 - w XXX-XXX-XXXX c XXX-XXX-XXXX

- Team Member 12 - w XXX-XXX-XXXX c XXX-XXX-XXXX
  - Team Member 08 - w XXX-XXX-XXXX c XXX-XXX-XXXX
  - Team Member 13 - w XXX-XXX-XXXX c XXX-XXX-XXXX
  - Team Member 01 - w XXX-XXX-XXXX c XXX-XXX-XXXX
  - Team Member 15 - w XXX-XXX-XXXX c XXX-XXX-XXXX
  - Team Member 22 - w XXX-XXX-XXXX c XXX-XXX-XXXX
  - Team Member 02 - w XXX-XXX-XXXX c XXX-XXX-XXXX
  - Team Member 04 - w XXX-XXX-XXXX c XXX-XXX-XXXX

3.2 Executive Leadership Call Tree

Team Member 23 - w XXX-XXX-XXXX c XXX-XXX-XXXX

- Team Member 09 - w XXX-XXX-XXXX c XXX-XXX-XXXX
  - Team Member 14 - w XXX-XXX-XXXX c XXX-XXX-XXXX
  - Team Member 10 - w XXX-XXX-XXXX c XXX-XXX-XXXX
  - Team Member 20 - w XXX-XXX-XXXX c XXX-XXX-XXXX
  - Team Member 21 - w XXX-XXX-XXXX c XXX-XXX-XXXX
    - Team Member 16 - w XXX-XXX-XXXX c XXX-XXX-XXXX
    - Team Member 03 - w XXX-XXX-XXXX c XXX-XXX-XXXX
  - Team Member 17 - w XXX-XXX-XXXX c XXX-XXX-XXXX
    - Team Member 06 - w XXX-XXX-XXXX
    - Team Member 05 - w XXX-XXX-XXXX c XXX-XXX-XXXX
  - Team Member 07 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 19 - w XXX-XXX-XXXX c XXX-XXX-XXXX

4 Emergency Locations

The following list defines the organization's emergency locations. Employees are to report to the evacuation locations in the event of an emergency evacuation such as a fire in the organization and to the shelter location in the event of a threat requiring shelter such as a tornado. At either location, supervisors will perform an employee rollcall and give further instructions as directed by the organization management.

Credit Union Alpha

Evacuation Location (Primary)	See Credit Union Alpha emergency plans for information
Evacuation Location (Secondary)	See Credit Union Alpha emergency plans for information
Shelter Location (Primary)	See Credit Union Alpha emergency plans for information
Shelter Location (Secondary)	See Credit Union Alpha emergency plans for information
Alternate Operating Location (Primary)	Anonymous Company - Site A [Address Redacted] Suite 100 [Redacted]
Alternate Operating Location (Secondary)	Remote Remote Location Your Home, Colorado 19426
Address	[Address Redacted] [Redacted]
Fire Extinguisher(s)	See Credit Union Alpha location of FE

Anonymous Company - Headquarters

Evacuation Location (Primary)	Front Northwestern portion of parking lot.
Evacuation Location (Secondary)	Remote Work Location

Shelter Location (Primary)	Interior location away from windows
Shelter Location (Secondary)	NA
Alternate Operating Location (Primary)	Remote Remote Location Your Home, Colorado 19426
Alternate Operating Location (Secondary)	Remote Remote Location Your Home, Colorado 19426
Address	[Address Redacted] Suite 200 [Redacted]
Fire Extinguisher(s)	Interior Walls, near bathroom, stair wells, and Network Closet. Total of 4
Is a Data Center	No

Remote

Evacuation Location (Primary)	Outside of remote location at a safe distance from the hazard
Evacuation Location (Secondary)	If safe, local 1st responder site (Fire, Police, Hospital)
Shelter Location (Primary)	Basement, interior room, or bathroom in the tub
Shelter Location (Secondary)	If safe, local 1st responder site (Fire, Police, Hospital)
Alternate Operating Location (Primary)	WeWork OnDemand or something similar at your location
Alternate Operating Location (Secondary)	Local Hotel Customer Business Office
Address	Remote Location Your Home, Colorado 19426

Fire Extinguisher(s)	These are remote locations owned by employees. There may or may not be fire mitigation.
Is a Data Center	No

