Business Continuity and Disaster Recovery Plan (BC & DR)



|  |  |
| --- | --- |
| Version | 1.0 |
| Last major review |  |
| Updated |  |
| Reason |  |
| Compiled by |  |
| Approved by |  |

[This template contains instruction text and examples that you can delete when adapting this business continuity plan for your business.]

# Contents

[Contents 2](#_Toc193266816)

[1. Plan overview 4](#_Toc193266817)

[1.1 Introduction 4](#_Toc193266818)

[1.2 Objectives 4](#_Toc193266819)

[1.3 Business Continuity & Disaster Recovery Plan Location 4](#_Toc193266820)

[1.4 Glossary 5](#_Toc193266821)

[2. Critical Business Functions & Assets 6](#_Toc193266822)

[2.1 Introduction 6](#_Toc193266823)

[2.2 Objective 6](#_Toc193266824)

[2.3 Document Locations 7](#_Toc193266825)

[2.4 Critical Business Functions & Assets 8](#_Toc193266826)

[3. Risk and Threat Management 10](#_Toc193266827)

[3.1 Introduction 10](#_Toc193266828)

[3.2 Instructions 10](#_Toc193266829)

[3.3 Objective 10](#_Toc193266830)

[3.4 Risk Register Location 10](#_Toc193266831)

[3.5 Likelihood 11](#_Toc193266832)

[3.6 Impact 11](#_Toc193266833)

[3.7 Level of risk 12](#_Toc193266834)

[3.8 Mitigation Strategies 12](#_Toc193266835)

[3.9 Risk Register 13](#_Toc193266836)

[4. Event Response 14](#_Toc193266837)

[4.1 Introduction 14](#_Toc193266838)

[4.2 Instructions 14](#_Toc193266839)

[4.3 Objectives 14](#_Toc193266840)

[4.4 Event Response Team Meeting Minutes Location 14](#_Toc193266841)

[4.5 Roles and Responsibilities 15](#_Toc193266842)

[4.6 Event Response Team Activation 15](#_Toc193266843)

[4.7 Event Response Checklist 16](#_Toc193266844)

[5. Plan Maintenance 17](#_Toc193266845)

[5.1 Introduction 17](#_Toc193266846)

[5.2 Objective 17](#_Toc193266847)

[5.3 Plan Review 17](#_Toc193266848)

[5.4 Plan Testing/Simulation 18](#_Toc193266849)

[5.5 Backup Testing 18](#_Toc193266850)

[5.6 Plan Improvements 18](#_Toc193266851)

#

# Plan overview

## Introduction

The following document template is aimed at small businesses who do not have the resources to exhaustively prepare detailed plans covering every eventuality and want a policy that allows a more agile approach to assessment and response to events and continued business operations.

The purpose of this business continuity and disaster recovery plan is to ensure the continuation of your Business during and following any critical incident that results in disruption to normal operation.

## Objectives

The objectives of this plan are to:

* Define and prioritise your **Critical Business Functions & Assets:**
	+ What your business does and how your business does it
	+ Identifies and prioritises key activities of a business adversely affected by disruptions
* Undertake an assessment of **Risks and Threats:**
	+ What could impact your businessand how
	+ Identifies and manages the likelihood and/or effects of risk associated with an incident.
* Form a team and provide a framework for **Event Response**:
	+ Define who is part of the Business Continuity and Disaster Recovery team
	+ Define the process to assess an event
	+ Outline actions to respond to an event
* Detail ongoing BC & DR Plan **Maintenance**
	+ Ensure the BC & DR Planis up to date and communicated to relevant parties
	+ Processes to regularly review, improve and test this plan.

## Business Continuity & Disaster Recovery Plan Location

It is important to maintain version control of this document. There should be a single digital location of the plan, as well as a single physical location for a printed version that can be accessed in the event that the digital version is inaccessible.

The Business Continuity & Disaster Recovery Plan is kept in this location:

 **[Digital location and physical location of document]**

**Important:** If you are reading a copy of this Business Continuity and Disaster Recovery Plan and it is not from the Master location it may not be up to date.

