Owner: Will Davies
Last Updated: 31/05/24
Last Updated By: Will Davies

Business Continuity Plan

1. Introduction

Purpose

The purpose of this document is to provide a structured approach for ensuring the continuity of critical business operations during and after a disaster or major disruption.

Scope

This plan applies to all critical business functions, processes, and operations within the organisation. It covers various types of disruptions, including natural disasters, technological failures, cyber-attacks, and other emergencies.

Objectives

- Ensure the safety of employees and stakeholders.
- Maintain critical business functions during and after a disruption.
- Minimise financial and operational impacts.
- Facilitate a coordinated and effective response to disruptions.

2. Business Continuity Management Team (BCMT)

Roles and Responsibilities

- **Business Continuity Manager**: Oversees the implementation and maintenance of the BCP, coordinates response efforts, and ensures communication with stakeholders. Manages internal and external communications.
- **IT Recovery Lead**: Manages the technical recovery of IT systems and infrastructure.

Contact Information

Role	Name	Contact Number	Email
Business Continuity Manager	Hugo Lu	+44 7477 613636	hugo@getorchestra.io
IT Recovery Lead	Will Davies	+44 7979 902431	will@getorchestra.io

3. Business Impact Analysis (BIA)

Objectives of BIA

- Identify critical business functions and processes.
- Assess the impact of disruptions on these functions.
- Determine Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). Defined as UK business hours.

Process

1. **Identify Critical Functions**: List all business functions and identify which are critical to operations.
2. **Impact Assessment**: Evaluate the potential impact of disruptions on these functions, including financial, operational, and reputational impacts.
3. **RTO and RPO Determination**: Establish acceptable recovery times and data loss thresholds for each critical function.

BIA Results

Function	Critical	RTO	RPO	Notes
IT	Yes	24 hours	24 hours	Includes all core IT services
Operations	Yes	24 hours	24 hours	Includes underlying application
Finance	Yes	12 hours	12 hours	

4. Risk Assessment and Mitigation

Risk Identification

- Natural Disasters: Earthquakes, floods, storms
- Technological Failures: Hardware failures, software bugs, network outages
- Cyber Threats: Malware, ransomware, data breaches
- Human Factors: Insider threats, human errors, pandemics

View the risk assessment documentation for more information

5. Business Continuity Strategies

Prevention Strategies

- Regularly conduct risk assessments and update mitigation plans. See risk assessment documentation for more information.
- Ensure regular backups and secure storage of critical data.
- Maintain up-to-date contact lists and communication protocols.

Response Strategy

- Activate the BCP and notify all relevant stakeholders.
- Ensure appropriate communication between relevant internal and external stakeholders

Recovery Strategies

- Prioritise the recovery of critical functions based on the BIA.
- Utilise backup systems and data to restore operations.
- Communicate recovery status and timelines to all stakeholders.

Resumption Strategies

- Gradually restore non-critical functions as resources become available.
- Conduct thorough testing to ensure systems and processes are fully operational.
- Perform a post-mortem to identify lessons learned and areas for improvement.

6. Plan Activation

Activation Criteria

The BCP is activated in response to events that significantly disrupt normal operations and require coordinated recovery efforts. Examples include:

- Natural disasters causing damage to facilities or infrastructure.
- Cyber-attacks impacting critical systems and data.
- Extended power outages or network failures.

Activation Procedure

1. **Incident Detection**: Identify the disruption and assess its impact on critical functions.
2. **Initial Notification**: Notify the Business Continuity Manager and other key personnel.
3. **Assessment and Decision**: The Business Continuity Manager, in consultation with senior management, decides whether to activate the BCP.
4. **Activation**: Officially activate the BCP and notify all relevant stakeholders.

7. Communication Plan

Internal Communication

- Notify internal stakeholders via Slack.

External Communication

- Communicate with customers, partners, and suppliers as necessary via Email.

Communication Channels

- Email
- Phone calls

8. Training

Training Programs

- Regular training sessions for BCMT members on BCP procedures and tools.
- Annual business continuity awareness training for all employees

9. Plan Maintenance and Review

Regular Reviews

- Review and update the BCP at least annually or after significant changes to the business environment or operations.
- Conduct a post-incident review after each activation of the BCP to identify lessons learned and areas for improvement.

Document Control

- Maintain version control of the BCP document.
- Ensure that all copies of the BCP are up to date and accessible to relevant personnel.

Continuous Improvement

- Implement improvements identified during reviews and exercises.
- Stay informed about best practices and industry standards in business continuity management.