**Name of Organization**

**Business Impact Analysis Template**

December 2021

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes Made | Changed By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Instructions

This (Name of Organization) Business Impact Analysis document is designated For Official Use Only (FOUO) and is the property of (Name of Organization). Only (Name of Organization) representatives may distribute this document to individuals on a need-to-know basis. Distribution by other individuals without prior authorization is prohibited. The handbook is unclassified but contains sensitive information.

**Table of Contents**

[I. Introduction and Purpose 5](#_Toc90308955)

[II. Scope 6](#_Toc90308956)

[III. System Description 6](#_Toc90308957)

[IV. BIA Data Collection 6](#_Toc90308958)

[Determine Process and System Criticality 7](#_Toc90308959)

[Identify Outage Impacts and Estimated Downtime 8](#_Toc90308960)

[Outage Impacts 8](#_Toc90308961)

[Estimated Downtime 9](#_Toc90308962)

[Alternate Mode (Business Continuity) 10](#_Toc90308963)

[Identify Resource Requirements 10](#_Toc90308964)

[Identify Recovery Priorities for System Resources 10](#_Toc90308965)

# Introduction and Purpose

This Business Impact Analysis (BIA) document is developed as part of the contingency planning process for the [System/System Name]. To quickly show status and progress of analysis over time the BIA history table below should be completed for every analysis exercise:

|  |  |  |  |
| --- | --- | --- | --- |
| Report Date | Current System Owner | Summary of Changes Since Last | Approved By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

The purpose of a BIA is to identify and prioritize system components by correlating them to the mission/business process(es) the system supports and use this information to characterize the impact on the process(es) if the system were to become unavailable.

BIA is composed of the following three steps:

1. **Determine mission/business processes and recovery criticality.** Mission/business processes supported and/or enabled by the system are identified and the impact of a system disruption to those processes is determined, along with outage impacts and estimated downtime. The downtime should reflect the maximum outage that an organization can tolerate while still maintaining the overall operation.
2. **Identify resource requirements.** Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, finance, and vital records.
3. **Identify recovery priorities for system resources.** Based upon the results from the previous activities, system resources can more clearly be linked to critical mission/business processes. Priority levels can be established for sequencing recovery activities and resources.

This document is used to build the [System/System Name] Information System Contingency Plan (ISCP) and is included as a key component of the ISCP. It may also be used to support the development of other contingency plans associated with the system, including, but not limited to, the Disaster Recovery Plan (DRP) or Incident Response Plan (IRP), also known as “the Plan.”

# Scope

All (Name of Organization) employees, contractors, part-time and temporary workers, and those employed by others to perform work on Organization premises or who have been granted access to Organization information or systems, are covered by the standard that covers this document and must comply with associated guidelines, procedures, and regulations.

# System Description

*(Provide a general description of system architecture and functionality. Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures. Provide a diagram of the architecture, including inputs and outputs and telecommunications connections.*

*Note: Information for this section should be available from the system’s System Security Plan (SSP) (if applicable) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this BIA document.)*

# BIA Data Collection

*(Data collection can be accomplished through individual/group interviews, workshops, email, questionnaires, or any combination thereof.)*

## Determine Process and System Criticality

Working with input from users, managers, mission/business process owners, and other internal or external points of contact (POC), list the specific mission/business processes that depend on or support the information system.

|  |  |
| --- | --- |
| Business Process | Description |
| *e.g., Accounts Payable* | *Accounts Payable is a short-term debt payment process which needs to operate to ensure timely payments to avoid late payment fines or fees. AP process would fail if this system were to become unavailable.* |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## Identify Outage Impacts and Estimated Downtime

*(This section identifies and characterizes the types of impact categories that a system disruption is likely to create in addition to those identified by the FIPS 199 impact level, as well as the estimated downtime that the organization can tolerate for a given process. Impact categories should be created, and values assigned to these categories to measure the level or type of impact a disruption may cause. An example of cost as an impact category is provided. Organizations could consider other categories like harm to individuals and ability to perform mission. The template should be revised to reflect what is appropriate for the organization.)*

### Outage Impacts

*(Impact categories and values should be created to characterize levels of severity to the organization that would result for that impact category if the mission/business process could not be performed. These impact categories and values are samples and should be revised to reflect what is appropriate for the organization.)*

The following impact categories represent important areas for consideration in the event of a disruption or impact.