## Glossary

[This table provides a consistent and commonly agreed set of definitions for terms used in the plan. Customise this list to suit your business.]

|  |  |
| --- | --- |
| Business continuity and disaster recovery plan | A document containing all of the information required to ensure that your business is able to resume critical business activities should a crisis/disaster occur. |
| Business continuity planning | A process that helps develop a plan document to manage the risks to a business, ensuring that it can operate to the extent required in the event of a crisis/disaster.  |
| Critical Business Functions | Identifies and prioritises key activities of a business adversely affected by disruptions |
| Recovery Time Objective (RTO) | How long the business can survive while that critical software or system is bought back online. It’s the time it takes to rebuild a system and/or restore its data. This determines the speed of your backup infrastructure and whether you have hot standby systems. Most small businesses can usually last a day or two while systems are brought online and data is restored (i.e. email can be useful if back in a few hours and the historical data restored over a couple days) |
| Restore Point Objective (RPO) | The regularity of backups and therefore how much information you can lose or have to re-enter or recreate (such as daily backups mean you could lose up to a day’s data and be able to recreate, re-enter or continue without it) |
| Risk management | The process of defining and analysing risks, and then deciding on the appropriate course of action in order to minimise these risks, whilst still achieving business goals. |
|  |  |
|  |  |

##

# Critical Business Functions & Assets

## Introduction

This section of the plan will ensure that there is a very good understanding of what the business does and the assets, systems, key staff and external contacts along with the data you use to run the business.

## Objective

The objective of this section is to provide a place to record detailed records of your Critical Business Functions & Assets. This should include any systems, hardware, services and other items needed for your business to function day to day. Feel free to add any categories as needed.

Document all Critical Business Functions & Assets (both physical and digital) by completing the provided tables to document, this needs to cover:

* All physical locations of the business
* Key people involved in the business both internally and externally
* All of the Physical and Digital (both hardware and software) assets and systems your business uses in order to operate

This section is also the ideal place to record any emergency and first aid kits as well as any other information pertinent to know in an event that may impact the business operations.

Critical Business Functions & Assets should be tailored to your individual circumstances and can include other categories not included in the examples below.

**Suppliers**

**Your suppliers could include:**

* Energy retailer
* Security company
* Electricians you have used before
* Plumbers you have used before
* ISP for your internet connections or telephones (mobile and fixed line)
* IT Support company
* Web host
* Insurance Broker
* Compliance such as Queensland Law Society or the Office of the Australian Information Commissioner

**Systems**

Think about your systems, both the hardware and software aspects of your business, this will vary depending on your business circumstances, but can include:

**Hardware:**

* Internet connection
* Router
* Firewall
* Network Switches
* Wi-Fi
* Servers
* PCs
* CCTV
* Printers
* Phone system and phones

**Software**

* Office 365
* Some of the Line of Business applications our clients use are as follows:
	+ ActionStep
	+ Triconvey/Smokeball
	+ SILQ
	+ LEAP
	+ AutoCAD
	+ Medical Director
	+ Clinko
	+ Practice Fusion
	+ Practice Protect
	+ ProfiitPlus
	+ TradeSoft
	+ HowNow
	+ FYIDocs
* Accounting software such as MYOB or XERO
* Website
* Marketing software/newsletters
* Social Media accounts
* Critical spreadsheets
* Password management tool
* CRM
* Phone system and phones

Along with documenting each of the critical infrastructure systems used in the business it is important to identify RTO and RPO for each listed piece of software or system used.

RPO is Restore Point Objective, i.e. the regularity of backups and therefore how much information you can lose or have to renter or recreate (such as daily backups mean you could lose up to a day’s data and be able to recreate, re-enter or continue without it)

RTO stands for Recovery Time Objective and is how long you can survive while that critical software or system is bought back online. It’s the time it takes to rebuild a system and/or restore its data. This determines the speed of your backup infrastructure and whether you have hot standby systems. Most small businesses can usually last a day or two while systems are brought online, and data is restored (i.e. email can be useful if back in a few hours and the historical data restored over a couple days)

## Document Locations

There is no single external document or register for the following information, all details should be kept within the BC&DR Plan.

