**Building Community Resilience**

**Business Continuity Plan**

**Template and Guidance**

for

Non-Profit and Community-Based Organizations

A group of cubes

Description automatically generated with medium confidence

All content and tools have been developed and adapted

![A picture containing text

Description automatically generated]()![Red text on a white background

Description automatically generated]() by Coordinated Consulting Services, LLC in coordination with Mercy Corps

**Table of Contents**

[Part I: Introduction to Business Continuity Planning 1](#_Toc65082528)

[Business Continuity Plan (BCP) Template Instructions 1](#_Toc65082529)

[Business Continuity Plan Contacts Toolkit Instructions 2](#_Toc65082530)

[Part II: Business Continuity Plan (BCP) 3](#_Toc65082531)

[Introduction 3](#_Toc65082532)

[Organization Overview 3](#_Toc65082533)

[Purpose 3](#_Toc65082534)

[Risk Management 4](#_Toc65082535)

[Understanding and Mitigating Risk 4](#_Toc65082536)

[Hazard and Vulnerability Assessment 5](#_Toc65082537)

[Insurance 6](#_Toc65082538)

[Business Impact Assessment (BIA) 8](#_Toc65082539)

[Identifying and Prioritizing Essential Functions 9](#_Toc65082540)

[Continuity Personnel and Teams 10](#_Toc65082541)

[Business Continuity Planning Team 10](#_Toc65082542)

[Essential Function Leads and Backups 11](#_Toc65082543)

[Leadership Team 11](#_Toc65082544)

[Authority to Activate the BCP 12](#_Toc65082545)

[Orders of Succession 12](#_Toc65082546)

[Delegation of Authorities 13](#_Toc65082547)

[Communications and IT Systems 15](#_Toc65082548)

[Internal Communications 16](#_Toc65082549)

[External Communications 17](#_Toc65082550)

[IT Disaster Recovery 17](#_Toc65082551)

[Essential Records 18](#_Toc65082552)

[Essential Records **Error! Bookmark not defined.**](#_Toc65082553)

[Alternate Operations 19](#_Toc65082554)

[Telework (Partial or Full) 20](#_Toc65082555)

[Working from an Alternate Site 21](#_Toc65082556)

[Plan Testing, Updates, and Location 21](#_Toc65082557)

[Training, Drills, and Exercises 22](#_Toc65082558)

[Plan Updates 22](#_Toc65082559)

[Electronic and Hard Copy Plan Location 22](#_Toc65082560)

[Appendix A – Hazard and Vulnerability Assessment 24](#_Toc65082561)

[Appendix B – Business Impact Assessment (BIA) Tool 26](#_Toc65082562)

[Appendix C – Incident Action Plan Template 27](#_Toc65082563)

# Part I: Introduction to Business Continuity Planning

The *Business Continuity Plan Template and Guidance* *for Non-Profit and Community-Based Organizations* is designed to provide small, community-based or non-profit organizations with a tool for developing a business continuity plan.

An organization’s business continuity plan (BCP) is designed to capture resources and procedures needed to keep the business operations and essential services running under a broad range of emergencies. It can be helpful to think of these resources as “The 4 S’s” and those include Staff, Space (Facilities), Systems (Information Technology and Communications), and Stuff (Equipment and Supplies). This plan will ideally ensure that organizations can resume specific functions within 24 hours and up to 30 days after the disruption. The business continuity plan may be used to address a variety of situations, including loss or damage to a facility, loss and shortage of staff, loss of communication and technology systems, and the need for telework or remote operations.

This plan is different from the “emergency response procedures” like evacuation, fire, and medical emergencies. Emergency response plans or procedures will likely address an immediate emergency and require immediate action. The continuity plan focuses on sustaining operations that support the organization’s essential functions. For example, in an emergency response, you may be doing initial notifications of staff, external partners, and clients. Continuity planning addresses the systems you use to contact them and ensuring those systems are backed up and accessible. If your organization provides essential services to the community, your continuity plan will focus on ensuring the resources are in place to support these essential services, even when emergencies occur.

## Business Continuity Plan (BCP) Template Instructions

The headings in the BCP template are intended to be the section headings in the actual plan. The text under the headings gives a brief description of the information that should be captured in the plan section. The blue boxes within each section provide step-by-step instructions for completing the section.

This template includes additional tools designed assist the organization with determining the hazards and vulnerabilities of the organization, determining and prioritizing the essential functions of the organization, and finally, guiding the organization through a business continuity response. Instructions for using the following tools are shown in the green boxes within the template.

* Hazard and Vulnerability Assessment (HVA) Tool
* Business Impact Assessment (BIA) Tool
* Incident Action Plan (IAP) Template
* Business Continuity Plan (BCP) Contacts Toolkit

## Business Continuity Plan Contacts Toolkit Instructions

The BCP Contacts Toolkit is an Excel workbook used to capture contact information for function lead and backup staff, leadership staff, business continuity planning team members, external vendors, and general staff. The toolkit is included as an annex to the BCP Template and is a separate excel document.

