**BUSINESS CONTINUITY PLAN – TEMPLATE**

Note: Delete this page once you complete the template.

**Who should use this template?**

Any organisation who requires a business continuity plan (BCP) to ensure the organisation can continue to operate.

**How to use this template**

* Make a copy of the template and save it with reference to your organisation
* All sections are for consideration as follows:
  + Mandatory: this section is core to building a business continuity plan to capture important information that would assist your organisation to recover.
  + Elective: this section may/may not be applicable depending upon your organisation’s structure and setup.
* Guidance text appears throughout the document, marked by the word Guidance. Where you see a guidance note, read and then delete it. Guidance has been added to help you complete the template and should not appear in your final version.
* [Placeholders] that have been left within the document to indicate editable sections
* <<insert content>> placeholders that require information specific to your organisation
* Appendix references:
  + Appendix A contains a Business Impact Analysis template that can be customised to understand resource requirements and priorities in the event that a disaster impacts your organisation.

**Disclaimer**

The information in this template is for general guidance only. The Digital Transformation Hub does not make any representations or warranties (expressed or implied) as to the accuracy, currency or authenticity of the information. The Digital Transformation Hub, its end users and agents do not accept any liability to any person for the information or advice given in this document.

[Insert Company Logo Here]

Business Continuity Plan

Version - 0.1

Effective Date: **<< Date Month Year>>**

**Contents**

[1. Introduction 4](#_Toc104538640)

[2. Business Impact Analysis 4](#_Toc104538641)

[3. Risk assessment 4](#_Toc104538642)

[3.1. Assumptions 4](#_Toc104538643)

[3.2. Disaster events 5](#_Toc104538644)

[3.2.1. Loss of building/functions 6](#_Toc104538645)

[3.2.2. Loss of technology 6](#_Toc104538646)

[4. Priorities, Roles and Responsibilities 6](#_Toc104538647)

[5. Execution of the plan 9](#_Toc104538648)

[5.1. Activate the Emergency Evacuation Procedures 9](#_Toc104538649)

[5.2. Activate the Business Continuity Plan 9](#_Toc104538650)

[5.3. Communication Priorities and Processes 10](#_Toc104538651)

[5.4. Reinstate Services at the office 11](#_Toc104538652)

[5.5. Transition to business continuity plans for specifc issues 13](#_Toc104538653)

[5.5.1. Business continuity plans by issue 13](#_Toc104538654)

[5.5.2. Payroll 13](#_Toc104538655)

[5.5.3. Finance payments 13](#_Toc104538656)

[5.5.4. Email 14](#_Toc104538657)

[5.5.5. Network (including file & print) & remote access 15](#_Toc104538658)

[5.5.6. Phones – landlines 16](#_Toc104538659)

[5.5.7. Phones – mobile 16](#_Toc104538660)

[5.5.8. [Specialist application] and accounting systems 17](#_Toc104538661)

[6. Emergency delegations list 18](#_Toc104538662)

[7. Testing the plan 18](#_Toc104538663)

[8. Contact lists 19](#_Toc104538664)

[8.1. Staff call tree 19](#_Toc104538665)

[8.2. Staff, supplier, and stakeholder contact lists 19](#_Toc104538666)

[9. Version Information and Changes 20](#_Toc104538667)

[Appendix A – Business Impact Analysis approach 21](#_Toc104538668)

# Introduction

Mandatory

This business continuity plan (BCP) has been developed to minimise disruption to <<Organisation Name>> products and services in times of crisis. It is a plan of actions required of the business if normal business activities cannot be continued due to a disabling event such as loss of technology, unavailability of office premises or a large proportion of staff.

The business continuity plan:

* formalises the actions required in a realistic manner
* minimises the downtime for the business, and
* identifies business priorities so that if limited services are available, these can be allocated effectively.

