**Atlas Archive**

Business Impact Analysis

USAO/TXW

March 16, 2023

Template Version: Fiscal Year 2022

Revision History

START OF INSTRUCTIONS: The following table summarizes the revision history of this template. The collective author for each revision of this template is the Cybersecurity Services Staff. **Remove the revision history for this template from the table below when updating this template for a specific information system and then enter revision information specific for that system’s Business Impact Analysis.** END OF INSTRUCTIONS

The following table summarizes the revision history of this document. The collective author for each revision of this document is the Provide Component or Organizational Unit Name Here.

| Release | Summary of Revisions | Date |
| --- | --- | --- |
| 1.0 | Baseline version. | 02/22/2017 |
| 1.1 | Accessible version. | 04/19/2017 |
| FY18 | * Updated for FY18 with minor corrections * Updated to include feedback from ISO20k external audit | 12/13/2017 |
| FY19 | * Updated for FY19 with minor corrections and formatting updates * Updated use instructions * Restricted editing to specific content/areas to maintain template integrity * Relabeled remaining appendices | 09/11/2018 |
| FY20 | * Updated cover page to clarify template version * Updated default footer to Limited Official Use * Updated Appendix O BIA to include system risk assessments | 10/17/2019 |
| FY22 | * Separated BIA to be separate document * Updated to new DOJ OCIO document template * Updated section and table numbers * Updated Section 2.3 to include requirement for system dependency resource documentation and assessment | 09/01/2021 |

instructions

How to use this template:

* Use the current/latest version of this [template](https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/index.php) as-is, without structural modifications
* Use of this template is **MANDATORY** for DOJ information system Business Impact Analyses (BIAs) required for systems that are part of the DOJ or Hybrid operating models (See ISCP Planning Guide Tables 1 and 3 for more details)
* The **BIA must be reviewed annually** **prior** to reviewing/updating the Information System Contingency Plan (ISCP) to ensure nothing has changed in the system’s mission, and to help inform updates to the system ISCP
* Editing of this document is restricted to the content contained in highlighted brackets ([])
* Text is marked as follows:
  1. Component/System-specific information that the Component will include in this document:
     + Enter your information directly over the requested text in highlighted brackets ([]) that begins with the word “Provide”
  2. Instructions that explain what is to be done or provided in each section by the Component/System Owner are contained within brackets ([]) and are marked with the words “START OF INSTRUCTIONS” and “END OF INSTRUCTIONS”
     + Delete the instructions after completing the section or document
* Use this template **as-is**… do not remove any sections that do not apply to the given information system; instead, remove the boilerplate text for such sections, and provide a brief statement explaining why the section does not apply
* Use this template **as-is**… do not add any sections to this template. If additional information is required that does not fit within the sections provided, include it in Appendix A at the end of this template.
* When done editing this template for an information system, update the Contents, Tables and any Figures list’s page numbers in the Table of Contents section (right-click in desired section, select “Update Field” and then select “Update Entire Table” and click “OK”)
* This template is marked Limited Official Use (LOU). Update the markings as appropriate for information systems with other classifications.
* Direct questions or comments regarding this document to the Component’s Policy Analyst
* You may delete this instruction page from the final document if desired

| CONTENTS |
| --- |

[Section 1 – Introduction 6](#_Toc80189449)

[1.1 Overview 6](#_Toc80189450)

[1.1.1 Introduction 6](#_Toc80189451)

[1.2 Purpose 6](#_Toc80189452)

[1.3 System Description 7](#_Toc80189454)

[Section 2 – Mission or business function assessments 8](#_Toc80189455)

[2.1 Mission or Business Functions and System Criticality 8](#_Toc80189456)

[2.2 Mission/Business Function Outage effects and Estimated Downtime 8](#_Toc80189457)

[2.2.1 Outage Effects 8](#_Toc80189458)

[2.2.2 Estimated Downtime 9](#_Toc80189460)

[2.3 Resource and dependency Requirements and Availability Risks 10](#_Toc80189461)

[2.3.1 Example/Sample Availability Risks 10](#_Toc80189462)

[Section 3 – Workarounds and Resource Requirements 15](#_Toc80189463)