## Critical Business Functions & Assets

**Key Locations**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Address** | **Main Number** | **Key Contact** | **Info** | **Emergency kit location** | **First Aid kit location** |
| *Store* | *1 Amber Street, Clear City* | *07 3328 9955* | *Simon Monk* | *Retail Store* |  |  |
| *CEO’s House* | *1 Saffron Street, Elm City* | *07 3328 7839* | *Chris Silver* | *Home* |  |  |
|  |  |  |  |  |  |  |

**Board Members**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Position** | **Email** | **Phone** | **Address** |
| *Ken Jones* | *Chair* | *ken@jones.com.au* | *0412 312 322* | *1 Scarlett Street, Clear City* |
|  |  |  |  |  |

**Key Employees**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Position** | **Email** | **Phone** | **Address** |
| *Alice Brown* | *CFO* | *alice@abcd.com.au* | *0455 633 685* | *1 Green Street, Clear City* |
|  |  |  |  |  |

**Key Clients**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Organisation** | **Email** | **Phone** | **Address** |
| *Frank White* | *United Workers* | *frank@white.co* | *0455 264 886* | *1 Pink Street, Clear City* |
|  |  |  |  |  |

**Suppliers**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Service** | **Company Name** | **Email** | **Phone** | **Account number** |
| *Electricity* | *Spark* | *o*utages@spark.com | *1300 885 663* | *56833994* |
|  |  |  |  |  |

**Data (Hard Copy and Digital)**

**Hardware**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Item** | **Qty** | **Physical Location** | **Important Settings** | **Login Credentials** | **RPO** | **RTO** | **Notes** |
| *Dell PowerEdge R720 Server* | *1* | *Rack in server cupboard, level 1 behind reception* | *[Link to digital or record physical location]* | *In Password Management Tool* | *1 day* | *2 days* | *Host for SQL server and CRM virtual machines* |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **System/App** | **Supplier** | **Users** | **Data locations** | **RPO** | **RTO** | **Login credentials** |
| *Accounting* | *MYOB* | *CFO, Accounts Clerk* | *Cloud* | *4 hours* | *1 day* | *Password Management Tool* |
| *Microsoft 365 Email*  | *Microsoft* | *All staff* | *Cloud* | *4 hours* | *1 day* | *Password Management Tool* |
| *Design Drawing Database* | *Microsoft* | *Engineering staff* | *Dell PowerEdge Server – SQL Virtual Machine* | *4 hours* | *1 day* | *Password Management Tool* |
|  |  |  |  |  |  |  |

**Software and Cloud SaaS**

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Type** | **Custodian** | **Data locations** | **Logins or Keys** |
| *Historical hard copy accounting info* | *CFO, Finance Assistant* | *Shelves in CFO’s office* | *CFO Office Key* |
| *External hard drive of product photos* | *Marketing Manager* | *Marketing Manager, top drawer of desk* | *Drawer not locked* |
|  |  |  |  |

# Risk and Threat Management

## Introduction

This section is to identify risks and threats to the business then assess their associated likelihood and consequences of the risk or threat occurring, the actions being taken to reduce those risks or threats and who is responsible for managing their mitigation strategy.

## Instructions

In this section of the Business Continuity and Disaster recovery plan you will need to develop a Risk Register. We recommend a brainstorming session with key people in your team to sit down and identifying each risk, assessing the likelihood, the impact and assigning it a score and finally to consider your mitigation strategies.

Your risk register should be a non-comprehensive list of identified risks that could happen to your business such as:

* **Natural Disasters**: Bushfires, floods, storms
* **Cybersecurity Threats**: Data breaches, ransomware, hacking
* **Infrastructure Failures**: Power outages, internet disruptions
* **Pandemics & Health Risks**: COVID-19, flu outbreaks

## Objective

The objective of this section is to provide the tools and information to clearly assess and document risks and threats to the business as well as strategies put in place to mitigate those risks and threats.

## Risk Register Location

It is important to log all risks and threats identified in this document. There should be a single digital location of this document, as well as a single physical location for a printed version that can be accessed in the event that the digital version is inaccessible.

The risk register is kept in this location:

 **[Digital location and physical location of risk register]**

## Likelihood

What is the likelihood of this risk or threat occurring to the business? Assign it a score based on how likely or often you think it will occur.

| Level | Likelihood | Description |
| --- | --- | --- |
| 3 | High | Happens more often than every year |
| 2 | Medium  | Happens every 1-2 years |
| 1 | Low | Happens less frequently than every 2 years |

## Impact

What is the level of impact it would have on the business? This could be anything from affecting a single employee for a 2-hour period to stopping daily operations for the entire business.

| Level | Impact | Description |
| --- | --- | --- |
| 3 | High | Significant impact to the business, stopping daily operations |
| 2 | Medium | Impacts the business for less than a day |
| 1 | Low | Impacts a single employee |