# Business Impact Analysis

Mandatory

Guidance: A Business Impact Analysis (BIA) facilitates the identification and documentation of:

* your organisation’s key products and services
* the activities and business processes required to deliver these
* the impact that a disruption to these business processes would have on your organisation
* the resources required to resume these activities and business processes.

Refer to Appendix A for templates to assist with working through this process in your organisation. Complete the Business Impact Analysis sections to provide a foundation for your business continuity plan.

**Note**: Using the results of the BIA and the risk assessment, you could outline certain business continuity scenarios for your organisation. These scenarios should be linked to the highest impacts to your organisation (i.e. loss of provision of key products or services) in the event of risks eventuating (from section 3 below) and determine the contingencies that you need to put in place. Refer to the table titled ‘Using Business Impact Analysis to build a plan’ in Appendix A for examples of these contingencies.

# Risk assessment

Mandatory

Guidance: A risk assessment is important to work through to identify potential scenarios that could impact on the operations of the organisation.

## Assumptions

Guidance: Some example assumptions are detailed below. List the assumptions that may be relevant to your organisation.

* Because <<Organisation Name>> operates from a single office, it is possible that the whole of the <<Organisation Name>>’s core business could be disrupted.
* Business support system failure could disrupt business, but the assumption is that serious disruption is not likely to occur until at least after a week of failure. The business continuity plan takes this into account.

## Disaster events

There are a number of potential disruptive threats which can occur with impacts to normal business operations.

Guidance: The table below lists potential scenarios. Determine the applicability of these scenarios to your organisation, add additional scenarios that may apply, and populate the additional columns to identify actions that can be taken in response.

Probability: 1=Very Low, 5=Very High.

Impact: 1= Minor inconvenience, 5= Critical impact.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Potential scenario** | **Probability Rating** | **Impact Rating** | **Description of potential consequences and remedial actions**  **(short-term)** | **Description of potential consequences and remedial actions**  **(long-term)** |
| Flood / Fire / Loss of building access |  |  |  |  |
| Electrical power failure |  |  | e.g. Redundant UPS array with standby generator tested weekly and remotely monitored. |  |
| Cyber security incident |  |  |  |  |
| Loss of communications network services |  |  |  |  |
| Loss of internet connectivity at primary site |  |  |  |  |
| Key third party supplier impacted |  |  | e.g. Contingency plans identified and documented in <<xxx>> location |  |
| Staff illness |  |  |  |  |
| … |  |  |  |  |

Elective

Guidance: The following sections outline particular scenarios that can be used as reference examples for your organisation’s business continuity scenarios.

This plan concentrates on the events that are most likely to occur. These three events (in order of impact) are:

1. Loss of office building (e.g. earthquake, fire)
2. Loss of office building functions (e.g. electricity, gas, flood)
3. Loss of technology:
   1. Payroll
   2. Finance payments
   3. Email
   4. Network (including file and print) and remote access
   5. Phones – landlines
   6. Phones – mobile
   7. [specialist application] and accounting systems.

.

### Loss of building/functions

A key risk for staff is inability to access or leave the office building. Departure or access may be denied as a result of transport failure, nature (e.g. floods, earthquake), personnel or political reasons.

The key response for responding to inability to depart or access the building is outlined below. Specific instructions for particular issues are detailed in the specifc business continuity plans by issue.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Characteristics of interruption* | *Risk assessment rating* | ***Action for short term interruption***  *(up to 1 week)*  *[Recovery Location]* | *Action for long term interruption* | |
| More than 1 wk (less than 1 mth) | **More than 1 mth** |
| **[Recovery location]** | **[Recovery location]** |
| No access to the local area housing the office premises | med | This would be a civic emergency and beyond the business continuity plan | | Staff to relocate to business recovery office |
| Staff unable to leave the office building | low-med |
| No access to the block on which office is located | med-low | Staff work off-site or remain at home | | Staff to relocate to business recovery office |

### Loss of technology

<<Organisation Name>> is heavily reliant on the information technology systems for the following areas:

Guidance: Outline IT systems/services for your organisation. Some examples are provided below.

