CAST COMMERCIAL ACUMEN LIMTED

Combined Business Continuity & Disaster Recovery Plan

1. Introduction

This document discusses the various disasters that could affect our business operations and outlines the options that must be considered in such circumstances. This document examines how our business could continue to operate with minimal disruption to its critical functions.

This document consists of a Business Continuity element, which focuses on:

a) Office facilities
b) Team members, and
c) Safety

It also consists of a Disaster Recovery element, which focuses on:

a) IT Recovery
b) Back up facilities, and
c) Telecoms recovery

By incorporating both types of planning, this document seeks to address critical events and actions that impact team members, facilities, and IT components in order to provide a holistic view of the recovery and continuity process.

2. Document & Version Control

Our Business Continuity Plan (BCP) & Disaster Recovery Plan (DRP) is only as effective as its last update and its last test. This documents control is assigned to Clayton John Ainger, who will be responsible for its maintenance. Whenever the document is updated, the changes should be noted as a revision and approved by the appropriate team member.

Current Control:

Document title:	Business Continuity Plan & Disaster Recovery Plan
Document status:	Final
Version number:	1.0
Date:	April 2023
Review date:	April 2025
Owner:	Managing Director
Approved by:	Clayton John Ainger
Signature:	

Version Control:

VERSION	DATE	AMENDMENTS	DETAILS	AMENDED BY
1.0	April 2023	Final version	BCP & DR Plan	CJA

BCP/DRP Contacts:

NAME	COMPANY	ROLE	MOBILE
Clayton John Ainger	CAST	MD & DPO	07495 818618
Olivia Alexandra Ainger	CAST	First Aid	07958 415416
Allison Kaye	CAST	Virtual Assistant	07702 203725

3. Assessing Our Current Situations and Risks

This document is a tool to assist our company in preparing for disaster occurrences that could make some or all of our resources unavailable for a period of time.

As a minimum, review, use and update the following questions once a quarter to help prepare our company for any such disasters and to determine our critical functions, critical hardware and software components that might be exposed to risk. Annually complete a detailed review using the checklist in Appendix 2.

Location If our main site goes down, can we continue to operate from a different site?	☐ **YES** ☐ **NO** ☐ **N/A**
Communications Do we have contact information for all team members, vendors, suppliers, insurance companies, and any other “need to know” contacts in the event of a disaster?	☐ **YES** ☐ **NO** ☐ **N/A**
Hardware Do we know what sits on each of our servers (internet, email, printing, back up, remote access etc.) and do we have this documented?	☐ **YES** ☐ **NO** ☐ **N/A**
Software What software and what versions of that software do we have and are these documented somewhere?	☐ **YES** ☐ **NO** ☐ **N/A**
Phone System Have we contacted our mobile phone provider and established a mobile phone number to be put on standby for potential redirection of our main number when and if needed?	☐ **YES** ☐ **NO** ☐ **N/A**
Paperwork Is all our paperwork backed up, scanned, or protected somehow?	☐ **YES** ☐ **NO** ☐ **N/A**
Recovery information and instructions Is our BCP / DRP stored online and accessible from a remote location?	☐ **YES** ☐ **NO** ☐ **N/A**
Backup systems Is our business data backed up and recoverable?	☐ **YES** ☐ **NO** ☐ **N/A**

4. How Will a Disaster Affect Our Business?

There are many possible disaster scenarios which can cause a wide variety of business disruptions. These disruptions can range from a component failure to a large-scale catastrophe. To make disaster planning more manageable, we have grouped these possible situations into categories, based on similar actions that will be required.

Disasters come in varying forms. We have grouped them as follows:

TYPE 1: File loss, partial system failure, phone system failure, internet failure

TYPE 2: Loss of location but the system is not affected.

TYPE 3: Full loss of system but the location is not affected e.g., Virus, equipment theft, hacking, or power outage.

TYPE 4: Full loss of location and system

TYPE 5: Loss of team members or loss of key associate trainers / training team

For the purposes of this document, we will focus on a recovery from a Full Loss of Location and System (Type 4), which encompasses recovery from all other event types except Type 5, which is addressed in the Team members Training & Recovery section towards the end of the document.

5. Response / Recovery Timelines (RRT)

Just like a government official declares a “state of emergency,” our Managing Director must decide when to call for disaster recovery actions. He must decide whether and when a BCP/DRP must be executed. It is important to set a fixed worst-case scenario timeframe for response and recovery. Critical Information may be unavailable (like when access to the building might be restored). Once we decide a DR event is occurring, we should move ahead with the BCP/DRP. Time is critical. From the start of action, a fully working office can be 48-72 hours away.