|  |
| --- |
| BCP Contacts Toolkit Instructions:   1. Complete all other sections of the BCP Template before filling out the BCP Contact Toolkit. 2. Refer to the Continuity Personnel and Teams section of the template to determine the appropriate staff for the Leadership and Business Continuity Planning Teams. 3. In order to capture function leads and backups, list essential functions in the function leads and backups tab and list the staff and contact information. 4. In order to capture key vendors, copy the list of essential functions into the tab and list all vendors and other external support agencies that support the function. 5. Call and verify the contact information and establish a backup point of contact for each vendor or external partner. 6. Establish a strategy and timeline for gathering all contact information for designated staff and vendors. 7. Update contact lists every quarter ideally. |

# Part II: Business Continuity Plan (BCP)

# Introduction

## Organization Overview

|  |
| --- |
| Section Instructions:   1. Provide a brief narrative description of your organization. Include the following:  * organization’s name * description of what your organizations does or provides * description of clients / customers serviced * why it is important for your organization to continue providing services during an emergency or disaster |

## Purpose

|  |
| --- |
| Section Instructions:   1. Fill in the bold spaces with your organization’s name and remove bold text. 2. Edit content as needed to fit your organization and your BCP.   Hint: You may want to look at this section again after completing the plan to ensure the plan content and objectives are still accurate. |

The purpose of this business continuity plan (BCP) is to increase the likelihood that **[organization name]** is able to continue or quickly restore essential functions across a wide range of potential emergencies or disasters. The plan outlines the organization’s top hazards, the business impact assessment, essential functions and discusses mitigating factors, such as insurance. The plan defines essential continuity staff, including who has the authority to activate the plan and orders of succession and delegation of authorities for key positions. The plan discusses communications, information technology, and essential records in relation to business continuity. Considerations and procedures for alternate operations are documented in this BCP.

The objectives of the **[organization name]** BCP include:

* Ensuring safety of staff and clients /customers;
* Ensuring the continuous performance of essential functions during an

emergency;

* Protecting essential facilities, equipment, records, and other assets;
* Reducing or mitigating disruptions to operations;
* Achieving a timely and orderly recovery from an emergency and resumption of

full service to clients / customers and community members;

* Providing a foundation for continued leadership under all circumstances; and
* Complying with legal and statutory requirements.

# Risk Management

## Understanding and Mitigating Risk

|  |
| --- |
| Section Steps:   1. Fill in the bold lettering with your organization’s name and remove bold text. |

Small businesses and organizations are particularly vulnerable to emergencies and disasters. FEMA reports up to 40% of small businesses will not reopen immediately following a disaster and within a year of a natural disaster, an additional 25% of small businesses will close as a result of the disaster. Within three years of a natural disaster, up to 75% of small businesses or organizations without a continuity plan will fail as a result of disaster impacts. This is why it is critical for small business owners, non-government organizations, and not-for-profits to understand their risks and engage in activities to mitigate the risks and reduce vulnerabilities.

Risk management methods can be put into two categories: risk control and risk financing. Risk control involves reducing risk by avoiding risk, building redundant systems, or through enhancing resilience. As an example, when controlling risk, small businesses might choose a location outside of a flood zone or in a building that is retrofitted for earthquakes, plan for and document back-up procedures for essential work functions and processes and information technology, and plan for emergencies and disasters by documenting procedures and policies before an event occurs.

Risk financing involves planning ways to pay for losses related to emergencies and disasters. Acceptance or retention of risk involves using your own funds to pay for losses. Transfer of financial risk, using others’ funds to cover losses, refers to having insurance coverage for business losses or using a noninsurance transfer, such as, contracts or government assistance. A Harvard Business Review study cites the biggest reason that businesses fail after emergencies and disasters is lack of insurance or being underinsured.

Risk assessment for small businesses and organizations is critical for several reasons, including: a small labor force, informal organization, and relatively vulnerable financial status. In addition to ensuring adequate insurance coverage to mitigate the risks associated with emergencies and disasters, small businesses and organizations can conduct hazard and vulnerability assessments (HVAs) and business impact assessments (BIAs) as part of their business continuity planning. Understanding the hazards that the organization may be subject to and the impact of those hazards on the organization will help prioritize continuity resources toward those hazards that cause the greatest impact to the organization. In addition, a BIA will determine the essential work functions required for the organization to continue operations.

The following sections outline the HVA, insurance, and BIA for **[organization name].** These are important mitigating factors that the organization has engaged in during the business continuity planning process to build resilience.

## Hazard and Vulnerability Assessment

|  |
| --- |
| Section Steps:   1. Fill out Hazard and Vulnerability Assessment (HVA) Tool in Appendix A of this plan. 2. Fill in the bold lettering in this section with your organization’s name and location / address and remove bold text. 3. List the organization’s top hazards in this section, as determined by the HVA tool, and remove bold text. |