[3.1 Workarounds – Peak Activity 15](#_Toc80189464)

[3.2 Work Area Requirements 15](#_Toc80189465)

[Section 4 – Recovery Priorities 17](#_Toc80189466)

[Appendix A – Additional Information 18](#_Toc80189467)

**TABLES**

[Table 1: Primary Point of Contact Information 6](#_Toc79482869)

[Table 2: Process Description 8](#_Toc79482870)

[Table 3: System Outage Effects and Impact Valuations 9](#_Toc79482871)

[Table 4: Estimated Downtime 10](#_Toc79482872)

[Table 5: Risk Assessment Scoring Heat Map 11](#_Toc79482873)

[Table 6: System Resources/Dependencies and Availability Risk Assessment 12](#_Toc79482874)

[Table 7: Resource Requirements 15](#_Toc79482875)

[Table 8: Point in Time Personnel Requirements 15](#_Toc79482876)

[Table 9: Point in Time Resource Requirements 16](#_Toc79482877)

[Table 10: Recovery Priorities 17](#_Toc79482878)

**FIGURES**

No table of figures entries found.**Note:** When in hard copy, this document is not a controlled copy and does not necessarily reflect the latest version. This is a living document and will be subject to change due to revisions in plans, funding availability, or other factors.

# Introduction

## Overview

### Introduction

This Business Impact Analysis (BIA) is a part of the contingency planning process for Provide System Name.

The BIA identifies key sources of information for each system business function, including the following details:

* Primary Point of Contact (PPOC)
* System Description
* The non-financial impact due to an outage
* Estimated recovery timeframes
* Availability risk assessment, and system operational dependencies
* Workarounds and periods of peak activity
* Work area requirements
* Critical points and resources required by your system/business function
* Recovery priorities

#### Primary Point of Contact

START OF INSTRUCTIONS: Complete the information below, which is required to identify the organizational unit’s primary point of contact for the information system. END OF INSTRUCTIONS

Table 1: Primary Point of Contact Information

| **Contact Type** | **Contact Details** |
| --- | --- |
| **Organizational Unit:** | Provide Organizational Unit Name |
| **Name:** | Provide PPOC Name |
| **Title:** | Provide PPOC Title |
| **Phone Number (Desk & Mobile):** | Provide PPOC Desk and Mobile Phone Numbers |
| **E-mail Address:** | Provide PPOC E-mail Address |

## Purpose

This is a foundational document to build the Provide System Name Information System Contingency Plan (ISCP).

The BIA identifies and prioritizes system components by correlating them to the mission(s) and/or business function(s) the system supports, and uses this information to characterize the impact on said mission(s) and/or business function(s) if the system was unavailable.

## System Description

START OF INSTRUCTIONS: To complete this section, document developers should follow the National Institute of Standards and Technology guidance, which states:

“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) 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.” END OF INSTRUCTIONS

# Mission or business function assessments

## Mission or Business Functions and System Criticality

START OF INSTRUCTIONS: Working with input from users, managers, mission/business process owners, and other internal points of contact, identify the specific missions or business functions that depend on or support the information system.

In Table 2 below, list and provide a brief description of the individual mission(s) and/or business function(s) that the specific information system enables or supports. Examples of missions/business functions include financial reporting, claims processing, legal research, litigation support, etc., as applicable to the information system. END OF INSTRUCTIONS

Table 2 identifies the specific missions or business functions that depend on or support the information system and reflects the missions the information system enables, not the functions the system performs, nor the tasks needed to ensure the system’s functionality.

Table 2: Process Description

| Mission or Business Function | Description |
| --- | --- |
| Provide System-Specific Mission/Business Function Here or N/A | Provide Mission/Business Function Description Here or N/A |
| Add Rows as Needed | Add Rows as Needed |

## Mission/Business Function Outage effects and Estimated Downtime

This section identifies and characterizes the types of effects that a system disruption is likely to create, in addition to those identified by Federal Information Processing Standard 199 (i.e., loss of confidentiality, integrity or availability), and the estimated downtime that the organization can tolerate for a given process.