1	**Type 1**	File loss, system failure, phone system failure, internet failure, hardware failure.
	Action	Contact IT Support Provider
	RRT	Determined by IT Support.
2	**Type 2**	Loss of location, but the system is not affected
	Action	Relocate team members to home or second location
	RRT	Refer to BCP
3	**Type 3**	Loss of systems but location is not affected
	Action	Full DR implementation
	RRT	Determined by IT Support
4	**Type 4**	Full loss of site and system
	Action	Full DR & BCP Implementation
	RRT	Determined by IT / BCP
5	**Type 5**	Loss of team members, or loss of key associate trainers / training team
	Action	Engage in Recruitment
	RRT	Varies with availability, skill set required

6. Detailed Review of Disaster Event Types

DRP actions and timeframes are dependent on the type of disaster event. Once an event is defined as a disaster, recovery actions start as soon as possible, but complications and delays may impede recovery, so full recovery may take some time.

Our BCP and DRP should be able to handle the majority of disasters that can be anticipated, but as with any serious and unexpected interruption, there can be special situations / circumstances that need to be dealt with. Below are the actions, timeframes and special circumstances associated with typical disaster types.

TYPE 1 EVENT

Failure type: There is a file loss, partial system failure, phone failure or internet failure.

Action: Communicate with IT for support or phone provider.

Time to action: Immediate - establish quickest time frame to action with IT support / phone provider.

Special circumstance: If a fix is not possible within 2 days for business-critical system loss, change event to a Type 3.

TYPE 2 EVENT

Failure type: There is a loss of location, but the system is not affected.

Action: Relocate team members to backup location or home.

Time to action:

1. If our location is lost for more than 1 day, then action immediately.
2. If police of emergency services estimate that the location will be unavailable for 1 day or longer, then action immediately.

Special circumstance: If during a Type 2 event, the power is cut or systems such as internet or phones fail, then change to Type 4 event.

TYPE 3 EVENT

Failure type: There is a complete loss of the system, but the location is not affected (e.g., virus, equipment, theft, hacking or power loss.)

Action: Full DR implementation.

Time to action: Immediate - establish quickest timeframe to action with IT support / provider.

Special circumstance:

1. If any of the critical systems cannot be repaired onsite, of it the time to repair is expected to be longer than 1 day, then change to Type 4 event.
2. In this event, a loss of power will be a Type 4 event, unless a generator is available and agreed to.
3. Wholesale location theft results in a Type 4 event.

TYPE 4 EVENT

Failure type:	There is a complete loss of location and systems.
Action:	Full BCP and DRP implementation
Time to action:	1 day
Special circumstance:	It is at the Managing Director's discretion whether action is delayed until agreement is reached with the insurance provider.

TYPE 4A EVENT

Failure type:	There is a fire, flood, or similar catastrophe that wipes our everything with no possibility of location or systems being recovered.
Action:	Full BCP and DRP implementation.
Time to action:	Immediate
Special circumstance:	If there is no possibility of recovering location and repairing physical systems, contact IT support / provider.

TYPE 5 EVENT

Failure type:	Loss of team members or loss of key associate trainers / training team
Action:	Start recruitment.
Time to action:	Immediate.
Special circumstance:	For bigger pandemic type events it may be very difficult to action any plans if human movement or engagement is limited or restricted.

7. Team members Action Points

Disaster events can create confusion, panic, misinformation, and misdirection. In such situations, our people need to be informed of what has happened and instructed on what needs to happen, with each member of team members knowing his or her role in advance. A clear line of communication should therefore be established to reach all affected parties, including internal and external organisations. A list of key company contacts should also be stored and updated on a regular basis so they are immediately available should a disaster occur.

7.1. Contact Information to be stored.

a) Full and updated team members member contact list

b) Full and updated associate trainer contact list

c) Full and updated customer list

d) Full and updated supplier list

e) Office management contacts e.g., Electricity, building services, local council, emergency services.

