Business Continuity Plan

Phase 1

Ryan Coon

CYB-515

Dr. Edward Marchewka

November 6, 2024

Table of Contents

Executive Overview 3

Document Change Control 4

Introduction 6

Plan Objectives 7

Risk Assessment Matrix 8

Critical Business Functions Overview 9

Company Organizational Structure Chart 10

References 11

Executive Overview

This Business Continuity Plan (BCP) outlines the company's strategy for maintaining critical business operations in the face of disruptions. A business continuity plan (BCP) is a defined set of proactive and reactive measures that key personnel will implement in response to a potential danger to your organization (Sukianto, 2024). It is designed to minimize the impact of potential events, including natural disasters, cyberattacks, pandemics, and other unforeseen circumstances, by providing a structured approach to recovery and ensuring business resilience.

The BCP is a living document, regularly reviewed and updated to reflect changes in the company's business environment, evolving threats, and technological advancements. It is a collaborative effort, involving key stakeholders across all departments, to ensure a comprehensive and effective plan.

This plan focuses on the following key objectives:

* Identifying Critical Business Functions: The plan identifies and prioritizes the company's most critical business functions, ensuring their continued operation is paramount for survival and success.
* Assessing and Mitigating Risks: A thorough risk assessment process identifies potential threats and vulnerabilities, enabling the development of appropriate mitigation strategies.
* Developing Recovery Strategies: The plan outlines specific recovery strategies for each critical business function, including alternative work arrangements, data backup and recovery procedures, and communication protocols.
* Establishing Clear Roles and Responsibilities: The BCP defines roles and responsibilities for all personnel involved in the plan's implementation, ensuring clear lines of authority and accountability.
* Testing and Exercising the Plan: Regular testing and exercises ensure the plan's effectiveness and allow for continuous improvement, ensuring it remains relevant and adaptable to changing circumstances.

This BCP serves as a roadmap for the company to navigate disruptions effectively, minimizing business impact and facilitating a swift and efficient recovery. By implementing this plan, the company demonstrates its commitment to business continuity, ensuring the long-term viability and success of the organization.

Document Change Control

A Document Change Control for a Business Continuity Plan (BCP) is like a meticulous logbook for your plan. It tracks every modification made, ensuring transparency and accountability. Imagine a table with columns for: the date of the change, the new version number, a clear description of what was changed, who made the change, who reviewed it, and who approved it. Every time the BCP is updated, a new row is added. This could be due to new risks identified, updated procedures, organizational changes, or regulatory updates.

This logbook is crucial for several reasons:

* It shows a clear history of all modifications, making it easy to see who made what changes and when.
* It ensures that all changes are documented and reviewed, preventing accidental or unauthorized modifications.
* It helps maintain the integrity of the BCP by ensuring that all versions are aligned and accurate.
* It provides a valuable resource for auditors who need to verify the BCP's completeness and compliance.

Document Change Control ensures your BCP remains relevant, accurate, and effective in the face of ever-changing circumstances. “The Document Change Control Process is intended to manage and regulate alterations, updates, or modifications made to critical documents within an organization. Its primary purpose is to ensure the accuracy, integrity, traceability, and compliance of documents throughout their lifecycle”(Document Change Control, n.d.).

Business Name: RC Cybersecurity Department: IT

Change Log Index

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Version | Requester | Specialist | Change/Review |
| 11/6/2024 | 1.0 | J.D. Coon | Ryan Coon | Initial BDC |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CHANGE STATEMENT | | Provide a brief description of the requested change | CHANGE No. |  |
|  | | | REPORT ID |  |
| DATE |  |
| LOCATION |  | | TIME |  |

|  |  |  |
| --- | --- | --- |
| REQUESTED BY | TITLE | CONTACT INFORMATION |
|  |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| REQUEST PRIORITY | LOW | MEDIUM | HIGH | CHANGE  TYPE | MINOR | MAJOR | STANDARD | EMERGENCY |
|  |  |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| DESCRIPTION OF CHANGE | | Provide a detailed description of the problem and circumstances leading to the requested change | | | |
|  | | | | | |
|
| SUPPORTING INFORMATION | | | Provide screenshots of an error or attach the error in a document / report | | |
|  | | | | | |
|
| REASONS AND JUSTIFICATION | | | | Describe the reason why the change has been requested and the justification for the request | |
|  | | | | | |
| AFFECTED AREAS  According to the perception of the requester | System | | | |  |
| Subsystem | | | |  |
| Documentation | | | |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| DECISION | |  | Project Manager Name | Signature | Date |
|  | ACCEPTED |  |  |  |  |
|  | REJECTED |  | Approver Name & Title | Signature | Date |
|  | More Info Requested |  |  |  |  |

Introduction

**Overview:**

The BCP is a critical component of the company's overall risk management strategy. It is designed to address the potential impact of a wide range of disruptions, including natural disasters, cyberattacks, and pandemics. The BCP is based on a comprehensive risk assessment that identifies the company's critical business functions and the potential threats to those functions.