5 Definitions

Criticality Levels

Criticality	Maximum Tolerable Downtime (MTD)
Critical	3 hours
Urgent	24 hours
Important	72 hours
Normal	7 days
Nonessential	30 days

Impact Categories

Impact Category	Insignificant	Low	Medium	High	Extreme
Compliance	Negligible compliance, contractual, regulatory, or legal concerns.	Potential for compliance, contractual, regulatory, or legal issues with minor implications.	Confirmed compliance, contractual, regulatory, or legal issues with moderate implications.	Major penalties and/or costs related to compliance, contractual, regulatory, or legal issues.	Extreme penalties related to compliance, contractual, regulatory, or legal issues (e.g., jail time for employees, closing of the organization, etc.)

Impact Category	Insignificant	Low	Medium	High	Extreme
Financial	Negligible direct loss/profit reduction (e.g., < $10,000 or < 1%).	Minor direct financial loss/profit reduction (e.g., < $100,000 or < 5%).	Moderate direct financial loss/profit reduction (e.g., < $500,000 or < 10%).	Major direct financial loss/profit reduction (e.g., < $1,000,000 or < 15%).	Extreme direct financial loss/profit reduction (e.g., > $1,000,000 or > 15%).
Operational	Negligible impact on operational functions.	Minor disruption to operations, staff, or supporting functions.	Moderate disruption to operations or sustained deterioration in working conditions.	Major disruption to operations or extended deterioration in working conditions.	Extreme disruption of operations or unacceptable working conditions.
Reputational	Negligible exposure or low impact that can be immediately remedied.	Minor exposure resulting in low impact that can be remedied at minimal cost.	Moderate exposure resulting in moderate-to-high impact that can be mitigated over time.	Major exposure resulting in high impact with the potential for long-term impact to the brand and reputation.	Extreme exposure resulting in high impact with the potential for irreversible damage to the brand and reputation.

6 Business Processes

Process	Criticality	Maximum Tolerable Downtime (MTD)
Business Technology Process	**Critical**	3 hours
Monthly Validations	**Critical**	3 hours
Bill Pay Flag updates	**Urgent**	24 hours
Bond File Redemption	**Urgent**	24 hours
CBR Reporting (Metro II)	**Urgent**	24 hours
Daily Tasks	**Urgent**	24 hours
Month End Statements	**Urgent**	24 hours
Rate Changes	**Urgent**	24 hours
Bill Pay Cleanup	**Important**	72 hours
Move Requests	**Important**	72 hours
Non-Monthly Validations	**Important**	72 hours
Quarterly Credit Score	**Normal**	7 days

6.1 Critical

6.1.1 Business Technology Process

Criticality	Critical
Maximum Tolerable Downtime (MTD)	3 hours

Responsibility

- Business Technology Support Department

Restoration Goal

Based on the organization's Business Impact Analysis (BIA) and operational needs during a disaster, management has identified the following objectives necessary to adequately restore this process:

Recovery Objective	Recovery Time Objective (RTO)
Return to normal operation	3 days

Other Business Processes Required

Based on the organization's Business Impact Analysis (BIA), organization management has identified the following business processes necessary to achieve the Restoration Goal defined above:

- Account Opening Process
- Core Banking Process
- Vendor Management Process

Staff Required

Based on the organization's Business Impact Analysis (BIA), organization management has identified the following skill sets necessary to achieve the Restoration Goal defined above:

- App Support-Online Banking Systems Specialist (1)

Third Parties Required

Based on the organization's Business Impact Analysis (BIA), organization management has identified the following critical third parties required for restoration of this process:

Third Party	Service	Contact
Amazon Web Services (AWS)	Web Hosting	XXX-XXX-XXXX
Socure	Identity Verification	
Temenos	Deposit Account Software	
Software Development Partner	Software Application Development	XXX-XXX-XXXX

See the Third-Party Contacts section for third-party contact information.

System/Equipment Required

Based on the organization's Business Impact Analysis (BIA), the organization's expected access to replacement system/equipment and implementation time requirements, organization management has identified the following system/equipment and time necessary to achieve the Restoration Goal defined above:

System/Equipment	Required for first Recovery Objective?
DNA Application (2)	No
DNA Database (2)	No
Internet Access (2)	No

See the System/Equipment Recovery Plan section for system/equipment recovery details.