|  |
| --- |
| HVA Tool Instructions (Appendix A):   * 1. Hazards are broken down into natural, technological, and human-caused hazards. Each type is pre-populated with several hazards. They are not meant to be an all-inclusive list, but a basic list, relevant for most organizations in the Pacific Northwest or West Coast. * Pre-populated hazards can be removed if they are not relevant to the region or organization. * There is an empty row in each hazard type to add additional hazards that are relevant for the organization. (E.g., tsunami could be added for organizations near the coast or security system failure might be added for an organization that relies heavily on their security system.) * Additional blank rows can be added, as needed, to include additional hazards in the assessment.   1. Fill out the probability column for all hazards. Consider how often an event has happened in the region’s, community’s, or organization’s history. * Low (1) is equivalent to a hazard occurring in greater than 20 years. * Medium (2) is equivalent to a hazard occurring at least once in 20 years. * High (3) is equivalent to a hazard occurring at least once in 5 years. * Very High (4) is equivalent to a hazard occurring at least once a year.   1. Fill out the “impact to critical business assets” columns for all hazards. Work across the row for each hazard, considering impacts to staff, space, equipment/supplies, and information/communication systems. * Negligible (1): Injuries or illness are treatable with first aid, minor quality of life lost, shutdown of facility and services for 24 hours or less, and/or less than 10% of property severely damaged. * Marginal (2): Injuries and illnesses do not result in permanent disability, complete shutdown of facility for up to a week, and/or more than 10% of property is severely damaged. * Critical (3): Injuries or illnesses may result in permanent disability, complete shutdown of facilities for at least two weeks, and/or more than 25% of facility is severely damaged. * Catastrophic (4): Multiple deaths, complete shutdown of facility for longer than two weeks, and/or more than 50% of property is severely damaged.   1. Add the **impact columns** for staff, space, equipment/supplies, and information/communications systems. Place this score in the “totals” row at the bottom of the table. This will allow the organization to rank critical business assets from those most impacted across all disaster to least impacted across all disasters.   2. Add the four impacts for each hazard across **the row** and divide the total sum of the impacts for each hazard by 4. This number goes in the average impact column (the gray column).   3. Multiply the average impact number (in the gray column) by the probability (likelihood) for each hazard, this is the risk score and goes in the yellow column. |

A Hazard and Vulnerability Assessment (HVA) was conducted for **[organization name]** during the business continuity planning process. The current location of the organization was used during the assessment: **[address of the organization]**. The completed HVA tool is included as Appendix A.

The HVA tool generated a risk score for each potential hazard. The risk shows the potential impact to the organization and can be used to prioritize resources and create strategies for mitigation of the top-rated hazards. The top-rated hazards include:

* **Hazard #1**
* **Hazard #2**
* **Hazard #3**
* **Hazard #4**
* **Hazard #5**

## Insurance

|  |
| --- |
| Section Steps:   1. Fill in the bold spots in this section with your organization’s name and remove bold text. 2. Fill out the insurance table with contact information and policy numbers and details for the organization’s insurance provider. It is beneficial to have a back-up contact for the insurance provider. 3. The questions at the end of the section can be used to guide discussions with insurance professionals. There are several options for the questions box:  * Leave it as is for future reference or use. * Use it as a space to document answers to the questions. * Remove the questions and document any relevant insurance information in paragraph form in this section. |

Adequate insurance coverage will help the organization recover more rapidly from an emergency or disaster. This section documents **[organization name]** insurance provider, contact information, and policy numbers and details. Included in this section is a list of emergency / disaster insurance related questions that can help guide a discussion with insurance providers.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| INSURANCE CONTACT INFORMATION | | | | |
| Insurance Company: | | | Agent/Contact Name: | |
| Street Address: | | | Agent/Contact Office Telephone Number: | |
| City, State, Zip Code: | | | Agent/Contact Mobile Number: | |
| Telephone Number: | | | Agent/Contact Emergency Telephone Number: | |
| Fax Number: | | | Agent/Contact Email: | |
| 24-Hour Claim Phone Number: | | | Backup Contact Name: | |
| Website: | | | Backup Contact Information: | |
| INSURANCE POLICY INFORMATION | | | | |
| Type of Insurance | Policy Number | Deductibles | Policy Limits | Coverage  General Description) |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |
| --- |
| Emergency/Disaster Related Insurance Questions:   1. Does the organization need Flood Insurance? 2. Does the organization need Earthquake Insurance? 3. Does the organization need Business Income and Extra Expense Insurance? 4. How much insurance is the organization required to carry to avoid becoming a co-insurer? 5. What types of records and documentation will the insurance company want to see? 6. How will the organization’s emergency management program/BCP affect the organization’s rates? 7. To what extent is the organization covered for loss due to power loss? Is coverage provided for both on- and off-premises power loss? 8. What perils or causes of loss does the organization’s policy cover? 9. How will the organization’s property be valued? 10. Does the organization’s policy cover the cost of required upgrades to code? 11. What does the policy require the organization to do in the event of a loss? 12. Is the organization covered for lost income in the event of a business disruption because of a loss? Do the organization have enough coverage? For how long is coverage provided? How long is the organization’s coverage for lost income if the business is closed by order of civil authority? 13. To what extent is the organization covered for reduced income due to customers’/clients’ not all immediately coming back once the business reopens? |

## Business Impact Assessment (BIA)

|  |
| --- |
| Section Instructions:   1. Fill out BIA Tool in Appendix B of this plan. 2. Edit this section as needed for the organization. |

|  |
| --- |
| BIA Tool Instructions:   1. The Business Impact Assessment (BIA) Tool is designed to guide the organization through the process of identifying and prioritizing essential functions. Essential functions are the ones that need to be resumed within 30 days. There are sample functions in the tool to show how they are scored. The samples can be removed as you work on the tool. 2. List all of the day-to-day functions and programs of the organization. Make sure that the functions you list can be broken down into smaller groups of work (sometimes called “processes”). If the function cannot be broken down, it is probably too small to be called a “function.”  * Examples of organization functions include: * Payroll/Accounting * Staff Benefits * Safety/Security * Procurement * Purchasing * Contract/Grant Management * Internal Communications * External Communications * Essential Service Delivery (each service may be a function) * Essential Programs (each program may be a function)  1. For each function listed, and within each impact category, rate the level of impact to the organization. Total the impact scores. 2. Identify the time period when you would first anticipate these impacts to the organization. Take the impact score and multiply it by the time frame multiplier. This gives a business impact score (BIS) for each function. |

The BIA is a process for identifying and prioritizing the essential functions of an organization. It identifies functions that could be deferred during extended emergencies. It measures how the loss of specific functions would impact the organization, the specific types of impacts, and the ideal time period that the functions should ideally be resumed.