## Level of risk

Once you have the Likelihood and Impact scores for each risk you can then calculate the Risk score, the risk score is the sum on Likelihood x Impact. Using this scale can result in 6 possible scores: 1,2,3,4,6 and 9.

| Rating | Description | Action |
| --- | --- | --- |
| 6-9 | Severe | Mitigate immediately and aggressively |
| 3-4 | High | Mitigate with a high priority  |
| 2 | Moderate | Mitigate with low-cost strategies  |
| 1 | Low | Assess as required |

## Mitigation Strategies

Mitigation strategies are there to reduce or remove the risk or threat, these fall into one of four approaches.

|  |  |
| --- | --- |
| Mitigation Strategy | Example |
| **Avoidance**Find a different way to do things to eliminate the risk. | *Instead of storing customer data on your own servers, use a secure cloud service to remove the risk.* |
| **Acceptance**Acknowledge the risk and make a backup plan in case it happens. | *If your internet goes down occasionally, instead of spending a fortune on a second connection, you accept the risk and have a mobile hotspot as a backup.* |
| **Transfer** Shift the risk to someone else, like an insurance company or a third party. | *Buying business insurance to cover damage from a fire instead of paying for repairs yourself.* |
| **Reduction**Take steps to lower the chance of the risk happening or lessen the damage if it does. | *Installing security cameras and alarm systems to reduce the chances of a break-in.* |

## Risk Register

Complete your risk assessment and document each in your Risk Register, we have included some examples below and a template layout for your Risk Register.

| Risk description | Likelihood | Impact | Level of Risk | Mitigation Strategy |
| --- | --- | --- | --- | --- |
| *Internet outage* | *1* | *2* | *2* | * *Look at backup internet solution such as a 5G dongle*
 |
| *2025 Cyclone Alfred* | *1* | *3* | *3* | * *Enable staff to work from home during this period*
* *VoIP Phone system to allow you to receive calls out of the office*
* *Cloud services such as Office 365 for email and file storage*
 |
| *Office 365 Outage* | *2* | *2* | *4* | * *Duplication of contact details outside of Office 365*
* *Backup of SharePoint libraries and Email*
* *Email queueing to ensure delivery once service is back up*
 |
| *Data Breach* | *2* | *2* | *4* | * *Firewalls*
* *Endpoint Protection Software*
* *Security Awareness Training*
 |
| *Regular robberies**(this is something that happened to a Pharmacy we supported)* | *3* | *3* | *9* | * *CCTV (we installed the system)*
* *Roller shutters*
* *Bollards on the footpath*
 |
|  |  |  |  |  |

# Event Response

## Introduction

This section of the BC&DR Plan is to provide the resources to select members of the Event Response Team and provide a structured approach to assess a potential event and respond effectively to ensure the business remains operational during an event and minimises any impact to the business including reputational damage.

## Instructions

Key members of the business should sit down to discuss and decide on who should form part of the Event Response Team, what are their roles and responsibilities and what steps to do to activate the team and respond to an event.

## Objectives

The objectives of this section are to

* Form the Event Response Team and assign roles
* Create a log of meeting minutes and actions
* Provide tools to assess an event
* Create process to respond to an event

## Event Response Team Meeting Minutes Location

It is important to keep notes of all meetings, decisions and actions and file them in a central repository for future reference. There should be a single digital location of this document, as well as a single physical location for a printed version that can be accessed in the event that the digital version is inaccessible.

The Event Response Team Meeting Minutes are kept in this location:

 **[Digital location and physical location of**

 **Event Response Team Meeting Minutes]**

Even an email to the Event Response Team (single member or whole team) to discuss whether something is an event or not needs to be logged. If a compliance audit is undertaken It’s suspicious when small incidents like that are missing, minor things happen to every business.

## Roles and Responsibilities

The following roles and responsibilities need to be assigned to members of the Event Response Team and recorded below. Note that members can share a number of roles.

|  |  |  |
| --- | --- | --- |
| Role | Team Member | Responsibilities |
| **Team Chair** | *First Last Name* | * Formalise the activation of the team for an event (any member can start this process)
* Chair meetings
 |
| **BC&DR Plan Owner** | *First Last Name* | * Document meetings
* Update and communicate changes to the BC&DR Plan
 |
| **Communications** | *First Last Name* | * Communication externally to suppliers, clients and other third parties to ensure a single point of contact during events
 |
| **Finance**  | *First Last Name* | * Ensure that any actions can be funded, and funding can be accessed during an emergency response - such as buying computer hardware or a 5G dongle Provide budgeting for mitigation strategies for ongoing risk management
 |
| **Human Resources** | *First Last Name* | * Communicate to staff
* Manage staff impacts of event
 |
| **OH&S** | *First Last Name* | * Ensure the safety of all involved during and after an event
* Ensure compliance to OH&S compliance for mitigation strategies for ongoing risk management
 |
| **Operations/IT** | *First Last Name* | * Manage tasks during an event and ensure operations are being maintained
* Provide technical input to event responses and mitigation strategies for ongoing risk management
 |