### Outage Effects

START OF INSTRUCTIONS: Example/sample mission/business function outage effect descriptions are provided below. Review this list and revise it as necessary to document the effects an outage of the system could have on the mission(s) or business function(s) it provides to customers/Components. END OF INSTRUCTIONS

The following outage effects represent important areas for consideration in the event of a disruption to normal operation of Provide System Name. Table 3 identifies the impact valuation(s) if the outage effect were to occur.

C = Significant Increase in Operating Costs

E = Negative Impact on Employees

F = Fines, Penalties, Litigation

K = Stakeholder Impact

L = Legal Ramifications or Contractual Agreements

M = Negative Media Impact

O = Others to be Specified

P = Impact Productivity of the Office of the Chief Information Officer customer

Q = Quality of Service to Customer

R = Regulatory Compliance

S = Security Implications

Table 3: System Outage Effects and Impact Valuations

| **Mission or Business Function** | **Outage Effect (Selected from list above)** | **Impact Rating**  **(Table 5: 1 to 3)** | **Explanation** |
| --- | --- | --- | --- |
| Provide System-Specific Mission/Business Function Here or N/A | Provide Area of Outage Impact Here or N/A | Provide Outage Impact Rating Here or N/A | Provide Outage Impact Explanation Here or N/A |
| Add Rows as Needed | Add Rows as Needed | Add Rows as Needed | Add Rows as Needed |

### Estimated Downtime

Working with mission/business function owners, Business Relationship Management (BRM), departmental staff, managers, and other stakeholders, the following downtime consideration estimations are documented in Table 4 for the organizational mission/business functions that rely on Provide System Name:

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

Table 4: Estimated Downtime

| **Mission or Business Function** | **Maximum Tolerable Downtime** | **RTO** | **RPO** |
| --- | --- | --- | --- |
| Provide System-Specific Mission/Business Function Here or N/A | Provide Mission/Business Function Maximum Tolerable Downtime Here or N/A | Provide Mission/Business Function RTO Here or N/A | Provide Mission/Business Function RPO Here or N/A |
| Add Rows as Needed | Add Rows as Needed | Add Rows as Needed | Add Rows as Needed |

## Resource and dependency Requirements and Availability Risks

This section identifies the resources and dependencies (other internal or external services, systems, and infrastructure) that comprise and support Provide System Name during normal operations. This list includes hardware, software, and other resources, such as data files, data centers, infrastructure services (e.g., power, data, heating, ventilation, and air-conditioning (HVAC), etc.), etc. It also identifies and assesses the potential risks affecting the availability of the system, and the probability of their occurring, the impact(s) if they did, and the overall risk priority.

### Example/Sample Availability Risks

START OF INSTRUCTIONS: Example/sample risks are provided below that could affect the overall availability of the information system, including its individual component resources/assets or supporting dependency resources/assets. Review this list and revise it as necessary to document the availability risks that could affect this system, its individual components, or dependencies. END OF INSTRUCTIONS

A = System/Device Failure (Partial or Complete)

B = Dependency Failure (e.g., network, power, other system, etc.)

C = Cyber Security Incident (e.g., malware, Denial-of-Service attack, etc.)

D = Human Error

E = Natural Disaster (e.g., fire, flood, earthquake, etc.)

F = Hosting Facility/Data Center Failure (e.g., internal power or data, fire suppression malfunction, generator failure, etc.)

G = Lack of Human Capital

#### Risk Assessment Scoring Heat Map

Use Table 5 to determine the risk prioritization, based on the likelihood of the risk occurring, and the impact to the systems/resource/dependency if it did occur.

Table 5: Risk Assessment Scoring Heat Map

|  |  | **Impact** | | |
| --- | --- | --- | --- | --- |
|  |  | **1 = Low** | **2 = Medium** | **3 = High** |
|  | * Impact will not significantly affect ability to achieve one or more of objectives or performance goals * Limited impact on organization, interested parties, processes, functions, services, operations, information assets or information security * Limited to no impact on reputation | * Impact could moderately affect ability to achieve one or more objectives or performance goals * Moderate impact on organization, interested parties, processes, functions, services, operations, information assets or information security * May cause service outage * Potential negative impact on reputation | * Impact could preclude or highly impair ability to achieve one or more objectives or performance goals * Major impact on organization, interested parties, processes, functions, services, operations, information assets or information security * Would cause service outage * Would cause security incident, breach of PII or misuse of funds * Negative impact on reputation |
| **Probability** | **3 = High**   * Would occur at least once or more than once per year * 45 – 100% | **2 = Medium** | **3 = High** | **3 = High** |
| **2 = Medium**   * Would occur in the next two (2) years * 21 – 44% | **1 = Low** | **2 = Medium** | **3 = High** |
| **1 = Low**   * Would occur in two (2) to five (5) years * 0 – 20% | **1 = Low** | **1 = Low** | **2 = Medium** |