The requirements of this section may be fulfilled by elements of a Disaster Recovery Plan.

* Payroll
* Finance payments
* Email communications
* Network (including file and print) and remote access
* Phones – landlines
* Phones – mobile
* [Specialist application] and accounting systems.

# Priorities, Roles and Responsibilities

Mandatory

Guidance: Identify the key priorities and roles and responsibilies required in the event of a disaster that requires enactment of the business continuity plan.

Examples are provided in the table below.

During an emergency these are the **priorities** for <<Organisation Name>>.

|  |  |
| --- | --- |
| General | All <<Organisation Name>> staff are safe and accounted for.  <<Organisation Name>> manages the situation by ensuring that:   * Managers or others notify the Business Continuity Manager (BCM immediately of business interruption issues * staff actions and priorities are consistent with overall business recovery strategy * there are manual workarounds for critical business processes * the public can be provided with fundamental services at an appropriate level. |

|  |  |
| --- | --- |
| Critical business function | Critical business functions of the <<Organisation Name>>:   * communications   + set up a central area for <<Organisation Name>> staff and key stakeholders, and in time the public   + ensure travelling staff know the extent of the emergency and have a contact number for <<Organisation Name>>’s office * establish what electronic systems are available and set up for use * ascertain what business functions will be provided. |

|  |  |
| --- | --- |
| Civil Defence Emergency | <<Organisation Name>> is not an organisation which manages major resources essential for an effective response in the event of a national emergency, and is therefore not a national body with a major civil defence role.  <<Organisation Name>>'s objective during a civil defence emergency is the safety of its staff and the maintenance of the essential functions of the office. |

In an emergency, the **roles and responsibilities** required to enact a response include:

|  |  |  |
| --- | --- | --- |
| Role | Who | Responsible for |
| Business Continuity Manager (BCM) | [indicate organisational role] | * Contacting the Chief Review Officer at first knowledge of an emergency * Arranging the initial meeting of the Emergency Decision Group (BCM, CRO and Technology Advisor) regarding: * activating the Business Continuity Plan * immediate emergency tasks * critical business functions and business recovery location * reinstating services at <<Organisation Name>>. |
| Chief Review Officer (CRO) | [typically Chief Executive Officer or the Deputy Chief Executive Officer] | * Contacting the BCM at first knowledge of an emergency * Ratifying the decisions of the Emergency Decision Group * Leading the <<Organisation Name>> Management team * Communicating to the organisation (including the board). |
| Technology Advisor | [typically a CIO /IT support provider/consultant] | * Co-ordinate the managment of ICT Disaster Recovery Planning. |
| Communication Contact Role | [typically a Marketing Executive or the Development Executive with Communications reponsibilities] | * Communicating with: * stakeholders * other Government departments and agencies * external clients including the media. |

# Execution of the plan

Mandatory

Guidance: This section oulines the steps to be taken to execute the business continuity plan within your organisation. Examples of actions and roles are provided within the tables below.

Edit this section to reflect the process that will be used by your organisation.

## Activate the Emergency Evacuation Procedures

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **When** | **Who** | **Procedure** | **Step** | **Action** | **Who/**  **completed** |
| As soon as you are informed of the emergency situation | <<Indicate role>> | The building is cleared of all staff using Emergency Evacuation Procedures |  |  |  |