**Plan Scope:**

The BCP covers all critical business functions, including operations, finance, IT, and human resources. The plan outlines the steps necessary to restore these functions to an acceptable level of operation within a specified timeframe.

**Applicability:**

The BCP is applicable to all employees of the company. All employees are expected to be familiar with the plan and their roles in its implementation.

**Cybersecurity Frameworks:**

The BCP aligns with industry-standard cybersecurity frameworks, such as NIST Cybersecurity Framework and ISO 27001, to ensure the company's cybersecurity program is robust and effective.

**Cyber Threat Models:**

The BCP analyzes various cyber threat models to identify and protect against cybercrime threat vectors, motivations, and ideologies. This includes understanding the tactics, techniques, and procedures (TTPs) used by attackers, as well as the motivations behind their attacks.

Plan Objectives

The objectives of this BCP are to minimize disruption, protect critical assets, and ensure business continuity in the face of unforeseen events. Specifically, this plan aims to:

* Preserve Life Safety - Prioritize the safety of employees and stakeholders during an emergency.
* Maintain Critical Operations - Ensure essential business functions continue uninterrupted or are restored quickly.
* Protect Reputation and Customer Relationships - Minimize damage to the organization's image and maintain customer trust.
* Reduce Financial Losses - Limit the financial impact of disruptions by minimizing downtime and recovering lost data.
* Facilitate a Smooth Recovery - Provide a structured framework for restoring operations and returning to normal business activities.

Plan Assumptions

* Resource Availability - The plan assumes access to essential resources like personnel, technology, and financial support during an emergency. This includes having backup systems, communication channels, and emergency funds readily available.
* Communication Channels - It assumes reliable communication channels will be available for disseminating information and coordinating recovery efforts. This could involve secure communication platforms, designated contact points, and pre-established communication protocols.
* Regulatory Compliance - The plan assumes compliance with relevant laws and regulations regarding disaster preparedness and business continuity. This ensures the organization adheres to legal requirements and industry standards.
* Third-Party Support - It assumes the availability of external support, such as vendors, service providers, and government agencies, when needed. This includes having established relationships with key partners and understanding their capabilities and response times.

Risk Assessment Matrix

Legend:

Vertical direction on the chart is the likelihood of an occurrence

Likely: One occurrence every week

Possible: Once a month or quarterly

Unlikely: Once every six months or longer

Horizontal Direction on the chart is the severity of the risk

Low: possible threat to a small target or group(ProjectManager, 2024).

Medium: Potential threat to a larger group that results in more harm and consequences.

High: Possible threat to a large target or group, this can lead to unintended consequences

A screen shot of a chart

Description automatically generated

Critical Business Functions Overview

This Business Continuity Plan (BCP) focuses on protecting critical business functions essential for continued operations during and after a disruption. These functions are identified as:

* Customer Service: Maintaining communication channels and providing uninterrupted support to customers.
* Financial Operations: Ensuring the continued processing of payments, financial reporting, and cash flow management.
* IT Infrastructure: Maintaining access to critical systems, data, and applications, including network connectivity and data security.
* Production/Operations: Ensuring the continued production of goods or services, including supply chain management and inventory control.
* Human Resources: Maintaining employee safety, communication, and payroll processing during and after a disruption.

This BCP aims to minimize the impact of disruptions, protect these critical functions, and enable a swift and effective recovery, ensuring business continuity and minimizing operational downtime.

“A vital business function encompasses the processes and activities inside a firm that have the most significant influence on its operations and are indispensable for its ongoing operations and ability to recover in the case of a disruption. The functionality of these operations is essential for the organization to carry out its business, and any interruption may result in significant safety, legal, operational, and financial ramifications” (Snedaker & Rima, 2014).

Company Organizational Structure Chart

A black and white diagram with words

Description automatically generated with medium confidence

References:

*Document Change Control*. (n.d.). ComplianceQuest QHSE Solutions. https://www.compliancequest.com/document-change-control/

Snedaker, S., & Rima, C. (2014). Business Impact Analysis. *Business Continuity and Disaster Recovery Planning for IT Professionals*, 225–274. https://doi.org/10.1016/b978-0-12-410526-3.00005-2

Sukianto, A. (2024, September 16). *How to Create a Business Continuity Plan | UpGuard*. Www.upguard.com. https://www.upguard.com/blog/business-continuity-plan