The BIA is also the basis for the BCP, which describes how essential functions will continue or be resumed, even during disruptions. Upon completion of the BIA tool, described in the next section, the organization will have a prioritized list of essential functions recovery time objectives that can be used to guide the response and recovery strategies when functions are disrupted.

## Identifying and Prioritizing Essential Functions

|  |
| --- |
| Section Instructions:   1. Refer to the completed BIA Tool for a list of scored essential functions. 2. Take the essential functions with the highest business impact scores and list them below in this section and remove bold text. List as many high priority essential functions as seems relevant to the organization. 3. Fill in the bold lettering in this section with your organization’s name and remove bold text. |

Essential functions are the ones that need to be resumed within 30 days. Some functions will need to be resumed within 0-24 hours, 2-3 days, 4-7 days, or within 8-30 days in order to reduce negative impacts to the organization. The BIA process helps an organization better understand the types of impact to the organization if functions are lost. Some examples of these impact categories include impacts to public image, impacts to service to vulnerable populations, impact to the health and safety of staff or clients, and regulatory, compliance, or legal considerations. **[Organization’s name]** essential functions are prioritized in the BIA Tool located in Appendix B. The essential functions with the highest BIS include:

* **Essential function #1**
* **Essential function #2**
* **Essential function #3**
* **Essential function #4**
* **Essential function #5**

# Continuity Personnel and Teams

|  |
| --- |
| Section Instructions:   1. Identify team members for each of the three teams (Business Continuity Planning Team, Essential Function Leads and Backups, and Leadership Team). 2. List team member titles in the Team Member lists for each team below. 3. Document the names and contact information in the BCP Contacts Toolkit (Excel doc). |

## Business Continuity Planning Team

In order to develop and maintain the BCP, it is important to establish a Business Continuity Planning Team (BCP Team). The team maybe be comprised of 1-2 people or if staffing allows, can be a larger team. The BCP Team responsibilities include:

* Meet regularly to develop and review each section of the BCP.
* The Business Continuity Lead will be responsible for filling out the template and documenting the information gathered in the meetings.
* Verifying information and providing subject matter expertise during plan development.
* Developing drills and exercises to test the BCP
* Keeping an improvement plan that identifies areas for improvement from each drill, exercise or real event.
* BCP Team Members may include:
  + **Business Continuity Lead**
  + **Subject Matter Experts (SMEs) from each area of the organization**
  + **Information Technology Lead**
  + **Facilities Lead**
  + **CEO/Director**
  + **Communications Lead**

## Essential Function Leads and Backups

Function Leads are personnel who have knowledge and expertise about a specific essential function. They understand the resources (staff, space, supplies, and systems) that support specific essential functions and could assist with getting a function up and running if it were disrupted. Sometimes, a function lead is a manager within in the agency, but that isn’t always true.

It is important to identify backup function leads in order to support continuity of essential functions. When identifying these backup positions, the organization may realize that only one person knows about certain functions or has access to specific information. In this case, organizations should work on cross-training back-up staff to be able to support essential functions and ensure they have adequate access to communication and IT systems, essential records, and databases.

Function Lead and Backup responsibilities include:

* Being available to respond to business disruptions when notified by the Leadership Team.
* Being prepared to report on the status of essential functions and whether they are fully operational, partially operational, or not operating during business disruptions.
* Contact external vendors and partners if necessary, during business disruptions.
* Assist with developing strategies for continuing or resuming essential functions during business disruptions.

## Leadership Team

The Leadership Team provides strategic direction for all phases of a business continuity response. This team will vary in size based on the size of the organization.

Leadership Team responsibilities include:

* Initial notifications of staff and function leads during emergencies and business disruptions
* CEO/Director may activate the BCP
* Manage all phases of the business disruption
* Notify Board of Directors and other key external partners
* Members of the Leadership Team may include:
  + **CEO/Director**
  + **Communications Lead**
  + **Program Managers**
  + **Human Resources Lead**
  + **Finance Lead**
  + **Other (as appointed by CEO/Director)**

## Authority to Activate the BCP

|  |
| --- |
| Section Instructions:   1. Add the title of the leadership position that will lead a business continuity response. 2. If the organization is able to outline a procedure for convening the Leadership Team, that can be added by creating additional steps. (E.g., The Leadership Team will be contacted by email if available. If email is not available, then a text message will be sent.) |

At the onset of an emergency or disaster, it may not be possible for specific staff to initiate a business continuity response or disaster operations. Therefore, it is necessary to have a flexible procedure to begin the response and convene the responsible staff members. At the onset of a business disruption the following procedure applies:

1. The Leadership Teamwill be convened to access the situation and determine if the BCP will be activated.
2. If BCP is activated, the **[leadership position]** or designee will be responsible for guiding the business continuity response until relieved of their position by another designated lead.