## Activate the Business Continuity Plan

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **When** | **Who** | **Procedure** | **Step** | **Action** | **Who/**  **completed** |
| As soon as you are informed of the emergency situation | <<Indicate role>> | <<Indicate role>> follows this procedure to activate and implement the BCP | 1 | Take details of the emergency from the initial call:   * what has happened * access to the building * who has been contacted (emergency services, key recovery teams, Department Managers) * details of any immediate injuries, etc to staff. |  |
|  |  |  | 2 | Check that the Evacuation Procedures are underway and request regular updates are provided to <<indicate role>>. |  |
|  |  |  | 3 | * Convene a meeting of the Emergency Decision Group (BCM, CRO and Technology Advisor) which assesses the impact of the emergency on the business and decides the following: * activating the BCP * immediate emergency tasks (1st hour's response) * determine the key business functions to carry out * agree the need and location of a business recovery office; assign role of Business Recovery Office Manager * assign individual to carry out the Communication Contact role who will communicate with internal and external stakeholders (as per section 5.3 Communication Priorities and Processes) * key staff members to remain on-site and agree actions for remaining staff |  |
|  |  |  | 4 | * Advise managers of decisions made and have them relay the information to their staff members. |  |
|  |  |  | 5 | * Contact staff members to take on the roles outlined in Section 4. Priorities, Roles and Responsibilties. |  |
|  |  |  | 6 | * Ensure appropriate delegated authorities are in place. |  |

## Communication Priorities and Processes

In the event of a disaster, communication with internal and external stakeholders is required to provide information on the impacts to the organisation’s operations and timelines for recovery. The <<insert role>>is responsible for contacting <<Organisation name>>’s stakeholders.

| **Stakeholders**  [Edit this section to reflect your Organisation] | **Communication content (examples only)**  [Edit this section to reflect your Organisation] | **Contact details** |
| --- | --- | --- |
| Internal Stakeholders (e.g. staff, board members, etc) | e.g. Implications of the disaster and impacts on IT systems and applications i.e. what services have been impacted. | <<insert process to be used to communicate with stakeholders>> |
| External stakeholders (e.g. authorities, clients, supporters, etc) | e.g. Anticipated impact on services, security of client information, actions being taken and anticipated timelines. | <<insert process to be used to communicate with stakeholders>> |

## Reinstate Services at the office

Elective

Guidance: Determine if the following steps apply to reinstate services at a physical office location.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **When** | **Who** | **Procedure** | **Step** | **Action** | **Who/**  **completed** |
| Once access and services at the office are available | <<Indicate role>> |  | 1 | Ensure all insurance needs have been covered, and that any additional insurance needs are considered. |  |
|  |  |  | 2 | Ensure that the usability of the office will still meet the needs of <<Organisation Name>>. |  |
|  |  |  | 3 | Assess the technology requirements to reinstate services at the office. |  |
|  |  |  | 4 | Assess furniture and fixture needs for the reinstatement of services in the office. |  |
|  |  |  | 5 | Ensure all health and safety requirements are in place. |  |
|  |  |  | 6 | Ensure all general offices services are in place. |  |
|  |  |  | 7 | Arrange for staff to return to the office. |  |

## Transition to business continuity plans for specifc issues

Elective

Guidance: this section provides examples of business continuity requirements for specific issues focused on the use of business support systems.

To re-establish the various business support systems, ensuring they are available and set up for use, activate the relevant business continuity plan, as specifed in the following chapters of this plan:

* Payroll
* Finance payments
* Email
* Network (including file and print) and remote access
* Phones – landlines
* Phones – mobile
* [Specialist application] and accounting systems.

### Business continuity plans by issue

Elective

Guidance: The following are some examples of organisational business process issues that may require short-term and long-term actions.

Consider whether these issues apply to your organisation and the necessary actions required to address business continuity.

Following a Business Impact Analysis, you may identity particular requirements that need to be included based on your organisation’s products, services and operations.

### Payroll

|  |  |  |  |
| --- | --- | --- | --- |
| **Core Business Functions** | **Characteristics of Interruption** | **Short Term (Up to 1 week)** | **Long Term ( More than 1 Week)** |
| **Payroll** | No access to building and no access to payroll system. | Arrange with [Bank] to process the same payments as the previous pay run. | Technology Advisor to arrange for payroll software and backups to be installed on a standalone PC. |
|  | Access to building but no access to payroll system. | Arrange with [Bank] to process the same payments as the previous pay run. | Technology Advisor to arrange for payroll software and backups to be installed on an alternative PC. |

### Finance payments

|  |  |  |  |
| --- | --- | --- | --- |
| **Core Business Functions** | **Characteristics of Interruption** | **Short Term (Up to 1 week)** | **Long Term ( More than 1 Week)** |
| **Finance payment** | No access to building and no access to [specialist application] and accounting systems. | Contact the producers of the significant projects and agree on payment requirements.  Arrange with [Bank] to process the payments. | Technology Advisor to arrange for [specialist and financial system] backups to be restored to a new server. |
|  | Access to building but no access to [specialist application] and accounting systems. | Contact the producers of the significant projects and agree on payment requirements.  Arrange with [Bank] to process the payments. | Technology Advisor to arrange for [specialist and financial system] backups to be restored to a new/repaired server. |

### Email

|  |  |  |  |
| --- | --- | --- | --- |
| **Core Business Functions** | **Characteristics of Interruption** | **Short Term (Up to 1 week)** | **Long Term ( More than 1 Week)** |
| ***Delivery of email*** | No access to building and Exchange server down. | * Technology Advisor will advise ISP. * Accounts will be setup for accessing email via webmail if the outage is extended. | * Collect backup tapes from off site storage. * Purchase/borrow server and rebuild. |
| ***Delivery of email*** | Access to building but Exchange server down. | * Technology Advisor will advise ISP. * Accounts will be setup for accessing email via webmail if the outage is extended. | * Collect backup tapes from off site storage. * May choose to “POP” email direct to laptops and PCs if delays getting replacement server running. * Repair existing, or purchase new server and rebuild. |
| ***Delivery of email*** | No access to building and firewall down -Email, VPN and Internet access unavailable. | * Technology Advisor will advise ISP. * Accounts will be setup for accessing email via webmail if the outage is extended. * Use laptops and PCs at home to access webmail accounts. | * If firewall destroyed, purchase and set up new firewall. * The implementation of the new firewall will have to wait until access to the building has been restored. |
| ***Delivery of email*** | Access to building but firewall down -Email, VPN and Internet access unavailable. | Technology Advisor will contact IT suppliers to install a temporary replacement firewall. | Repair existing or purchase new firewall and rebuild. |

### Network (including file & print) & remote access

|  |  |  |  |
| --- | --- | --- | --- |
| **Core Business Functions** | **Characteristics of Interruption** | **Short Term (Up to 1 week)** | **Long Term ( More than 1 Week)** |
| ***Email, accounting, funding & marketing information & general business applications*** | No access to building but servers operating. | * Technology Advisor to contact all IT suppliers. IT provide support remotely. * IT assist staff to access network remotely. | * Work offsite. * Temporary IT systems will be arranged at business recovery office if necessary. |
| ***Accounting, funding & marketing information & general business applications*** | * No access to building and Terminal Server not running. * There will be no access to shared drives, print services or [specialist and financial system] / [specialist application]. | * Technology Advisor to contact all IT suppliers. IT provide support remotely. * If the server cannot be fixed remotely there is no access to shared drives, print services or [specialist and financial system] / [specialist application]. | * The implementation or repair of the Terminal Server will have to wait until access to the building has been restored. * If all servers are running except the Terminal Server, at some stage a decision may be made to purchase and setup all the services at the business recovery office. |
| ***Accounting,funding and marketing information and general business applications*** | * Access to building but Terminal Server not running. * There will be no access to shared drives, print services or [specialist and financial system] / [specialist application]. | * Technology Advisor to contact IT suppliers to attempt repair of server. * Until the server can be fixed or replaced, configure the standby server (Porkpie) to run terminal services (gives access to [specialist and financial system] / [specialist application]), printing and backups. Limited shared drives may be made available. * IT assist staff to access the new configuration. | * If the Terminal Server is unrepairable, purchase a new server. * Implement the new/repaired Terminal Server. |