7.2. Examples of Actions to be taken by team members during a Disaster Event.

Team Member 1:
Clayton John Ainger

- Refer to BCP plan and decide on event type and severity. Initiate team members contact.
- Engage IT support - Call IT support / provider who will proceed to action DRP dependent on event type and severity.
- Get in touch with critical contacts and inform them of the incident and estimated lead time for recovery.
- Contact insurance company and inform of the event, confirming relevant coverage and any actions required to ensure all possible claims are covered.
- Contact relevant team members under your Contact Tree Branch and pass on the message detailing the event type.
- For location loss, contact and arrange office space for the team members on a day-by-day basis, and verify that the insurance company agrees with this arrangement (where appropriate).
- Contact any live location associate trainers / training teams (refer to relevant Contact List for contact information)

Team Member 2
Allison Kaye

- Contact current clients and advise of the event type and severity along with any deadlines in the sales process that may not be met.
- Contact relevant team members under your Contact Tree Branch and pass on the message detailing the event type.

Team Member 3
Olivia Alexandra Ainger

- Contact Suppliers (Refer to relevant Contact List for Contact Information) and inform them of the event type and severity along with any critical payments that may be delayed.
- Contact relevant team members under your Contact Tree Branch and pass on the message detailing the event type.

8. BCP Location Recovery

Working space can be at a premium if a major event occurs. The inability to hold team meetings and have ongoing team interaction can severely impede business continuity. Here are three options to help us deal with loss of location in the disaster event stage.

OPTION 1 - Preferred	OPTION 2 - Backup	OPTION 3 - Last Resort
a) If space is available at a Directors home, this would be preferable to rental space for the short term.	b) Provision space is serviced offices; locate 1-3 spaces in our area and ensure we have relevant contact details.	c) Recreate our servers in a hosted environment and have all team members work done remotely from home. This solution will require an investment in standby hosting space and possibly team members equipment.
Action: Identify location and space if feasible.	**Action:** Confirm location and enter initial dialog with preferred location and provider.	**Action:** Engage hosting facility provider.

8.1. Paperwork and Non-IT Physical Items

When planning for Business Continuity, it is important to take stock all of the non-IT items that support or are a part of our business. Things like furniture items for insurance reporting, or security devices for logging into your bank, should not be taken for granted.

We may also have a lot of information on paper. Does this need to be scanned? Do we have a digital backup that can be accessed remotely? Please ensure we follow our GDPR, Data and Communication policies (https://bit.ly/CASTCoPolicies) to ensure scanning of all paperwork takes place and is stored securely in the Cloud in accordance with these protocols.

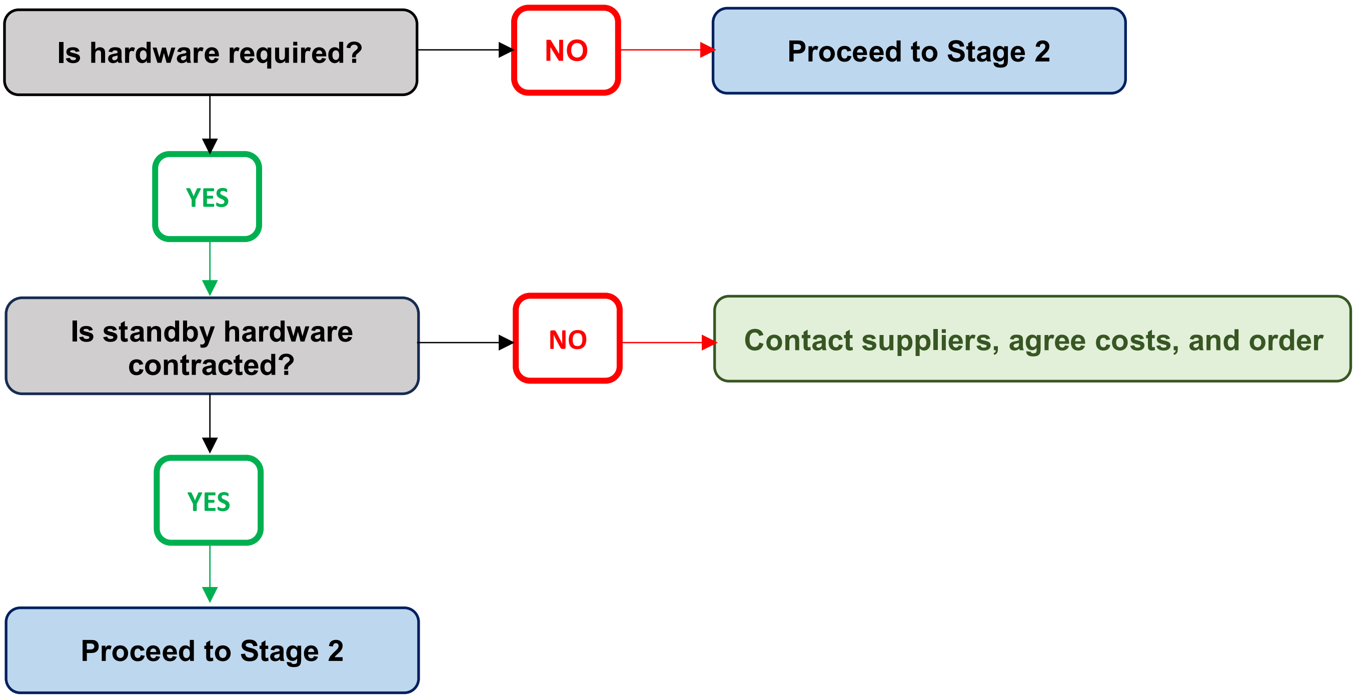
While this should be sufficient for most paperwork, there may be certain kinds (such as training programme design drawings or training plans) that would be hard to digitize and almost impossible to recreate without significant effort. These, along with sensitive information like banking figures, should be stored offsite in the home of a Director.