## Orders of Succession

|  |
| --- |
| Section Instructions:   1. Fill out of the Order of Succession table.  * Identify the key leadership and management positions in the first column. * Identify at least one successor for each key leadership and management position. * If possible, identify a second and third successor for key positions. |

In the wake of an emergency or major disaster impacting the organization or region, key staff may be ill, injured, caring for loved ones, deceased, or otherwise unable to report to work. As a result, it is necessary to have a procedure for filling these vacated positions (either temporarily or permanently) and giving authority to individuals who are able to work. Best practices dictate that at least two individuals, identified by position/title, are identified to replace key positions. Below are considerations for the establishment and initiation of the orders of succession process.

* Positions (not names) that assume a particular role under specific circumstances are listed in the tables below.
* Positions may be prescribed by statute, order, or directive.
* There should be a “succession procedure” that specifies under what circumstances succession would occur and the method of notification.
* Orders of succession are primarily for leadership positions and key managers.
* Successors serve until formally appointed by the appropriate authority, replaced, or relieved.

**Table 1 – Order of Succession**

| **Key Position** | **Successor 1** | **Successor 2** | **Successor 3** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Delegation of Authorities

|  |
| --- |
| Section Instructions:   1. Fill out the Delegation of Authorities table.  * List key leadership and management positions in the first column. These can be the same list of key leadership and management positions in the Order of Successions table. * For each position listed, fill in the rest of the row, identifying: * “Yes” that person has the same authorities in that category as the highest leadership position listed. * “No” they do not have any authorities in that category. * “E” for exception, that they do have authorities in that category, but there are exceptions. Note the specific exception in the chart (e.g., E- $60,000). * Examples in the table can be removed. |

Delegations of authority denote a pre-determined transfer of responsibility that takes effect when normal channels of succession have been disrupted. These delegated authorities will lapse when these channels have been reestablished. This provides successors with the legal or organizational authority to act on behalf of another person for a specific purpose.

The following list of authorities may act as a guideline when planning for delegation of authorities:

* Expenditure approval
* Release of financial information (to auditors, taxing authorities, bankers, the public, or other constituencies)
* Hiring and firing
* Information Technology (adding new users or adding new software)
* Supervisory/management duties (assigning work, scheduling, leave authorization, etc.)
* Alert and notifications (if needed specify who can notify which audiences)
* Emergency authorization (activating emergency plans/continuity plans, relocation, staffing changes)
* Release of public information

The following Delegation of Authorities table summarizes the authorities and any exceptions for each key position. “Yes” refers to a position having all the authorities in that category. “No” refers to the position not having any authorities in that category. “E” stands for exceptions and refers to the position having authorities in that category, but with certain exceptions.

**Table 2 – Delegation of Authorities**

| **Authority** | **Expenditure Approval** | **Release of Financial Info.** | **Hiring and firing** | **IT** | **Mgmt. / Supervisory Duties** | **Alert and Notifications** | **Emergency Authorization** | **Release of Public Info.** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Position** |
| Executive Director | $ 100,000 | Yes | Yes | No | Yes | Yes | Yes | Yes |
| Assistant Director | E- $60,000 | No | Yes | No | Yes | Yes | Yes | Yes |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

# Communications and IT Systems

|  |
| --- |
| Section Instructions:   1. Fill in the bold lettering in this section with your organization’s name and remove bold text. 2. Go back to the organization’s list of essential functions from the BIA Tool in Appendix B. 3. Fill out Table 3 – Essential IT and Communication Systems.  * Copy the organization’s essential functions in the left column. (Essential Functions were identified during the Business Impact Assessment in Appendix B.) * For each essential function, list the critical IT systems needed for the function to operate. * For each essential function, list the communication systems or platforms needed for the function to operate.  1. Fill out Table 4 – Audiences and Priority Systems.  * There is a pre-populated list of audiences in the left column. Edit this list (remove or add audiences) to align with the organization. * For each audience, provide a brief note describing the audience. * For each audience, list the priority communication systems used to communicate with that audience. |

Communications and IT systems are critical to **[organization’s name]** operations. IT systems are resources that support most, if not all, essential functions. In addition, the delivery of clear, timely, accurate, and consistent messaging and notifications is critical to any continuity of operations or disaster response and is often dependent on specific IT and communication systems. Communication systems refer to the equipment and platforms used to communicate (i.e., texts, email systems, notification systems, phone calls, radios etc.). Table 3 below lists the communication and IT systems by function that the organization will use, if available, during a business disruption.

Table 4 lists and describes the different audiences the organization may need to establish communication with during a business disruption. Both internal staff and external partners and vendors must be informed on a regular basis throughout the incident. Table 4 also notes priority systems that are used for each audience.

