CHRISTOPHER NEWPORT
UNIVERSITY

Business Impact Analysis Standard

VERSION 1.1

June 2023
Department: Information Security

Proprietary Statement

This document was developed specifically for and by Christopher Newport University. The concepts and methodologies contained herein are proprietary to Christopher Newport University. Duplication, reproduction, or disclosure of information in this document without the express written consent of Christopher Newport University is prohibited.

All Trademarks, Registered Trademarks, Service Marks, and brand and product names used in this document are the property of their respective owners.

Review and Revision History

Date	Version	Description of Change (Affected Sections)	Author
2/16/2023	1.0	Initial Release	Wendy L. Wilde
June 2023	1.1	Annual Review	Wendy L. Wilde

TABLE OF CONTENTS

Introduction

A Business Impact Analysis (BIA) is developed as part of the systems risk assessment process and is a point-in-time analysis of system components that determines the criticality and potential impact to Christopher Newport's mission-critical processes and data should the system component become unavailable. The analysis allows university leadership to establish priority levels for sequencing recovery activities and resources.

Purpose

The purpose of the Business Impact Analysis (BIA) is to identify and prioritize system components by correlating them to mission critical processes that support ongoing university operations. If any of these systems were to be unavailable, the BIA could be used to identify the impact to the university.

Scope

The scope of the Business Impact Analysis (BIA) applies to any university-owned or operated IT resource or service that stores, processes, or transmits data. Additionally, this includes any IT resources or services identified by the Information Security Officer as important to security operations.

Roles and Responsibilities

These roles and responsibilities are assigned to individuals, and may differ from the actual role title or working title of the individual's position. Individuals may be assigned multiple roles, as long as the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud and do not lead to a conflict of interest. Refer to the Role Based Security Training Information Security Standard for roles and responsibilities.

a. **System Owner** - Responsible for completion of the BIA. System owners may require additional support or input from the Data Owner. Additionally system owners may delegate this responsibility to another department member.

b. **Data Owners** - Participate in the development of the BIA to establish recovery time objectives (RTO) and recovery point objectives (RPO). Additionally, the data owner makes decisions about the data classification, accessibility and retention requirements.

c. **Chief of Staff, Provost, Vice Presidents, Deans, Directors, Department Heads and Supervisors** - University executives and senior management in academic and business units of the university are responsible for, and must participate in, the development of their respective departments' BIA to ensure that overall priorities for the recovery of systems and data are established and reviewed annually.

d. **Information Security Office** - Responsible for overseeing and executing this standard annually.

Definitions

a. **Business Impact Analysis (BIA)** - A Business Impact Analysis (BIA) is developed as part of the systems risk assessment process and is a point-in-time analysis of system components that determines the criticality and potential impact to mission-critical processes and data as well as the impact should the system component become unavailable.

b. **Class 1 (Restricted) Data** - May be subject to disclosure laws and warrant careful management and protection to ensure its integrity, appropriate access, and availability. Restricted data includes Social Security Number (SSN), Drivers License number, Federal ID, medical records or other individually identifiable health information, collectively known as protected health information, Payment Card Holder Data, and Protected Health Information (PHI), when combined with identifying information.

c. **Continuity of Operations Plan (COOP)** - A process of identifying the essential functions, including staff, systems, and procedures, that ensures the continuation of the university's ability to operate.

d. **Data Owners -** Stewards of a system or its information assets during its development and/or operation.

e. **Information Technology Resources** - Defined as computers, software, telecommunication equipment, networks, automated data processing, databases, the Internet, printing, management information systems, and related information, equipment, goods, and services.

f. **Recovery Point Objectives (RPO)** - The maximum amount of data as measured by time that can be lost after a recovery from a disaster, failure, or comparable event before data loss will exceed what is acceptable to the university.

g. **Recovery Time Objectives (RTO)** - The overall length of time an information system's components can be in the recovery phase before negatively impacting the university's mission and business processes.

h. **Risk Assessment** - a managerial process used to determine the probability and impact of threats caused by the human and technological environment on university assets.

i. **System Owners** - Individuals who are responsible for formulating policy and guidance that may impact information system and/or security policy and operations. System Owners allocate resources to manage risk.

Standards Statement

The Business Impact Analysis (BIA) is an integral part of the Business Continuity Planning and Disaster Recovery planning. The BIA defines certain critical information needed to complete and complement the University Continuity of Operations Plan (COOP).

System Owners, Data Owners and University leadership are required to participate in the assessment and development of the Business Impact Analysis (BIA).

Business Impact Analysis (BIA) Procedures

New Systems

A Business Impact Analysis (BIA) is initiated as part of the university's Technology Vetting Program to ensure that the BIA data is captured at the time of a new system implementation.

Existing Systems

A Business Impact Analysis (BIA) should be completed for university-owned IT resources or service that stores, processes, or transmits data.

The steps listed below summarize how a BIA is completed:

1. A Business Impact Analysis (BIA) Intake Form is distributed to the system owner via email with a pre-determined deadline to complete and return to iso@cnu.edu. The form is located here.
2. Once the responses are received, the Information Security Officer will review the responses. Follow-ups with the form respondent will be completed as needed to ensure the data is accurate, complete and objective.
3. Mission critical systems are identified the System and Data Owners, and next steps are taken to ensure that the system recovery/Continuity of Operations (COOP) is documented accordingly.
4. The Business Impact Analysis (BIA) will be reviewed annually. A new Business Impact Analysis (BIA) will be conducted every three years or following a significant change.

Business Impact Analysis (BIA) Outputs

The data obtained from the BIA questionnaire will be used to:

1. Ensure the correct data classification has been applied to the system according to the University Data Classification Standard
2. Determine the priority for restoring functions of the University
3. Data such as RTO and RPO are used as input for the department Continuity of Operations (COOP)
4. Identify mission critical resources required to support Department recovery
5. Identify mission critical technology infrastructure requirements

Reporting

Results of the Business Impact Analysis (BIA) will be reported to the University leadership.

References

Information Security Policy - 6045

University Emergency Response Oversight Policy - 1035

Information Technology Disaster Recovery Plan

Information Technology Role Based Security Training Standard

University Technology Vetting

Business Impact Analysis Intake Form