## Event Response Team Activation

The Event Response Team is activated when any member discovers or is notified about any event that is current or impending. The Event Response Team then assembles either in person, or virtually via phone, email or video conferencing, to assess the event and whether a formal activation and response is warranted. Once formally activated the Event Response Team will work through actions tailored to the event to ensure ongoing business operations.

## Event Response Checklist

For any potential event below are a list of potential actions to be carried out. These actions are tailored to both the business as well as the event and its assessed impact to ongoing business operations.

| **Event response** | **Actions taken** |
| --- | --- |
| [ ]  Assessed the severity of the incident |  |
| [ ]  Logged the event |  |
| [ ]  Assess the event and appropriate actions |  |
| [ ]  Evacuated the site if necessary |  |
| [ ]  Accounted for everyone |  |
| [ ]  Identified any injuries to persons |  |
| [ ]  Contacted emergency services |  |
| [ ]  Activated staff members and resources |  |
| [ ]  Appointed a spokesperson |  |
| [ ]  Gained more information as a priority |  |
| [ ]  Briefed team members on incident |  |
| [ ]  Allocated specific roles and responsibilities |  |
| [ ]  Identified any damage |  |
| [ ]  Photographed or recorded damage |  |
| [ ]  Identified critical activities that have been disrupted |  |
| [ ]  Kept staff informed |  |
| [ ]  Contacted key stakeholders |  |
| [ ]  Contacted insurance company |  |
| [ ]  Understood and complied with any regulatory/compliance requirements |  |
| [ ]  Initiated media/public relations response |  |
| [ ]  Reviewed the response plan and updated as appropriate |  |

# Plan Maintenance

## Introduction

This section of the plan is to ensure that the contents of the Business Continuity and Disaster Recovery Plan are reviewed, mock disaster scenarios tested and the plan is updated and improved as needed, especially as the business grows or changes.

## Objective

The objective of this section is to provide processes to review and test the Business Continuity and Disaster Recovery Plan on a regular basis to ensure it is:

* Up to date
* Fit for purpose
* Communicated to all relevant parties.

## Plan Review

We recommend that this document is reviewed at least annually in line with all business policies.

The review process should include:

* A log of any meetings, actions or improvements, with the person responsible for the implementation of the actions or improvements and their subsequent completion recorded
* Updating the lists of Critical Business Functions and Assets
* Updating the Risk Register
* Ensuring that all stakeholders are using the most up-to-date version of the Business Continuity and Disaster Recovery Plan
* Updating the filed digital and hard copies of the Business Continuity and Disaster Recovery Plan

## Plan Testing/Simulation

Along with the review process, we also recommend testing a simulated run of an Event Activation once per year. Ideally you want to make the event as realistic as possible, involve staff and measure their response.

To undertake this simulated testing the Event Response Team will need to:

* Decide on the type of event they wish to simulate
* Decide on a day and time of the simulation
* Trigger the simulated event and Activate the Event Response Team
* Complete the Event Response Checklist
* Log any and all actions
* Confirm systems can be recovered without incident or adjust the response plan to suit
* Convene post event to identify any points for improvement and document

## Backup Testing

Additionally, we also recommend test restores on data backups are undertaken and documented at least quarterly to ensure the restorability of data. Completion of a backup doesn’t guarantee a restore is viable.

## Plan Improvements

Subsequent to both the plan review and plan testing the Event Response Team should meet to identify any improvements or areas of note and update the overall Business Continuity and Disaster Recovery Plan.

To ensure that all stakeholders are using the most up-to-date version of the Business Continuity and Disaster Recovery Plan subsequent to these reviews we recommend that you:

* Assign a version number (e.g., BCDRP v1.2) to every revision.
* Maintain a change log documenting updates and improvements.
* Distribute the latest version to all locations relevant staff.
* Archive outdated versions for reference.

**END OF DOCUMENT**