**Table 3 – Essential IT and Communication Systems**

|  |  |  |
| --- | --- | --- |
| **Essential Function** | **IT Systems**  (Google Suite, HRIS, OnGuard, VPN, network drives, finance or payroll systems, etc.) | **Communication Systems/Platforms**  (E.g., text, email, VOIP/landline phone, radios, Skype or Zoom, WhatsApp, Slack, social media, etc.) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Table 4 – Audiences and Communications Systems**

| **Audience** | **Description of Audience** | **Communications Systems** |
| --- | --- | --- |
| Staff/Employees |  |  |
| Clients/Customers |  |  |
| Vendors/Contractors |  |  |
| Regulatory Agencies |  |  |
| Other Stakeholders |  |  |
|  |  |  |

## Internal Communications

|  |
| --- |
| Section Instructions:   1. If the organization has a communications staff person or team, consider changing the responsibility in this section from Leadership Team to Communications Staff or Team. |

It is important to develop ongoing messaging as the organization responds to business disruptions and develops alternate operations strategies. The Leadership Team must keep staff informed of the situation, the organization’s strategy to manage the business disruption, and any changes to procedures and policies. The following list contains considerations for internal communications:

* Refer employees to local emergency response organizations for emergent and changing information.
* Align messaging with relevant authorities.
* Ensure employees are notified of the primary and redundant communication systems being utilized during the incident.
* Employees should be reminded to check the organization’s communication systems regularly and frequently.
* Clear messaging is particularly important in emergencies and disasters. Present information in sequence:
  + Reason for the message
  + Supporting Information
  + Conclusion
  + Where to go for more information
* Ensure messaging is consistent across varying communication systems for redundant communications.

## External Communications

|  |
| --- |
| Section Instructions:   1. If the organization has a communications staff person or team, consider changing the responsibility in this section from Leadership Team to Communications Staff or Team. |

Once the Leadership Team has developed internal communications strategies, they will need to develop external communication strategies for clients / customers, media engagement, public messaging, and other external stakeholders. The following list contains considerations for external communications:

* Align messaging with relevant authorities and response partners.
* Ensure messaging is consistent across varying media sources.
* Ensure communication systems are reliable during the emergency or disaster.
* Choose systems that are appropriate for the level of urgency needed.

# IT Disaster Recovery

|  |
| --- |
| Section Instructions:   1. If the organization has specific IT disaster recovery procedures, they can be added into or referenced in this section. 2. If the organization hires a service to provide IT disaster recovery or back-up services, include the contact information in the BCP Contact Lists, External Vendors tab. |

IT Disaster Recovery is an organization’s strategy and procedures for regaining access to and operations of the IT infrastructure and systems after emergencies or disasters. Data security and back-up should be an ongoing process; however, it is crucial before an emergency or disaster. IT Disaster Recovery plans and procedures are usually developed and managed by an IT lead staff person within an organization. If the organization uses a contractor for IT support, they should be included in your business continuity and recovery planning. If the organization does not have a lead IT staff person or contractor, best practice recommends developing an IT disaster recovery plan and having separate storage for critical IT systems and data.

Key Components of a disaster recovery plan:

* Disaster recovery team: Identify a specialist or team of specialists that will be responsible for creating, implementing and managing the disaster recovery plan.
* Risk evaluation: Focus on hazards with the highest impact scores in the Information Technology and Communications column of the HVA in Appendix A.
* Essential functions: Focus on IT systems and applications that are required for the essential functions with the highest business impact scores.
* Backups: Determine what needs back-up (or to be relocated) based on risk evaluation and essential functions, who should perform backups, and how backups will be implemented. The amount of downtime an organization can handle and how frequently the organization backs up its data will inform the disaster recovery strategy.
* Testing and optimization: The disaster recovery specialist or team should continually test and update its strategy to address ever-changing threats and business needs. By continually ensuring that a company is ready to face the worst-case scenarios in disaster situations, it can successfully navigate such challenges.

# Essential Records

|  |
| --- |
| Section Instructions:   1. Go back to your list of essential functions from the BIA Tool. 2. For each essential function, list the record name, record type, and storage location in the Essential Records and Access table in this section. |

Essential records are the records you would need, after a disaster, in order to continue your mission and are needed to perform one or more of your essential functions. These are the records you need to service both your internal and external clients and may be near impossible to recreate if lost. Examples of essential records include emergency plans, policies, and procedures; maps and building plans; systems manuals; employee data, contact lists, and payroll; client records; financial and insurance records; titles, deeds, and contracts; licenses and long-term permits; emergency purchasing records; customer data; and legal and lease documents.

|  |  |  |
| --- | --- | --- |
| **Record Name** | **Record Type**  (E.g., paper, electronic, web-based, etc.) | **Location**  (E.g., on-site, network drive, cloud-based, etc.) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Alternate Operations

|  |
| --- |
| Section Instructions:   1. Fill in the bold lettering in this section with your organization’s name and location and remove bold text. 2. Use the considerations /questions as a guide to plan for alternate operations. There are three options:  * The information can be added directly into the section under each question. * The questions can be removed from the plan and used to develop more detailed procedures that are then placed in the plan. * Leave the questions in the plan as in and use them as a guide during future planning or during a business disruption. |

|  |
| --- |
| Incident Action Plan (IAP) Template Instructions (Appendix C):   1. The IAP will only be used during a business disruption to maintain situational awareness, by documenting objectives, operational periods, needed resources, staff assignments, and safety considerations. 2. The IAP can become a permanent record to document the organization’s response to a business continuity event. |

This section documents procedures for alternate operations. When the organization is not able to operate according to standard operating procedures, the organization is functioning in alternate operations. Alternate operations strategies will be utilized for any emergency or disaster that leaves the **[organization’s name]** facility in **[county or city location of organization]** inaccessible or inhabitable. This may include, but is not limited to, extended disruption of utility services to the facility (water, sewer, air, heat, electricity) or damage to the facility. Alternate operations strategies will also be utilized while safety and structural assessments of the facility are being performed and if public infrastructure damage (e.g., roads, public transportation) or severe weather inhibits travel to the facility. Two alternate operations strategies, telework and alternate site, are listed below with considerations for each.