Software Required

Based on the organization's Business Impact Analysis (BIA), organization management has identified the following software necessary to achieve the Restoration Goal defined above:

- Cisco AnyConnect (2)
- Google Chrome Web Browser (2)
- KeePass (2)
- Temenos JIRA Ticketing System (2)
- Development Partner JIRA Ticketing System (2)

Supplies Required

Based on the organization's Business Impact Analysis (BIA), organization management has identified the following supplies necessary to achieve the Restoration Goal defined above:

- Computer Audio Headset (2)
- Computer Keyboard (2)
- Computer Mice (2)
- Docking Station (2)
- External Monitors (2)
- Internet Connectivity (2)
- Laptop Computer (2)
- Mobile Phone (2)

6.1.2 Monthly Validations

Criticality	Critical
Maximum Tolerable Downtime (MTD)	3 hours

Responsibility

- Business Technology Support Department

Restoration Goal

Based on the organization's Business Impact Analysis (BIA) and operational needs during a disaster, management has identified the following objectives necessary to adequately restore this process:

Recovery Objective	Recovery Time Objective (RTO)
Return to normal operation	3 days

6.2 Urgent

6.2.1 Bill Pay Flag updates

Criticality	Urgent
Maximum Tolerable Downtime (MTD)	24 hours

Restoration Goal

Based on the organization's Business Impact Analysis (BIA) and operational needs during a disaster, management has identified the following objectives necessary to adequately restore this process:

Recovery Objective	Recovery Time Objective (RTO)
Return to normal operation	3 days

6.2.2 Bond File Redemption

Criticality	Urgent
Maximum Tolerable Downtime (MTD)	24 hours

Responsibility

- Business Technology Support Department

Restoration Goal

Based on the organization's Business Impact Analysis (BIA) and operational needs during a disaster, management has identified the following objectives necessary to adequately restore this process:

Recovery Objective	Recovery Time Objective (RTO)
Return to normal operation	3 days

6.2.3 CBR Reporting (Metro II)

Criticality	Urgent
Maximum Tolerable Downtime (MTD)	24 hours

Restoration Goal

Based on the organization's Business Impact Analysis (BIA) and operational needs during a disaster, management has identified the following objectives necessary to adequately restore this process:

Recovery Objective	Recovery Time Objective (RTO)
Return to normal operation	3 days

6.2.4 Daily Tasks

Criticality	Urgent

Maximum Tolerable Downtime (MTD)	24 hours

Responsibility

- Business Technology Support Department

Restoration Goal

Based on the organization's Business Impact Analysis (BIA) and operational needs during a disaster, management has identified the following objectives necessary to adequately restore this process:

Recovery Objective	Recovery Time Objective (RTO)
Return to normal operation	3 days

6.2.5 Month End Statements

Criticality	Urgent
Maximum Tolerable Downtime (MTD)	24 hours

Responsibility

- Business Technology Support Department

Restoration Goal

Based on the organization's Business Impact Analysis (BIA) and operational needs during a disaster, management has identified the following objectives necessary to adequately restore this process:

Recovery Objective	Recovery Time Objective (RTO)
Return to normal operation	3 days

6.2.6 Rate Changes

Criticality	Urgent

Maximum Tolerable Downtime (MTD)	24 hours

Responsibility

- Business Technology Support Department

Restoration Goal

Based on the organization's Business Impact Analysis (BIA) and operational needs during a disaster, management has identified the following objectives necessary to adequately restore this process:

Recovery Objective	Recovery Time Objective (RTO)
Return to normal operation	3 days

6.3 Important

6.3.1 Bill Pay Cleanup

Criticality	Important
Maximum Tolerable Downtime (MTD)	72 hours

Responsibility

- Business Technology Support Department

Restoration Goal

Based on the organization's Business Impact Analysis (BIA) and operational needs during a disaster, management has identified the following objectives necessary to adequately restore this process:

Recovery Objective	Recovery Time Objective (RTO)
Return to normal operation	3 days