#### Resources and Availability Risks

The risks to availability of system or dependency resources, assets or infrastructure identified in Table 6 could impact mission or business functions provided by the information system.

START OF INSTRUCTIONS: In Table 6, list the hardware, software, and other resources, such as data files, data centers, infrastructure services (e.g., power, data, heating, ventilation, and air-conditioning (HVAC), etc.), etc., that comprise or support the entire information system. Then fill in details about the resources or assets listed, their description, RTO in order to recover the entire system within its stated RTO, and then individual risks to the availability of the resource or asset (from the list in Section 2.3.1 above). For each risk documented, system owners/teams must specify if the risk still requires mitigation or not, and if it does, open a POA&M(s) to track resolution of the risk(s) and record the POA&M ID in Table 6 below. Assign numerical values for risk probability and risk impact from Table 5 above to each risk identified. Correlate the risk priority for each individual risk identified by comparing the probability and impact for each risk, from Table 5 (e.g., if the probability of an identified risk is “2” (medium) and the impact of the same risk is “3” (high), the priority of that specific risk is “3” (high)). Then compute the average availability risk for the specific resource or asset by adding all the numerical risk priorities together and dividing by the total number of risks identified for the resource or asset. Finally, add all of the average risk priorities from all of the system resources or assets together, divide by the total number of resources or assets listed, and place that number in the last row to derive the “Average System Availability Risk Score.” END OF INSTRUCTIONS

Table 6: System Resources/Dependencies and Availability Risk Assessment

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **System/ Dependency Resource, Asset, or Infrastructure Name** | **Description** (Including Purpose, Platform, Operating System, Version, etc.) | **RTO** | **Availability Risk(s)**  (Select from Section 2.3.1) | **Risk Requires Mitigation** (Yes/No) | **POA&M ID** (Only if mitigation = “Yes”, else “N/A”) | **Risk Probability Rating(s)**  (Select from Table 5:  1 to 3) | **Risk Impact Rating(s)**  (Select from Table 5:  1 to 3) | **Individual Risk Priority(ies)**  (Select from Table5: 1 to 3) | **Average Risk Priority** |
| Provide System/Dependency Resource, Asset or Infrastructure Name Here or N/A. Examples: ESXi Server, CEF-E, Mainframe Services, etc. | Provide System, Dependency Resource, Asset or Infrastructure Description Here or N/A. Example:  Virtual environment host VMware ESXi 6.7.0 U3, Data Center Power, IBM v2.3, etc. | Provide System, Dependency Resource, Asset or Infrastructure RTO Here or N/A. Example:  4 Hours | Provide System, Dependency Resource, Asset or Infrastructure Availability Risk(s) Here or N/A. Example:  A  B  C  E  F | Provide Yes or No for Each Risk Identified in Previous Column Here or N/A. Example:  No  No  Yes  Yes  No | Provide ID for POA&M(s) Opened for All Risks Requiring Mitigation Here or N/A. Example:  N/A  N/A  12345  67890  N/A | Provide Risk Probability Rating(s) Here or N/A. Example:  3  3  2  1  2 | Provide Risk Impact Rating(s) Here or N/A. Example:  3  3  3  2  3 | Provide Risk Priority Rating(s) Here or N/A (Example: 3, 3, 3, 1, 3) | Provide Computed Average of Individual Risk Priority Cell Values to Nearest Whole Number (summed risk values divided by total values given) Here or N/A. Example: 3 |
| Add Rows as Needed (**Right Click🡪Select “Insert”🡪Select “Insert Rows Above”**) | Add Rows as Needed (**Right Click🡪Select “Insert”🡪Select “Insert Rows Above”**) | Add Rows as Needed (**Right Click🡪Select “Insert”🡪Select “Insert Rows Above”**) | Add Rows as Needed (**Right Click🡪Select “Insert”🡪Select “Insert Rows Above”**) | Add Rows as Needed (**Right Click🡪Select “Insert”🡪Select “Insert Rows Above”**) | Add Rows as Needed (**Right Click🡪Select “Insert”🡪Select “Insert Rows Above”**) | Add Rows as Needed (**Right Click🡪Select “Insert”🡪Select “Insert Rows Above”**) | Add Rows as Needed (**Right Click🡪Select “Insert”🡪Select “Insert Rows Above”**) | Add Rows as Needed (**Right Click🡪Select “Insert”🡪Select “Insert Rows Above”**) | Add Rows as Needed (**Right Click🡪Select “Insert”🡪Select “Insert Rows Above”**) |
| **Average System Availability Risk Score** | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | Provide Computed Average of Total Average Risk Priority Column Values to Nearest Whole Number (summed risk values divided by total values given) Here or N/A (Example: 3 (Moderate)) |