When the organization is experiencing a business disruption and developing and implementing an alternate operations strategy, an Incident Action Plan (IAP) will be used to document the situation, objectives, needed resources, assignments, and safety issues. The IAP template is located in Appendix C and can be filled out throughout the business disruption at intervals that capture the changing environment.

## Telework (Partial or Full)

A telework strategy involves employees working from their homes. Telework can be partial, with employees working at home, but still able to come to the facility for brief periods of time, or a hybrid work-from-home and work-from-facility schedule. Partial telework could also be set up with certain employees assigned to telework, and some are assigned to work at the facility. Full telework would entire all employees teleworking with no access to the facility. The following questions can be used ahead of an emergency or disaster to develop a plan for telework or during a business disruption to facilitate telework.

### Telework Considerations:

Staff:

* Which positions are able to complete work processes as a teleworker?
* Which employees are NOT able to telework?
* Do any adjustments to workload need to be made as staff transition to telework?

Stuff (Equipment/Supplies):

* What IT equipment do teleworkers need to complete their work processes?
* What other equipment or supplies do teleworkers need to complete their work processes?

Systems (IT/Communications)

* How will employees access IT systems, applications, and communication systems remotely?
* Do employees need VPN to access work remotely?
* What systems and platforms should employees use to communicate internally and to hold internal and external meetings?
* Will the organization assist employees with the cost of improved broadband for increased telework functioning?

## Working from an Alternate Site

An alternate site strategy involves employees working for an alternate temporary location while the permanent site is unavailable. Alternate operations could have some employees working from home and some employee working from an alternate site. The following considerations and questions can be used ahead of an emergency or disaster to develop an alternate site plan or during a business disruption to facilitate transitioning to an alternate site.

0

### Alternate Site Considerations:

Staff:

* Staff ability to commute to an alternate facility.
* Teams that need to work together to complete essential functions.
* Availability of services in the facility and in the area for staff.

Space (Facility):

* Consider commuter routes and access to public transportation and parking.
* Consider capacity within the space and prioritize space for essential functions with the highest BIS scores.
* If space is limited in the alternate site, consider assigning staff to work in shifts.
* Are needed utilities available at the alternate site?

Stuff (Equipment/Supplies):

* What equipment and supplies need to be set up at the alternate site?
* Who is in charge of setting up the alternate site?

Systems (IT/Communications):

* Are IT and communication systems set up at the alternate facility?

# Plan Testing, Updates, and Location

|  |
| --- |
| Section Steps:   1. Fill in the bold lettering in this section with your organization’s name and remove bold text. 2. Edit the following section to fit in with the organization’s training, drills, and exercise goals. Currently these are noted to be done on an annual basis. If this is not feasible, adjust the time interval to meet the needs and capacity of the organization. 3. Edit the section on Plan Updates to meet the needs of the organization. This is also noted to be plan updates annually. If this is not often enough or too often for the organization adjust the time interval. 4. Edit the Electronic and Hard Copy Plan Location section to align with the organization and identify specifically where the electronic version on the plan will be kept and where hard copies of the plan will be kept at the work site. |

## Training, Drills, and Exercises

The identification and training of staff to sustain business continuity is critical. The best plans will be of little assistance, if staff do not understand their roles and responsibilities in an emergency or disaster. Staff must be knowledge of the BCP and other emergency and crisis plans. Participation in ongoing training, drills, and exercises must be required of staff on a regular basis. BCP training will be provided to employees on an annual basis. Additional training will be provided as needed to account for staff turnover and reassignment.

Along with training, exercises provide an opportunity for staff to become familiar with continuity plans and procedures. Exercises may take the form of a simple drill (e.g., fire drill or communications drill), a tabletop exercise (i.e., a facilitated scenario-based discussion about a possible event), or participation in a more complex, functional exercise with community partners. At a minimum, **[organization name]** staff will participate in a drill or exercise once a year.

## Plan Updates

The **[organization’s name]** BCP will undergo regularly scheduled updates on an annual basis. Scheduled updates include a review of the plan and updating any changes to reflect organizational changes, procedural changes, new system capabilities, equipment upgrades, new hazards, and other relevant changes to the organization’s operating environment. Scheduled annual updates should coincide with the yearly business continuity training and drill or exercise. Lessons learned from drills and exercises can be used to update the plan and to set priorities for future training and continuity planning priorities within the organization. Contact lists associated with business continuity will be updated quarterly.

Unscheduled plan updates will occur after any real-world emergencies or disasters that cause a business disruption and should not wait for the annually scheduled update. Any major changes to staffing, facility, equipment, operations, etc. should trigger an unscheduled plan update.

## Electronic and Hard Copy Plan Location

The BCP will be stored both electronically and in hard copy form. The plan should be readily and easily accessible by key staff with a role in business continuity and all **[organization’s name]** staff.

