Prepared by Cub Cyber based on NIST 800-34, Rev 1

BUSINESS IMPACT ANALYSIS (BIA)

www.cubcyber.com

{Your Company Name}

{Your Company Logo}

{Information System Name}

{Date Last Edited}

TABLE OF CONTENTS

1. OVERVIEW

This Business Impact Analysis (BIA) is developed as part of the contingency planning process for the {system name} It was prepared on {insert BIA completion date}.

1.1 Purpose

The purpose of the BIA is to identify and prioritize system components by correlating them to the mission/business process(es) the system supports, and using this information to characterize the impact on the process(es) if the system were unavailable. The BIA is composed of the following three steps: 1. Determine mission/business processes and recovery criticality. Mission/business processes supported 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 that an organization can tolerate while still maintaining the mission. 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, 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 name} Information System Contingency Plan (ISCP) and is included as a key component of the ISCP. It also may 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 Cyber Incident Response Plan.

2. SYSTEM DESCRIPTION

{Insert System description from your system security plan}

3. BIA DATA COLLECTION

{Describe how you collected data for the BIA. For example: interviews with employees and groups to determine important mission/business processes and systems}

3.1 Determine Process and System Criticality

Mission/Business Process	Description
e.g. Pay vendor invoice	*e.g. Process of obligating funds, issuing check or electronic payment and acknowledging receipt.*

3.1.1 Identify Outage Impacts and Estimate Downtime

You may add or remove impact categories to best suit your organization’s needs.

Outage Impacts

Impact Values			
Impact Category	Severe	Moderate	Minimal
Financial	*{define what constitutes a severe financial loss to your company}*	*{define what constitutes a moderate financial loss to your company}*	*{define what constitutes a minimal financial loss to your company}*
Service Delivery	*{define what constitutes a severe inability to deliver services to your clients}*	*{define what constitutes a moderate inability to deliver services to your clients}*	*{define what constitutes a minimal inability to deliver services to your clients}*
Image/Credibility	*{define what constitutes a severe impact to your company’s image}*	*{define what constitutes a moderate impact to your company’s image}*	*{define what constitutes a minimal impact to your company’s image}*

Mission/Business Process	Impact Category			
	Financial	**Service Delivery**	**Image/Credibility**	**Impact**
e.g. Pay vendor invoice	*e.g. minimal*	*e.g. minimal*	*e.g. moderate*	*e.g. minimal*

Estimated Downtime

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 it could leave continuity planners with imprecise 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.

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 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.).*

Mission/Business Process	Dependent System (s)	MTD	RTO	RPO
e.g. Pay vendor invoice		*e.g. 72 hours*	*e.g. 48 hours*	*e.g. 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.). Include a description of any alternate means (secondary processing or manual work-around) for recovering the mission/business process(es) that rely on the system. If none exist, so state.}

3.2 Identify Resource Requirements

{Cite or include system resources form the hardware list of your System Security Plan}

3.3 Identify Recovery Priorities for System Resources

The table below lists the order of recovery for {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) 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.

Priority	System Resource	Function/Role	Recovery Time Objective (RTO)
e.g. high	*e.g. OptiplexGX280*	*e.g. Webserver*	*e.g. 24 hours to rebuild or replace*

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.

RECORD OF CHANGES

Date	Description	Change Made By: