**Text

Description automatically generated with low confidence**

**Council Name**

Business Continuity Plan

Date

**Contents**

[1. Introduction 3](#_Toc99706105)

[1.1 Purpose 3](#_Toc99706106)

[1.2 Objective 3](#_Toc99706107)

[1.3 Scope 3](#_Toc99706108)

[2 BCP Management 4](#_Toc99706109)

[2.1 Critical Business Services 4](#_Toc99706110)

[2.2 BCP Process 4](#_Toc99706111)

[2.3 Recovery 5](#_Toc99706112)

[2.4 Incident Response Priority Levels 6](#_Toc99706113)

[2.5 Escalation Path 8](#_Toc99706114)

[2.6 BCP Team Roles & Responsibilities 9](#_Toc99706115)

[2.7 BCP Communications Plan 10](#_Toc99706116)

[2.8 Communication Escalations 10](#_Toc99706117)

[2.9 BCP Scenarios & Activation Criteria 10](#_Toc99706118)

[2.10 Exercising, Maintaining and Reviewing the Plan 11](#_Toc99706119)

[2.11 Audit and Review Process 11](#_Toc99706120)

[3 Appendix A – Standing Down an Incident 11](#_Toc99706121)

[4 Appendix B – Incident Response Forms 13](#_Toc99706122)

[5 Appendix C – Emergency Numbers 18](#_Toc99706123)

[6 Appendix D – Response Team Contact List 18](#_Toc99706124)

[7 Appendix E – Key Suppliers 19](#_Toc99706125)

[8 Appendix F – Key Customers (if applicable) 20](#_Toc99706126)

[9 Appendix G – Key Sites in the event of a Business Disruption 20](#_Toc99706127)

[10 Appendix H – BCP Communication Plan 20](#_Toc99706128)

[11 Appendix J – Definitions 21](#_Toc99706129)

# **Introduction**

## **Purpose**

The purpose of this Business Continuity Plan (BCP) is to define how Council Name will respond to and manage incidents in the case of a disaster or other disruptive incidents and the steps that will be taken to recover Council activities within set timeframes.

This plan is focused on ensuring that the Councils Recovery Time Objectives (RTO) and Recovery Point Objective (RPO) for critical Council services have been documented and achievable. See Appendix J: RTO and RPO definitions for further details.

## **Objective**

The following are the specific objectives of this BCP:

* Serve as a guide for the Council Name response teams
* Embed business continuity management into the culture of Council Name
* Anticipate and manage changes and challenges to Council demands
* Complete and maintain a business impact analysis identifying critical Council services
* Minimise disruption to Council Name‘s operations
* Ensure that Council Name‘s critical business processes can maintain continuity of service
* Ensure that clear step by step direction is given to the Council’s recovery team to help them to meet the above objectives
* Set clear accountabilities and responsibilities for enactment of the continuity plan, operation of the plan in the event of an incident, and resumption of normal business processes
* Ensure the business continuity plans are tested and reviewed on a regular basis
* Identify vendors and customers that must be notified in the event of a disaster
* Document storage, safeguarding and retrieval procedures for vital records
* *Add additional objectives as required ……*

## **Scope**

The scope of this plan is confined to critical business services, as defined by the Business Impact Assessment (BIA). The business service will include information systems, internal processes, resources, and the data required to deliver critical business services in Council Name. The BIA process determines if that business service is deemed “Critical”, “Important” or “Normal”. This scope of this BCP, is to develop plans for Business Services that have been deemed “Critical” from the BIA process.

The plan will provide the basis to:

* Protect the safety of Council Name Staff, Contractors and visitors.
* Protect Council Name Property and assets.
* Minimise disruption to a critical Council service.
* Facilitate restoration to normal service provision.

# **BCP Management**

## **Critical Business Services**

A BIA should be conducted to understand Council Name services and the impact of their disruption. This includes the identification and prioritisation of key components (e.g., products, services, business functions, key people and processes) as part of the BIA exercise.

The Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are defined to determine the prioritisation. Do

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Business Service** | **Service Owner** | **Level** | **RTO** | **RPO** | **Order of Recovery** |
| Data Centres |  | Critical | RTO-0 1 hour or less to restore | RPO-0 No Data Loss | 1 |
| Communications |  | Critical | RTO-1 2 hour or less to restore | RPO-1. 1 hour or less of data loss | 2 |
| Databases |  | Critical | RTO-1 2 hour or less to restore | RPO-1. 1 hour or less of data loss | 3 |
| Connectivity - networks |  | Critical | RTO-1 2 hour or less to restore | RPO-1. 1 hour or less of data loss | 4 |
| IT Service Desk |  | Critical | RTO-2 4 hours or less to restore | RPO-2 2 hours or less of data loss | 5 |
| Security Tools |  | Critical | RTO-2 4 hours or less to restore | RPO-2 2 hours or less of data loss | 6 |
| Payment System |  | Critical | RTO-3 8 hours or less to restore | RPO-2 4 hours or less of data loss | 7 |

## **BCP Process**

The decision to activate the BCP, in part or full, will be made by the BCP Coordinator in conjunction with the Incident Management Team (IMT).

The process is as follows:

* A potential incident or disaster is reported by an internal or external user to service desk or line manager.
* The potential incident or disaster is escalated to the IMT.
* The IMT triages the potential incident or disaster and assess the BCP priority and informs the BCP Coordinator.
* The BCP Coordinator will notify appropriate stakeholders if priority levels 1 or 2 should be activated.

The BCP Coordinator will activate the priority 1 and priority 2 BCP plan during Triage if the event is out of hours and it is time sensitive and requires an immediate decision.

## **Recovery**

The IMT will manage, via the BCP Coordinator, a process for recovery from an incident. See Appendix A: Standing Down an Incident.

Recovery will include:

* Identification of the resources needed for instigating the recovery strategy for the BCP. The BIA will identify the prioritisation to restore critical Council functions.
* Understanding the costs involved in responding to and restoring from the incident.
* Create a report of the incident or disaster.
* Identify any lessons learnt.

## **Incident Response Priority Levels**

| Priority | Definition | Example | Impact |
| --- | --- | --- | --- |
| Priority 5 | Disruption to an **individual** but otherwise normal working conditions | Loss of an individual’s equipment such as phone or laptop. | * Any events affecting an individual’s normal working arrangements should be referred to relevant line manager. * The IMT should carry out a risk assessment to understand the impact to Council Name and start the process to mitigate any risks. |
| Priority 4 | Disruption to a **small local team** but otherwise normal working conditions | Staff absence within a team. | * To be dealt with by appropriate management action. |
| Priority 3 | Disruption localised to a **geographical area** but otherwise normal working conditions | Fire, Flood, or staff absence due to sickness or weather. | Following immediate risk assessment and liaise with the IMT:   * To be assessed by the BCP coordinator. * Incident Form to be completed. |
| Priority 2 | Disruption to a **business unit** that affects the majority of staff impacting normal working conditions | Major incident or emergency. | The IMT should initiate an immediate response with either an evacuation or a Major Incident implementation to ensure they have secured the safety of all affected personnel:   * IMT to consider appropriate response as Serious Incident or emergency requiring Business Continuity Plan activation. * IMT to be stood up and undertake initial assessment and implement the BCP. * IMT to escalate to senior management. |
| Priority 1 | Disruption to the **whole Council** or serious health and safety issues impacting normal working conditions. | Country wide incident or major pandemic illness. | The IMT should initiate an immediate response with a Major Incident implementation to ensure they have secured the safety of all affected personnel:   * IMT team to escalate to Executive Management. * IMT with Executive Management support to be stood up and undertake initial assessment and implement the business continuity plan. |

## **Escalation Path**

The decision to activate the BCP, in part or full, will be made by the BCP Coordinator in conjunction with the IMT.

## **BCP Team Roles & Responsibilities**

The following teams within Council Name will be responsible for managing any BCP event and will be authorised to perform certain activities. (e.g. activation of the plans).

| **Role** | **Responsibilities** |
| --- | --- |
| **CEO** | * Maintain current awareness of any major BCP activities and provide ongoing guidance and strategic decision making * Inform the relevant stakeholders of any BCP events that might affect them * Authorised to declare a crisis |
| **Senior Management Team (SMT)** | * Maintain current awareness of all relevant BCP activities and provide ongoing guidance and decision making * Regularly inform the CEO’s Office and relevant stakeholders of any BCP events that might affect them * Provide authorisation to invoke plan * Authorised to declare a crisis in the absence of the CEO |
| **BCP Coordinator** | Management interface between the IMT and SMT.   * Conduct the initial BCP assessment * Assumes operational management of Disaster Recovery Response * Mobilise the IMT * Confirm the correct teams have been deployed * Provide updates to Senior Management for the entire duration of a the BCP event * Provide management reports on any BCP event and identify any Lessons Learned * Review and develop Business Continuity response plans |
| **Incident Management Team (IMT)** | * Participate in initial BCP event assessment * Keep a log of responses to the BCP event * Report to the BCP Coordinator with continuous updates * Respond to BCP Coordinator instructions * Act as a subject matter expert to support the BCP Coordinator response * Individual who is on duty at the time an incident needs to be categorised. They will select the correct response plan to any incident or disaster report. * Oversee the development, maintenance, management, and improvement of business continuity plans and the associated business continuity management system |
| **Communications** | The Communications Manager will have a key role in any major disaster or incident. This role will have to plan the communications for business recovery and liaise with the IMT, BCP Coordinator and SMT in line with the communications strategy. |
| **Specialist Support** | Depending on the nature of the disaster or incident, there may be a requirement to call upon subject matter experts to provide the specialist support needed for a recovery. |

## **BCP Communications Plan**

This section defines what BCP content shall be communicated across Council Name’s internal, external and interested stakeholders. See Appendix H for further details.

The Communications Manager in consultation with the IMT will develop a communications plan to cover communications with:

* Staff
* Media
* Partner organisations
* External users

## **Communication Escalations**

In the event of any incident or disaster, the staff member or line manager involved should contact the BCP Coordinator immediately, who will then communicate the event to the IMT. Post IMT triage, the BCP Coordinator will engage with the relevant manager regarding actions, who will in turn communicate to the other members of the SMT and CEO as appropriate dependent of the prioritisation category of the incident.

Where an external facing business service is unavailable and impacts the external users and/or external stakeholders of Council Name, an external communication will be issued to inform the relevant stakeholders and users affected by the incident or disaster. This will explain the situation in as much detail as is appropriate and in a timely and transparent manner.

## **BCP Scenarios & Activation Criteria**

There are three core categories that could potentially initiate the BCP.

* Environmental Disaster: (Flood Fire, Pandemic, Public Health Emergency)
* Operational Disaster: (Explosions, Cyber Misconfiguration, Data Protection, Intrusion, Loss of Staff, Single Points of Failure (SPOF), lack of availability for third parties, knowledge transfer, physical damage to networks etc.)
* Malicious and Wilful damage: (Cyber DoS, civil disturbance. Workplace violence, cybercrime.)

Situations where an enactment of the plan may be required include but are not limited to:

* Disaster incident at the Council Name’s office premises including IT infrastructure:
* Cyber-attack / Ransomware
* Loss of telecommunications
* Loss of power
* Loss of access to the building
* Fire
* Flood
* Internal damage (i.e., water damage, electrical fault, etc.)
* An extended utility failure
* Building closure due to contamination
* Major natural disaster
* An act of terrorism

Generally, activation scenarios can be grouped by the potential impact on the ability of staff to access their desks and conduct business on a day-to-day basis.

There are a number of activities that are needed to address disruptions to Council services prior to a full business continuity response being activated.

However, at the point of a significant event, the need to respond to an emergency will need to be carried out in parallel with a review of the impact on Council Name services and the activation of appropriate plans to ensure their continuation or recovery over the shortest period possible.

Activation of a BCP is not automatic and requires the decision of the IMT to escalate to the SMT.

## **Exercising, Maintaining and Reviewing the Plan**

Council Name will test its BCP on a regular basis. This will include:

* A review of the BCP every year.
* A tabletop exercise every year.
* A ‘live’ exercise every 3 years.

Council Name will conduct their own internal workshops and tabletop exercises.

## **Audit and Review Process**

Council Name’s BCP should be subject to audit in the following ways:

* Internally and annually via the IMT
* Regularly by Internal Audit
* Post Incident

Routine responsibility for ensuring the BCP is up to date and fit for purpose rests with the IMT, on behalf of the Council Name CEO.

# **Appendix A – Standing Down an Incident**

|  |
| --- |
| **Activity** |
| BCP Co-ordinator ensures all IMT are formally ‘stood down’. |
| BCP Co-ordinator assign write up of all event logs. |
| Review all completed logs with the IMT. |
| Ensure all logs, emergency reports and status reports are collected and retained in a safe place. |
| Ensure welfare support arrangements are made available to staff (if applicable). |
| Consider providing staff with a post–emergency briefing (email, letter, presentation) thanking them for their co-operation and providing them with an overview of the situation. |
| Liaise with stakeholders as deemed appropriate in order to provide reassurance / visibility. |
| Review status of business continuity related actions, identifying assistance / support required from response team members. |
| Make arrangements to ensure any resources that may be needed to support a future emergency response are replenished. |
| Make arrangements for full review of the disaster and response to ensure that improvement actions are identified and implemented. |

# **Appendix B – Incident Response Forms**

Upon notification of an incident/disaster situation the BCP Coordinator will make the initial entries into this form. It will then be forwarded to the IMT, where it will be continually updated. This document will be the running log until the incident/disaster has ended and “normal business” has resumed.

**B.1 Incident Handling and Response Check**

|  |  |  |
| --- | --- | --- |
| **#** | **Action** | **Completed** |
|  | **Detection and Analysis** |  |
| **1.** | Determine whether an incident has occurred |  |
| **1.1** | Analyse the precursors and indicators |  |
| **1.2** | Look for correlating information |  |
| **1.3** | Perform research (e.g. search engines, knowledge base) |  |
| **1.4** | As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence |  |
| **2.** | Prioritise handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.) |  |
| **3.** | Report the incident to the appropriate internal personnel, and consider whether specialist external support is required |  |
| **4.** | Report the incident to the appropriate external/regulatory bodies, such as the ICO or police as required |  |
|  | **Containment, Eradication, and Recovery** |  |
| **4.** | Acquire, preserve, secure, and document evidence; this may require specialist skills. |  |
| **5.** | Contain the incident |  |
| **6.** | Eradicate the incident |  |
| **6.1** | Identify and mitigate all vulnerabilities that were exploited |  |
| **6.2** | Remove malware, inappropriate materials, and other components |  |
| **6..3** | If more affected hosts are discovered (e.g. new malware infections), repeat the Detection and Analysis steps to identify all other affected hosts, then contain and eradicate the incident for them |  |
| **7.** | Recover from the incident |  |
| **7.1** | Return affected systems to an operationally ready state |  |
| **7.2** | Confirm that the affected systems are functioning normally |  |
| **7.3** | If necessary, implement additional monitoring to look for future related activity |  |
|  | **Post-Incident Activity** |  |
| **8.** | Create a follow-up report |  |
| **9.** | Conduct a lesson learned meeting (mandatory for major incidents, optional otherwise) |  |
| **10.** | Resolve any outstanding legal, regulatory, or contractual issues or concerns |  |

**B.2 Incident Response Report**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **General Information** | | | | | | | | | | | | | | | | | | |
| **Incident Number:** <###-MMYYYY or ServiceDesk #> | | | | | | | | | | | | | | | | | | |
| **Incident Detector’s Information** | | | | | | | | | | | | | | | | | | |
| **Name:** | |  | | | | | | **Date and Time Detected:** | | | | |  | | | | | |
| **Title:** | |  | | | | | | **Detector’s Location:** | | | | |  | | | | | |
| **Phone:** | |  | | | | | | **Additional Information:** | | | | |  | | | | | |
| **E-mail:** | |  | | | | | |  | | | | |  | | | | | |
|  | |  | | | | | |  | | | | |  | | | | | |
| **Incident Summary** | | | | | | | | | | | | | | | | | | | |
| **Incident Type** | | | | | | | | | | | | | | | | | | | |
| Security Privacy | | | | | | | | | | | | | | | | | | | |
| **Incident Priority** | | | | | | | | | | | | | | | | | | | |
| High | | | | | Medium | | | Low | | | | | | None | | | | | |
| **Incident Impact** | | | | | | | | | | | | | | | | | | | |
| None | Privacy / Confidentiality Breach | | | | | Proprietary Breach | | | | Integrity Loss | | | | | | Availability Loss | | | |
| **Type of Incident Detected (Check All that Apply)** | | | | | | | | | | | | | | | | | | | |
| Unauthorised Access | | | | Unauthorised Disclosure | | | | Malicious Code | | | | Probe | | | | | Hoax |  | |
| Unauthorised Use | | | | Denial of Service | | |  | Other: | | |  | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | |
| **Incident Location (Site):** |  | | | | | | | | **Site Point of Contact:** | | | | | |  | | | | |
|  | | | | | | | | | | | | | | | | | | | |
| **Reported externally, e.g. to the ICO or police (provide details):** | | | | | | | | | | | | | | | | | | | |
| **Responder’s Information** | | | | | | | | | | | | | | | | | | | |
| **Responder Name:** | | |  | | | | | **Date of Response:** | | | |  | | | | | | | |
| **Phone:** | | |  | | | | | **Time of Response:** | | | |  | | | | | | | |
| **Email:** | | |  | | | | |  | | | |  | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Incident Details** | | | | | | | | | | | | | | |
| **How the Incident was Detected:** | |  | | | | | | | | | | | | |
|  | |  | | | | | | | | | | | | |
|  | |  | | | | | | | | | | | | |
|  | |  | | | | | | | | | | | | |
|  | |  | | | | | | | | | | | | |
| **Location(s) of Affected Systems (at site):** | | | |  | | | | | | | | | | |
|  | | | |  | | | | | | | | | | |
|  | | | |  | | | | | | | | | | |
|  | | | |  | | | | | | | | | | |
|  | | | |  | | | | | | | | | | |
| **Classification of System(s) or Data Impacted:** | | | | | | Sensitive | | | | | Confidential | |  |  |
|  | | | | | | Restrict | | | | | Public | |  |  |
|  | | | | |  | | |  | | | |  | |  |
| **Was Customer Data Impacted:** | | * Yes | | | * No | | |  | | | |  | |  |
|  | |  | | |  | | |  | | | |  | |  |
| **Type of Data Impacted:** | Personally Identifiable Information (PII) | | | | | | | | | Credit Card Information | | | | |
|  | Protected Health Information (PHI) | | | | | | | | | Financial Information | | | | |
|  | Source Code | | | | | | | | | Organisational Information | | | | |
|  | Employment Records | | | | | | | |  | | | | | |
|  | Other: | | | | | |  | | | | | | | |
|  |  | |  | | | | | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Affected Systems** | | | | | | | |
| **Describe affected Information System(s) (One Form per System is Recommended)** | | | | | | | |
| **Make:** |  | | **Serial Number:** |  | | | |
| **Model:** |  | | **Asset Number (If Applicable):** | | | |  |
| **Hostname:** |  | | **Operating System:** | |  | | |
| **IP Address:** |  | | **Function or Purpose:** | | |  | |
| **Description of Incident Status:** | |  | | | | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
| **Incident Response Steps Taken:** | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
| **Estimated Technical Impact:** | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
| **Incident Handler Comments:** | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
| **Resolution:** |  | |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | | |
|  |  | | |
|  |  | | |
|  |  | | |
|  |  | | |
|  |  | | |
|  |  | | |
| **List of Evidence Collected:** | | **1:** |  |
|  | | **2:** |  |
|  | | **3:** |  |
|  | | **4:** |  |
|  | | **5:** |  |

|  |  |  |
| --- | --- | --- |
| **Council Staff / Key Suppliers Contacted** | | |
| **Name** | **Type** | **Comments** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# **Appendix C – Emergency Numbers**

**First Responders, Public Utility Companies, Others**

|  |  |  |  |
| --- | --- | --- | --- |
| **Utility Name** | **Contact Name** | **Email** | **Phone Number** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# **Appendix D – Response Team Contact List**

**Response Team**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Address** | **Home Phone** | **Mobile Phone** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Operations**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Address** | **Home Phone** | **Mobile Phone** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# **Appendix E – Key Suppliers**