6.3.2 Move Requests

Criticality	Important
Maximum Tolerable Downtime (MTD)	72 hours

Responsibility

- Business Technology Support Department

Restoration Goal

Based on the organization's Business Impact Analysis (BIA) and operational needs during a disaster, management has identified the following objectives necessary to adequately restore this process:

Recovery Objective	Recovery Time Objective (RTO)
Return to normal operation	3 days

6.3.3 Non-Monthly Validations

Criticality	Important
Maximum Tolerable Downtime (MTD)	72 hours

Responsibility

- Business Technology Support Department

Restoration Goal

Based on the organization's Business Impact Analysis (BIA) and operational needs during a disaster, management has identified the following objectives necessary to adequately restore this process:

Recovery Objective	Recovery Time Objective (RTO)
Return to normal operation	3 days

6.4 Normal

6.4.1 Quarterly Credit Score

Criticality	Normal
Maximum Tolerable Downtime (MTD)	7 days

Responsibility

- Business Technology Support Department

Restoration Goal

Based on the organization’s Business Impact Analysis (BIA) and operational needs during a disaster, management has identified the following objectives necessary to adequately restore this process:

Recovery Objective	Recovery Time Objective (RTO)
Return to normal operation	3 days

7 Escalation Process

Escalation from Major/Critical Incident Management

Activation of the DRP will result in most cases from the Critical Incident Management Plan (CIMP) escalation. Critical roles defined in the CIMP will continue or be created in the DRP. These critical roles are Critical Incident Manager (CIM), Critical Incident Technical Manager (CITM), and Critical Incident Documentation Specialist (CIDS). Their responsibilities are outlined in the CIMP and continue in the DRP. All communications and correspondence established in the CIMP, including distribution list, triage bridges, conference bridges, and WebEx™ sessions, carry forward into DRP. The DRP can be activated for the loss of a single service or up to and including the loss of a data center.

The first goal of the DRP is to assess and communicate the current status to the Executive team and customer base. This is necessary to approve a disaster event from the impacted customer(s). It is critical to decide on the declaration of a disaster as quickly as possible to limit the duration of the interruption. It is important to provide the team with current information to enable a fair review of the risks of the declaration with its current impact.

Suppose the service impact is like physical site damage to a production data center. In that case, the following subset of activities needs to be triggered to provide sufficient communication above the data gathered within critical incident management. The following outlines the actions required to assess physical location events.

The Critical Situation Management team will physically visit the site and make an initial determination of the extent of the damage. Based on their assessment, all or part of the DRP will be initiated. Detecting an event that could result in a disaster affecting credit union (CU) customers or information processing systems at the AnonCo primary data center is the responsibility of Technical Services, Facilities, Information Systems, or whoever first discovers or receives information about an emergency.

As soon as a situation occurs that could result in a severe disruption to service, the on-site personnel should contact the Service Desk or emergency authorities and then take the necessary steps to minimize property damage and injury to people in the vicinity. The following people must also be notified:

- Usually, the Chief Technology Officer, Director of Data Center Architecture, Manager of Systems Administration, and/or the Information Security group unless notification has been received through their alarm monitoring capabilities. Immediately notify these areas if the problem does not activate a normal alarm system.
- Building Contacts: Team Member 11 (owner) XXX-XXX-XXXX or Team Member 18 XXX-XXX-XXXX
- Once the appropriate authorities and building contacts have been notified, follow the *Critical Incident Management Process.* Creating a Critical Situation Management Communication team.
- The Operations and Systems Primary and Secondary contacts will be contacted by the Critical Situation Manager and/or their designees as appropriate.

If normal operations can be continued at the site and repairs can be started as soon as possible.

- Minor Damage: Processing can be restarted quickly with no special personnel recall.
- Anticipated downtime is less than one day.

- Damage could be due to hardware, software, mechanical equipment, electrical equipment, or the facility.