Impact Category: **Cost**

|  |  |
| --- | --- |
| Severe | Estimated Cost\* exceeding $XX |
| Moderate | Estimated Cost\* between $XX and $XX |
| Low | Estimated Cost\* up to $XX |

*\* Including fines, fees, penalties, liabilities, etc.*

Impact Category: [Category Name]

|  |  |
| --- | --- |
| Severe | [Impact Value] |
| Moderate | [Impact Value] |
| Low | [Impact Value] |

Impact Category: [Category Name]

|  |  |
| --- | --- |
| Severe | [Impact Value] |
| Moderate | [Impact Value] |
| Low | [Impact Value] |

The table below summarizes the impact on each mission/business process if [System/System Name] were unavailable, based on the following criteria:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Business Process | Impact Category | | | |
| Cost | Cat. Name | Cat. Name | Impact |
| *Accounts Payable* | *Moderate* | *Low* | *Moderate* | *Moderate* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Estimated Downtime

Working directly with mission/business process owners, departmental staff, managers, and other stakeholders, estimate the downtime factors for consideration due to a disruptive event.

* **Maximum Tolerable Downtime (MTD).** The MTD represents the total amount of time leaders/managers are willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because continuity planners need precise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.
* **Recovery Time Objective (RTO).** RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD, including provision of expensive Disaster Recovery capabilities.
* **Recovery Point Objective (RPO).** The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data must be recovered (given the most recent backup copy of the data) after an outage.

The table below identifies the MTD, RTO, and RPO (as applicable) for the organizational mission/business processes that rely on [System/System Name]. *(Values for MTDs and RPOs are expected to be specific time frames, identified in hourly increments (i.e., 8 hours, 36 hours, 97 hours, etc.).)*

|  |  |  |  |
| --- | --- | --- | --- |
| Business Process | MTD | RTO | RPO |
| *Accounts Payable* | *72 hours* | *48 hours* | *12 hours* |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*(Include a description of the drivers for the MTD, RTO, and RPOs listed in the table above (e.g., mandate, workload, performance measure, etc.).)*

### Alternate Mode (Business Continuity)

The table below identifies the Alternate Mode, an alternate means (secondary processing, or manual workaround) for recovering the mission/business process(es) that rely on the system. If no Alternate Mode exists, a gap exists that bears consideration for remediation.

|  |  |
| --- | --- |
| Business Process | Alternate Mode |
| *Accounts Payable* | *Manual Processing via Ledger* |
|  |  |
|  |  |
|  |  |

## Identify Resource Requirements

The following table identifies the resources that compose [System/System Name] including hardware, software, and other resources such as data files.

|  |  |  |
| --- | --- | --- |
| System Resource | Platform/OS/Model | Description |
| *Web Server* | *Win 2K12 VM* | *Company.com website* |
|  |  |  |
|  |  |  |
|  |  |  |

It is assumed that all identified resources support the mission/business processes identified during the Determine Process and System Criticality process unless otherwise stated.

*Note: Information for this section should be available from the system’s System Security Plan (SSP) (if applicable) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan.*

## Identify Recovery Priorities for System Resources

The table below lists the order of recovery for [System/System Name] resources. The table also identifies the expected time for recovering the resource following a “worst case” (complete rebuild/repair or replacement) disruption.

* **Recovery Time Objective (RTO)**. RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.

|  |  |  |
| --- | --- | --- |
| System Resource | RTO | Recovery Modality |
| *Web Server config and data* | *24 hours* | *Restore from backup* |
| *Web Server new VM* | *4 hours* | *Spin up from gold image* |
|  |  |  |
|  |  |  |

*(A system resource can be software, data files, servers, or other hardware and should be identified individually or as a logical group.*

*Identify any alternate strategies in place to meet expected RTOs. This includes backup or spare equipment and vendor support contracts.)*