Green Thumb Business Impact Analysis

1. Overview

This Business Impact Analysis (BIA) is developed as part of the contingency planning process for Green Thumb Nursery.

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 Green Thumb 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.

3. BIA Data Collection

Data collection can be accomplished through individual/group interviews, workshops, email, questionnaires, or any combination of these.

3.1 Determine Process and System Criticality

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

Mission/Business Process	Description
Pay vendor invoice	*Process of obligating funds, issuing check or electronic payment, and acknowledging receipt*
Ordering Supplies (Risk ID: Ordering Supplies)	Process of contacting suppliers and scheduling product delivery
Processing Customer Transaction (Risk ID: Technology)	Process of entering customer transactions into the Point of Sales (POS) system
Creating Security Reports (Risk ID: Physical Security)	Process of creating the security reports of the previous business day
Tracking Grow Technique Data (Risk ID: Technology)	Process of logging techniques for proper growth cycles
Creating Safety Reports (Risk ID: Safety)	Process of creating the safety reports of the previous day
Logging/Tracking Product (Risk ID: Asset Management)	Process of keeping track of product

If criticality of mission/business processes has not been determined outside of the BIA, the following subsections will help to determine criticality of mission/business processes that depend on or support the information system.

3.1.1 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 in order 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 in order to characterize levels of severity to the organization that would result for that particular 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: Severe, Moderate, Minimal

Impact values for assessing category impact:

- Severe = 3
- Moderate = 2
- Minimal = 1

Example impact category = Cost

Severe *– temp staffing, overtime, fees are greater than $1 million*
Moderate *– fines, penalties, liabilities potential $550K*
Minimal *– new contracts, supplies $75K*

The table below summarizes the impact on each business process if the business process were unavailable, based on the following criteria:

Mission/Business Process	Impact Category			
	1	2	3	Impact
Example: Pay vendor invoice		*X*		*Moderate*
Ordering Supplies		X		Moderate
Processing Customer Transactions			X	Severe
Creating Security Reports	X			Minimal
Tracking Grow Technique Data		X		Moderate
Creating Safety Reports	X			Minimal
Logging/Tracking Product			X	Severe

Estimated Downtime

Working directly with mission/business process owners, departmental staff, managers, and other stakeholders, estimate the downtime factors for consideration as a result of 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 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. 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	MTD	RTO	RPO
Example: Pay vendor invoice	*72 hours*	*48 hours*	*12 hours (last backup)*
Ordering Supplies	72 hours		
Processing Customer Transactions		6 hours	
Creating Security Reports			24 hours
Tracking Grow Technique Data	24 hours		

Creating Safety Reports			24 hours
Logging/Tracking Product		12 hours	

3.2 Identify Resource Requirements

The following table identifies the resources that compose Green Thumb, including hardware, software, and other resources such as data files.

System Resource/Component	**Platform/OS/Version (as applicable)**	Description
Example: Web Server 1	*Optiplex GX280*	*Web Site Host*
Workstation	Microsoft Windows 10	Device that accesses the internet
Internet Router	ISP Provided	Device used to access the internet
Network Switch	Netgear	Device that provides network connection to all network resources
Wireless Access Point	Netgear	Device that provides wireless access to the network infrastructure
Cell Phones	Galaxy s7 Straight Talk Wireless	Devices used for business communications
Advertising Computer	Microsoft Windows 10	Device used for internal advertising in the store
Environmental Sensors	APC	Devices used for environmental monitoring. For example, temperature sensors, humidity sensors, and power sensors.

Tracking/Backup Server	Microsoft Windows Server 2016	Device used for tracking and logging product data and maintaining data backup
Security Cameras	Arlo 5 Fixed, 1 PTZ	Devices used for property monitoring. For example, fixed site cameras and pan, tilt, zoom cameras.

It is assumed that all identified resources support the mission/business processes identified in Section 3.1 unless otherwise stated.

3.3 Identify Recovery Priorities for System Resources

The table below lists the order of recovery for Green Thumb 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.

Priority	System Resource/Component	Recovery Time Objective
Example: Web Server 1	*Optiplex GX280*	*24 hours to rebuild or replace*
Processing Customer Transactions	Microsoft Windows 10 PC	24 hours
Logging/Tracking Product	Microsoft Windows Server 2016	12 hours