Procedures for physical damage are outlined below:

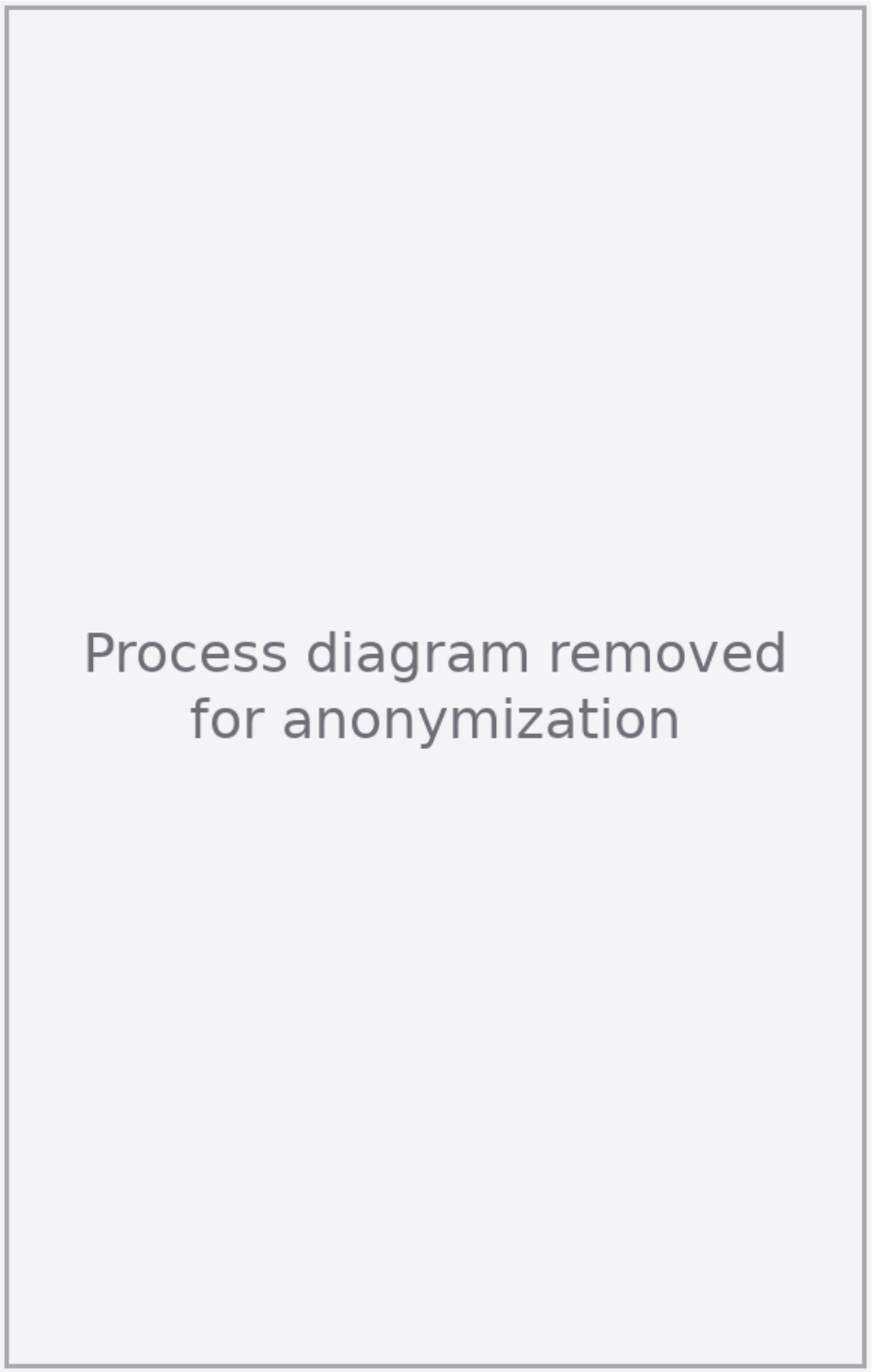
1. If the normal operation can be continued or restarted with the assistance of only certain recovery teams

- Major Damage: Selected teams will be called to direct the restoration of normal operations at the current site
- Major damage to hardware or facility

1. If limited operations can be continued at the site and plans started to repair or replace unusable equipment.
2. If the facility is destroyed to the extent that an alternate facility must be used

- Catastrophe: Damage is extensive
- Restoration will take upwards of one week
- The computer room or facility could be destroyed
- All team leaders will be called to begin a total implementation of the Contingency Plan to determine the extent that the DRP must be initiated.