# Workarounds and Resource Requirements

## Workarounds – Peak Activity

Table 7 lists the greatest times of risk to the mission/business function if Provide System Name were to go down, along with any available workarounds to an outage.

Table 7: Resource Requirements

| **Mission or Business Function** | **Time of Greatest Risk** | **Potential Workaround/Mitigation** |
| --- | --- | --- |
| Provide System-Specific Mission/Business Function Here or N/A | Provide Time of Greatest Risk to Mission/Business Function Here or N/A | Provide Potential Workaround/Mitigation Here or N/A |
| Add Rows as Needed | Add Rows as Needed | Add Rows as Needed |

Noted below are other peak load or stress considerations:

* START OF INSTRUCTIONS: If there are no other considerations to note, enter “Not Applicable” here. END OF INSTRUCTIONS

## Work Area Requirements

Support requirements (staff, space, office equipment, etc.) for the information system under normal operations, and continuity operations, are described in Tables 8 and 9.

Current Staffing Level for Provide System Name

START OF INSTRUCTIONS: Specify the minimum (critical personnel), maximum and additional number of employees required to keep the system operational at specific time intervals during an incident. END OF INSTRUCTIONS

Components should assume each employee requires a desk and chair, laptop or desktop, and phone at an alternate work site.

Table 8: Point in Time Personnel Requirements

| **Requirements** | **<12 hours** | **<24 hours** | **<36 hours** | **<48 hours** | **<72 hours** | **>72 hours** | **>30 days** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Minimum Employees** | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. |
| **Maximum Employees** | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. |
| **Additional Employee Requirements** | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. |

In addition to employee requirements, there may also be unique work area business resources (e.g., specialized equipment or hardware and software) required to maintain system operations at the time of the disaster.

Table 9: Point in Time Resource Requirements

| **Required Resource** | **<12 hours** | **<24 hours** | **<36 hours** | **<48 hours** | **<72 hours** | **>72 hours** | **>30 days** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Cell is intentionally left blank so that the user can enter specific content | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. |
| Cell is intentionally left blank so that the user can enter specific content | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. |
| Cell is intentionally left blank so that the user can enter specific content | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. | This data cell is intentionally left blank. Enter Component-specific content here. |

# Recovery Priorities

Table 10 provides the order of recovery for each Provide System Name resource (including dependency services/systems) documented in Table 6. The table also identifies the expected RTO for each resource following a “worst case” (complete rebuild/repair or replacement) disruption.

Table 10: Recovery Priorities

| **Priority** | **System/Dependency Resource** | **RTO** |
| --- | --- | --- |
| 1 | Provide System/Dependency Resource Name/Description Here or Mark “N/A” | Provide System/ Dependency Resource RTO Here or Mark “N/A” |
| Add Rows as Necessary | Add Rows as Necessary | Add Rows as Necessary |

###### Additional Information

START OF INSTRUCTIONS: Include any additional information that did not fit in other sections of this BIA template. Be sure to reference the section(s) in this BIA to which the additional information applies; otherwise, enter “Not Applicable” for this section. END OF INSTRUCTIONS