9. DRP - IT Recovery

A full IT and network recovery relies on information and backed up data kept away from the office. It is highly recommended that a full Disaster Recovery rehearsal is carried out at least once a year to ensure all relevant information and data is correct and recoverable. If this is not done, there is a significant chance that the recovery will suffer partial or total failure.

Once an event has been declared, the first point is to define the hardware requirement. Certain events will not need hardware e.g., Hacking or virus attacks that format the system.

9.1. Stage 1 - Hardware Requirements


Is hardware required?
NO
Proceed to Stage 2
YES
Is standby hardware contracted?
NO
Contact suppliers, agree costs, and order
YES
Proceed to Stage 2

9.2. Stage 2 - Component Recovery

External Mail **Process:** Check with our ISP provider to verify continued viability.

Internet Provider **Process:** Liaise with our ISP provider to ensure at least a viable connection for our needs, and test.

Phone System: **Process at point of failure:**

1. Contact phone provider and redirect main numbers to the standby mobile number set up and outline in Section 3 above.
2. Arrange for temporary lines. This is only actioned if a significant long-term event has occurred, as line provision may take 3-5 days to set up.
3. Contact VOIP provider and set up a temporary VOIP provision. Consider forwarding numbers to that system.
4. Test phone system functions, including inbound, outbound, voicemail, caller line identification, and call forwarding.

Servers:

Process at point of failure:

When disaster occurs and servers are gone, where is the data? Call IT support or back up vendor and request high priority copy to USB driver. Provide delivery address and confirm ETA.

Email functionality

1. Rebuild server, configure all users and applications, configure printers. Test to make sure all clients have server access, where applicable.
2. Test internal and external mail. Make sure all applications are working. Test printers.

Data Recovery

1. Recover all file data and email data (may require loss of the system while this is happening)
2. Confirm and configure any permission requirements.
3. Confirm and recover any third-party applications.
4. Test different application types and data locations on data drive. Confirm emails are accurate and complete. Confirm permissions are correct. Test third party apps.

Work Stations & Printers

To re-establish business continuity, it may be necessary for team members to work from home or from another location. Laptops can be provided to members to allow them mobility and to give them more options in team placement. Verify that laptops are covered by insurance, if the location is unsecured, take precautions to prevent theft.

After provisioning:

1. Build standard configuration for laptops.
2. Connect to network. Test user-specific settings (email, drives, printer etc)
3. Give user instructions for passwords and access.
4. Test email and printing to and from multiple locations / laptops
5. Confirm access to all file and email data.

10. TEAM MEMBERS TRAINING AND RECOVERY

As required, we will provide team training to assess our skill and knowledge levels. Our periodic testing of the DRP will reveal training needs.

Key team members will also be trained to ensure familiarity with critical server operation, software versions, phone and telecommunications equipment, and vendor information.

Where necessary, team members will be cross trained in other team member roles and responsibilities to provide backup support where needed.

We also need to ensure we have relationships with trusted recruiters and trusted training partners in case of a Type 5 event.

Appendix 1 - Contact Detail Templates

Team members Contact Details

It is useful to have a full list of all team members contact details in the event of an incident.

Name	Home Address	Email	Mobile Tel Number	Home Tel Number

Associate Trainer Contact Details

It is useful to have a full list of all associate trainer contact details in the event of an incident.

Name	Home Address	Email	Mobile Tel Number	Home Tel Number

Customer contact details

Identifying key customers is critical to business continuity planning. Their contact details should be set out below in a table similar to below.

Customer	Company	Contact Details

Suppliers contact details.