1. The Management team will decide on its action plan and notify senior management. The Critical Situation Management team will escalate from the Critical Incident Management Process document to the policy outlining DR activation *AnonCo Business Continuity Management Program Policy*.
2. If further action requires the assistance of other recovery teams, those teams will be notified.



8 Cross Training

List the organization's key positions based on the positions identified in the "Staff Required" section of the Restoration of Processes section. Identify the people (primary and backup) that can fill each position.

Cross-Training Matrix

Position	Personnel
Business Technology Administrator	Team Member 01 Team Member 13 Team Member 22
Business Technology Manager	Team Member 12
Sr. Business Technology Administrator	Team Member 15
System Specialist	Team Member 02 Team Member 04 Team Member 08

9 Order of Succession

In the event of the loss or incapacity of senior or key management, the following order of succession will be followed. An asterisk marks a person that currently holds the position.

Business Technology Manager their successors.

Person	Job Title
Team Member 12*	Manager of Business Technology
Team Member 15	Sr. Business Technology Administrator

CEO their successors.

Person	Job Title
Team Member 23*	Chief Executive Officer
Team Member 21	Chief Technology Officer
Team Member 10	Chief Innovation Officer
Team Member 17	Chief Information Security Officer

10 Software

Software	Criticality
Bomgar	**Urgent**
Cisco AnyConnect	**Critical**
DUO MFA/ Mobile App	**Critical**
Monarch	**Important**
MS Edge Web Browser	**Critical**
MS Office 365 Suite	**Urgent**
MS Teams	**Critical**
NotePad ++	**Important**
Temenos JIRA Ticketing System	TBD
Velocity Warehouse	**Important**

Bomgar

Remote Desktop solution

Recovery

Criticality	Urgent

Cisco AnyConnect

Endpoint VPN client

Recovery

Criticality	Critical
Responsibility	End-User Services Dept

Recovery Details

Download the latest approved version of Cisco Anyconnect.

DUO MFA/ Mobile App

Recovery

Criticality	Critical
Responsibility	Systems Administration Dept

Monarch

Monarch is **a data preparation solution that can extract data from reports such as HTML, PDF, and XPS**

Recovery

Criticality	Important

MS Edge Web Browser

Recovery

Criticality	Critical
Responsibility	End-User Services Dept

MS Office 365 Suite

Recovery

Criticality	Urgent
Responsibility	End-User Services Dept

MS Teams

Recovery

Criticality	Critical
Responsibility	Systems Administration Dept

NotePad ++

Web Application URL	To_have_the_application_installed_please_submit_a_ticket_in_SysAid_or_if_SysAid_is_not_working_reach_out_to_End_User_Support

Recovery

Criticality	Important
Responsibility	End-User Services Dept

Temenos JIRA Ticketing System

Velocity Warehouse

Lending -copy of Velocity data accessible thru cView for the purpose of Data mining

Recovery

Criticality	Important

11 Systems/Equipment

System/Equipment	Criticality
Bill Pay CST Platform	Normal
Bomgar	Urgent
CU Branch Networks	Critical
CU Corporate Networks	Critical
cView	Critical
DNA Application	Critical
DNA Database	Critical
Fiserv Client 360	Urgent
ID Scanner	Urgent
iDenitfi	Critical
Internet Access	Critical
Internet Branch Locations	Critical
IQQ	Normal
Remote Access	Critical
SysAid	Critical
Temenos Ticketing System	Urgent
tMagic Check Scanner	Urgent
Topaz Device	Urgent
Venture Portal	Important
Watchdox	Important

Bill Pay CST Platform

Type	System

Recovery

Criticality	Normal

Bomgar

Bomgar is a remote support software that allows IT professionals to access and control remote computers and devices. It is used by businesses of all sizes to provide support to their employees, customers, and partners. Bomgar offers a variety of features that make it a valuable tool for IT professionals, including: Secure remote access: Bomgar uses a variety of security features to protect data and systems during remote access sessions, including two-factor authentication, encryption, and session recording. Robust session controls: Bomgar gives IT professionals complete control over remote sessions, including the ability to view, control, and transfer files, as well as chat with the user. Easy to use: Bomgar is easy to use for both IT professionals and end users. It has a simple, intuitive interface that makes it easy to get started and provides a variety of customization options to meet the specific needs of each organization.