**Server and Computer Equipment Suppliers**

|  |  |  |  |
| --- | --- | --- | --- |
| **Company Name** | **Contact Name** | **Email** | **Phone Number** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Communications and Network Services Suppliers**

|  |  |  |  |
| --- | --- | --- | --- |
| **Company Name** | **Contact Name** | **Email** | **Phone Number** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Mechanical Engineering (HVAC, Facilities, etc.)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Company Name** | **Contact Name** | **Email** | **Phone Number** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Plumbing**

|  |  |  |  |
| --- | --- | --- | --- |
| **Company Name** | **Contact Name** | **Email** | **Phone Number** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Site Security Services**

|  |  |  |  |
| --- | --- | --- | --- |
| **Company Name** | **Contact Name** | **Email** | **Phone Number** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# **Appendix F – Key Customers (if applicable)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Company Name** | **Contact Name** | **Email** | **Phone Number** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# **Appendix G – Key Sites in the event of a Business Disruption**

Recovery sites are locations pre-designated in a BCP, other than the primary Council site. They are used to coordinate the recovery effort and/or to recover the functionality of business processes in the event of a disaster.

**Office Locations**

|  |  |
| --- | --- |
| **Description of Site Purpose** | **Location** |
|  |  |
|  | |
|  | |
| **Contact Details**  <phone numbers>  <phone numbers>  <phone numbers> | |

**Meeting Locations**

[Insert meeting location details]

# **Appendix H – BCP Communication Plan**

[Insert crisis communication plan]

# **Appendix J – Definitions**

For the purposes of this plan, the following terms will have the meaning as described below:

|  |  |
| --- | --- |
| **Business continuity** | The capability of the Council to continue delivery of products or services at acceptable predefined capacities following a disruption. |
| **Business continuity management** | The process of implementing and maintaining business continuity and is about preparing a Council to deal with disruptive incidents in order to prevent loss and prepare for, mitigate and manage disruptions. |
| **IT Disaster Recovery (ITDR)** | ITDR is the ability to react to ITDR events in a controlled, pre-planned manner. |
| **Business Continuity Plan (BCP)** | A document that outlines how a Council will continue operating during an unplanned disruption in service. |
| **RTO** | The recovery time objective (RTO) is the maximum amount of time a system resource can be unavailable before there is an unacceptable impact on other system resources or business processes.  For further information please refer to the “***IT Disaster Recovery (ITDR) Plan and Process Guide***”. | |
| **RPO** | The recovery point objective (RPO) represents the point in time, prior to a disruption or system outage, that data can be recovered (in other words, the acceptable data loss).  For further information please refer to the “***IT Disaster Recovery (ITDR) Plan and Process Guide***”. | |
| **Business Impact Assessment (BIA)** | Tells us what is critical and essential. | |
| **Disaster** | An event that results in damage or destruction, loss of life, or drastic change to the environment. | |
| **Incident Management Team (IMT)** | The team that will carry out the initial triage of any incident and then respond as required by the BCP to any incident.  Oversees the development, maintenance and improvement of business continuity plans and the associated business continuity management system. | |
| **Disaster - Business Context** | In a business context, a disaster is an unplanned event that has the potential to disrupt the delivery of mission-critical services and functions, jeopardise the welfare of employees, customers, or business partners, and/or cause significant financial harm. |
| **Disaster - Security Context** | From a security perspective, a disaster manifests itself as a sustained disruption of system availability and/or confidentiality or integrity controls. The cause can be environmental, operational, accidental, or wilful. |
| **Environmental Events** | Severe weather, earthquakes, fire, flood, air contaminants, and public health emergencies. | | |
| **Operational issues** | Failures or misconfiguration of equipment, disruption of communication systems, unavailability of third-party systems or personnel, and degradation of power. | | |
| **Accidents** | Nuclear, biological, or hazardous chemical exposure, explosions, and user or operator error. | | | |
| **Wilful damage** | Cyber crime, terrorism, sabotage, civil disturbances, war, workplace 'and surrounding area'. | | | |
| **Business Continuity Threat:** | A potential danger to the Council. Threats can be business specific, local, regional, national, or even global. | | | |
| **Business Continuity Threat Assessment** | Identify viable threats and predict the likelihood of occurrence. Threat modelling should take into account historical and predictive geographic, technological, physical, environmental, third-party, and industry factors. | | | |
| **Business Impact Assessment (BIA)** | Identify essential services/processes and recovery timeframes. | | | |
| **Critical Service** | Critical means that the absence or disruption to a service would result in significant, irrecoverable, or irreparable harm to the organisation, employees, business partners, external users or community. | | | |