Identifying key suppliers is critical to business continuity planning. Their contact details should be set out below in a table similar to below.

Supplier	Company	Contact Details

Other useful telephone numbers (e.g., utility companies)

In the case of an DR event, it is useful to have contact details of our e.g., utility companies, quickly to hand. This will enable our business to get up and moving whether at its own location or a different location as quickly as possible.

Company/Account Details	Contact	Telephone Number(s)

Insurance Details

This section will help ensure / assess whether we have sufficient insurance in place given the nature of the potential Events.

Company	Contact	Telephone Number(s)	Policy Details

Back-up information/equipment register.

Use this section to determine what information and equipment is critical to the functioning of the business, how that information is stored and backed-up. This register should also list where its Emergency Pack is kept and what it contains.

IT records/back-up details/data location	
Critical documents records/information location	
Asset register/inventories/key equipment records	
Emergency Pack, Contents & Location	

Appendix 2 - BCP / DRP Checklist

Business Area	Question	Y, N, N/A
General	Do you test your plan regularly?	
	Does someone have overall responsibility for BCP within the organisation?	
	Do you have an emergency pack stored in a safe place? (Contains BCP, key contact information, tools (keys, torches, mobile phones etc), plan of site, IT back up disks, cash and first aid kit).	
People	Are team members aware of the BCP / DRP and do they have easy access to it?	
	Do team members know what to do in both an incident and an emergency?	
	Do you have all team member information and contact details on file? Are up to date and accessible copies of this stored off site?	
	Do your team members know where to get information/guidance in an emergency?	
	Have team members been given specific roles and received appropriate training that will be used in the event of an emergency?	
	Have team members been cross trained in colleagues' roles? Can workloads be absorbed by others in the event of absence?	
	Are team members able to work remotely in the event of an incident?	
	Can you stop performing some activities and divert resources to more essential activities if required?	
	Do you have arrangements with agencies and partners for replacing team members at short notice?	
Safety & Security	Do you have a security policy and is the security system regularly maintained?	
	Do team members know the location of stopcocks, valves, and electrics mains switches?	
	Do you regularly check all water, electricity & gas supplies are in good working order? Is there a back-up generator?	
	Do you check all team members have left the premises at the end of each day?	
	Do you turn off appliances?	
	Do you check all external doors, windows etc are shut and locked?	
	Do you check references?	
	Are contractors fully checked?	

Business Area	Question	Y, N, N/A
Premises	Do you have alternative workspace to use if necessary?	
	Do your premises comply with fire safety regulations?	
	Do you have evacuation procedures available in all buildings and are these tested regularly? Do you have evacuation points?	
	Are emergency exits clearly marked?	
	Do you have a floor plan to your building(s)?	
Documents	Do you regularly copy/backup your information?	
	Are your critical documents adequately protected?	
	Do you have copies of your critical records at a separate location?	
Equipment	Do you have an asset register?	
	Have you identified the most critical equipment, plant, and machinery?	
	Could this equipment be easily bought or leased if it was destroyed?	
	Do you hold spare parts for key pieces of plant and machinery?	
IT	Is IT critical to your business?	
	Do you have an IT recovery plan?	
	Are your computer records regularly backed up and stored in a secure location?	
	Is all anti-virus software up to date?	
	Are all team members aware of IT security policies and procedures?	
	Are alternative telephone & IT methods available?	
Hardware	In accordance with this document ensure you do a full review of Servers, PC’s, Laptops, Printers, Offsite data backup & DR Solution	
Software	Review the operating system and version, Applications, Offsite data backup & DR solution.	
Telecoms	Review the Phone system, Internet ISP, Email, Remote access	
Suppliers	Do your key suppliers have BCPs in place?	
	Have you identified alternative sources for key supplies if necessary?	
	Do you have up to date contact details for all suppliers?	

Business Area	**Question**	**Y, N, N/A**
Customers	Do you have up to date contact details for all customers?	
	Do you have customers you would need to contact in an emergency?	
	Would it affect your business if one of your key customers went out of business?	
Location	Have you identified and considered environmental risks to your business (e.g., flooding etc) and other external risks (e.g., pollution, nearby chemical plants etc)? Could an incident at a neighbour's site impact your business?	
Insurance	Do you have sufficient insurance in place to pay for: • Disruption to business. • Cost of repairs. • Hiring temporary equipment, team members. • New stock; and Temporary accommodation?	
	Do you have a copy of the insurance company's details and where is the policy (and a copy) held?	