The electronic version of the BCP will be kept on the **[computer drive or location]** in a folder called Business Continuity. The BCP Toolkit will be kept on this shared drive as well. Shared drive access will require internet access. Hard copies of the plan will be kept in the following location(s) at **[organization’s name]**:

* **Hard copy plan location**
* **Hard copy plan location**

Key staff will need to access the BCP from home, during non-work hours, if an emergency or disaster occurs outside of the organization’s normal business hours. These key staff will be provided a hard copy of the plan to keep at home or in an emergency go-bag.

# Appendix A – Hazard and Vulnerability Assessment

|  | | | **IMPACT TO CRITICAL BUSINESS ASSETS** | | | |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| HAZARD TYPE | HAZARD EVENT | PROBABILITY  *(Likelihood)*  1 = Low  2 = Medium  3 = High  4 = Very High | STAFF  *(Availability, illness, injury, or death)* | SPACE  *(Damage and loss)* | EQUIPMENT/  SUPPLIES  *(Unable to access, operate, damage, & loss)* | INFORMATION / COMMUNICATION  SYSTEMS  *(Unable to access, operate, damage, & loss)* | AVERAGE  IMPACT  Sum of impacts, divided by 4 | RISK SCORE  Average Impact x Prob. |
| 1 = Negligible  2 = Marginal  3 = Critical  4 = Catastrophic | 1 = Negligible  2 = Marginal  3 = Critical  4 = Catastrophic | 1 = Negligible  2 = Marginal  3 = Critical  4 = Catastrophic | 1 = Negligible  2 = Marginal  3 = Critical  4 = Catastrophic |
| Natural | Severe Weather *(Windstorm, Extreme Cold/Heat, Winter Weather)* |  |  |  |  |  |  |  |
|  | Earthquake |  |  |  |  |  |  |  |
|  | Flood |  |  |  |  |  |  |  |
|  | Wildfire |  |  |  |  |  |  |  |
|  | Pandemic / Infectious Disease Outbreaks |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| Techno-logical | Power Outage |  |  |  |  |  |  |  |
|  | Water Failure |  |  |  |  |  |  |  |
|  | HVAC Failure |  |  |  |  |  |  |  |
|  | Internal Fire |  |  |  |  |  |  |  |
|  | External Fire |  |  |  |  |  |  |  |
|  | Supply Shortage |  |  |  |  |  |  |  |
|  | IT/Comms Failure |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| Human | Workplace Violence |  |  |  |  |  |  |  |
|  | Armed Intruder / Active Shooter |  |  |  |  |  |  |  |
|  | Bomb Threat |  |  |  |  |  |  |  |
|  | Cyber Attack |  |  |  |  |  |  |  |
|  | Civil Disturbance |  |  |  |  |  |  |  |
|  | Chemical Release *(Accidental or Intentional)* |  |  |  |  |  |  |  |
|  | Biological Terrorism *(Anthrax, Smallpox)* |  |  |  |  |  |  |  |
|  | Terrorism Explosion |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | TOTALS |  |  |  |  |  |  |  |

# Appendix B – Business Impact Assessment (BIA) Tool

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Department/ Agency Name:** |  | | | | | | | | |
|  | **IF THIS FUNCTION WERE DISRUPTED FOR 0-30 DAYS, TO WHAT DEGREE WILL THE AGENCY HAVE:** | | | | | |  |  |  |
|  | **Missed contract or grant obligations?** | **Financial or revenue impacts?** | **Regulatory, compliance or legal liability impacts?** | **Public image impacts?** | **Impacts to health and safety of staff or clients?** | **Interruption of direct services to vulnerable populations?** | **Total Impact** | **Time Frame Multiplier**  0-24 hours (x4)  2-3 days (x3)  4-7 days (x2)  8-30 days (x1) | BUSINESS IMPACT  SCORE |
| No Impact (0)  Low Impact (1)  Med Impact (2)  High Impact (3) | No Impact (0)  Low Impact (1)  Med Impact (2)  High Impact (3) | No Impact (0)  Low Impact (1)  Med Impact (2)  High Impact (3) | No Impact (0)  Low Impact (1)  Med Impact (2)  High Impact (3) | No Impact (0)  Low Impact (1)  Med Impact (2)  High Impact (3) | No Impact (0)  Low Impact (1)  Med Impact (2)  High Impact (3) |
| ESSENTIAL FUNCTION |  |  |  |  |  |  |  |  |  |
| Payroll | 0 | 1 | 1 | 1 | 3 | 0 | 6 | 4-7 days (x2) | 12 |
| Meal Delivery | 2 | 0 | 1 | 3 | 3 | 3 | 12 | 2-3 days (x3) | 36 |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| TOTALS |  |  |  |  |  |  |  |  |  |

# Appendix C – Incident Action Plan Template

|  |  |  |
| --- | --- | --- |
| **Incident Action Plan** | | |
| **Incident Name:** | | **Operational Period:** (from date/time to date/time) |
| **Objectives:**  (including alternate operations strategies) | | |
| **Situational Awareness:**  (size, scope, effect, or potential effect of the incident to the organization) | | |
| **Identify Resources Needed:** | | |
| **Issue Assignments:** | | |
| **Safety Considerations:** | | |
| **Communication Plan:**  **Internal:**  **External:** | | |
| **IAP Approved by:**  (name & title) | **Signature:**  **Date/Time:** | |