Type	System

Recovery

Criticality	Urgent
Responsibility	End-User Services Dept

Recovery Plan

This app is not owned and is subject to an SLA with Vendor Management. In lieu of the SaaS being unavailable EUC can pivot to MS Teams or Webex and remote control endpoints.

Recovery Time	1 Day

Recovery Details

Systems/Equipment Dependencies	Internet Access

Software Required	• Cisco AnyConnect • Google Chrome Web Browser • MS Edge Web Browser

CU Branch Networks

Active-Active

Type	System

Recovery

Criticality	Critical
Responsibility	Data Center Architecture Dept
Backup Profile(s)	Tier 1 Replication (RTO/RPO 5 min)

Recovery Plan

Active-Active

Recovery Time	5 Minutes

CU Corporate Networks

Active-Active

Type	System

Recovery

Criticality	Critical
Responsibility	Data Center Architecture Dept
Backup Profile(s)	Tier 1 Replication (RTO/RPO 5 min)

Recovery Plan

Active-Active

Recovery Time	5 Minutes

cView

Active-Standby

Type	System

Recovery

Criticality	Critical
Responsibility	Application Support Dept
Backup Profile(s)	Tier 2 Replication (RTO/RPO 15 min)

Recovery Plan

Active-Standby

Recovery Time	15 Minutes

DNA Application

Active-Standby

Type	System

Recovery

Criticality	Critical
Responsibility	Application Support Dept
Backup Profile(s)	Tier 1 Replication (RTO/RPO 5 min)

Recovery Plan

Active-Active

Recovery Time	5 Minutes

DNA Database

Active-Standby

Type	System

Recovery

Criticality	Critical
Responsibility	Data Management Dept
Backup Profile(s)	• DEN - AnonCo SQL Retention • DEN - AnonCo SQL Retention - Transaction Logs • Tier 1 Replication (RTO/RPO 5 min)

Recovery Plan

Active-Standby

Recovery Time	5 Minutes

Fiserv Client 360

Type	System

Recovery

Criticality	Urgent

ID Scanner

Type Equipment

Recovery

Criticality Urgent

iDenitfi

Document storage

Type System

Recovery

Criticality Critical

Recovery Plan

Recovery Time 5 Minutes

Internet Access

Type System, Equipment

Recovery

Criticality Critical

Recovery Plan

Failover to other circuits. One via ATT the other via Lumen

Recovery Time 15 Minutes

Internet Branch Locations

Active-Standby

Type	System, Equipment

Recovery

Criticality	Critical
Responsibility	Data Center Architecture Dept
Backup Profile(s)	Tier 1 Replication (RTO/RPO 5 min)

Recovery Plan

Active-Standby

Recovery Time	5 Minutes

IQQ

Type	System

Recovery

Criticality	Normal

Remote Access

Active-Active

Type	System, Equipment

Recovery

Criticality	Critical

Responsibility	Data Center Architecture Dept
Backup Profile(s)	Tier 1 Replication (RTO/RPO 5 min)

Recovery Plan

Active-Active

Recovery Time	5 Minutes

Recovery Details

Physical Location	FLEXCO
Recovery Location	FLEXPHL

SysAid

SysAid is an IT service management (ITSM) software that helps businesses to manage their IT infrastructure and services. It provides a comprehensive set of features, including incident management, problem management, change management, asset management, and service desk. SysAid is easy to use and can be customized to meet the specific needs of any business.

Type	System

Recovery

Criticality	Critical
Responsibility	End-User Services Dept

Recovery Plan

This app is not owned and is subject to an SLA with Vendor Management.

Recovery Time	3 Days

Recovery Details

Systems/Equipment Dependencies	Internet Access
Software Required	• Google Chrome Web Browser • MS Edge Web Browser

Temenos Ticketing System

Type System

Recovery

Criticality Urgent

tMagic Check Scanner

Type System, Equipment

Recovery

Criticality Urgent

Topaz Device

Type Equipment

Recovery

Criticality Urgent

Venture Portal

Type System

Recovery

Criticality Important

Watchdox

Type System

Recovery

Criticality Important

12 Revision/Approval Log

Revision	Revision Date	Approval	Comments
1.0	10/31/2023		