### Phones – landlines

|  |  |  |  |
| --- | --- | --- | --- |
| **Core Business Functions** | **Characteristics of Interruption** | **Short Term (Up to 1 week)** | **Long Term ( More than 1 Week)** |
| ***Phone calls*** | No access to building and phone system down. | * Contact telco and phone system suppliers. * Phone system suppliers to attempt remote repair but unlikely, as phone system must be running for remote access to work. * Arrange for the telco to setup diversions of main number (includes all DDIs) to a mobile phone or to a landline in the business recovery office. | * If phone system is unrepairable, purchase a new system. * The implementation or repair of the phone system will have to wait until access to the building has been restored. * Arrange for telco to remove phone diversions. |
|  | Access to building but phone system down | * Contact telco and phone system suppliers. * Phone system suppliers to attempt repair. * In the meantime, calls will automatically divert to the red emergency analogue phone at reception. * Install a temporary phone system. | * If phone system is unrepairable, purchase a new system. * Implement the new/repaired phone system. * Arrange for telco to remove the phone diversions. |

### Phones – mobile

|  |  |  |  |
| --- | --- | --- | --- |
| **Core Business Functions** | **Characteristics of Interruption** | **Short Term (Up to 1 week)** | **Long Term ( More than 1 Week)** |
| ***Phone calls*** | No access to building and mobile phones not working | * Contact mobile telco to access extent of issue. * Arrange for the mobile telco to setup diversions of the mobile numbers to business recovery office or to staff home phones if possible. | * Contact telco to access extent of issue. * Arrange for mobile telco to remove the diversions. |
|  | Access to building but mobile phones not working | * Contact telco to access extent of issue. * Arrange for the mobile telco to setup diversions of the mobile numbers to the business recovery office; or to staff home phones if this is not possible. | * Contact telco to access extent of issue. * Arrange for mobile telco to remove the diversions. |

### [Specialist application] and accounting systems

|  |  |  |  |
| --- | --- | --- | --- |
| **Core Business Functions** | **Characteristics of Interruption** | **Short Term (Up to 1 week)** | **Long Term ( More than 1 Week)** |
| ***Accounting, funding & marketing information*** | No access to the building and [specialist and financial system] / [specialist application] not working | * Technology Advisor to contact IT suppliers. * IT suppliers to attempt remote repair of SQL server. | * If SQL server is unrepairable, purchase a new server. * Collect backup tapes from off site storage. * The repair of the SQL Server will have to wait until access to the building has been restored or [specialist and financial system] / [specialist application] will be implemented on a new/borrowed server in the business recovery office. |
|  | Access to the building, but [specialist and financial system] / [specialist application] not working | Technology Advisor to contact IT suppliers to attempt repair of SQL Server. | * If SQL server is unrepairable, purchase a new server. * Implement [specialist & financial system] / [specialist application] on the new/repaired SQL Server. |

# Emergency delegations list

Mandatory

Guidance: Outline the organisation’s delegation of expenditure that may be required in the event the business continuity plan requires enactment. This may refer to the organisation’s delegation policy.

Delegations will be sought to ensure emergency expenditure can be approved by:

|  |  |
| --- | --- |
| **Position** | **Level of Authority** |
| CEO | [Indicate amount] |
| Deputy CEO | [Indicate amount] |
| Business Affairs manager | [Indicate amount] |
| Accountant | [Indicate amount] |

# Testing the plan

Mandatory

Guidance: It is key that elements of the business continuity plan are tested to ensure that the plan works for the organisations needs. Some examples of test approaches include walkthroughs and simulations of the scenarios within the business continuity plan.

1. **Walkthroughs**

Team members verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses.

This test provides the opportunity to review a plan with a larger group of people, allowing the Business Continuity Manager role to draw upon a correspondingly increased pool of knowledge and experiences. Staff should be familiar with procedures, equipment, and offsite facilities (if required).

1. **Simulations**

A disaster is simulated so normal operations will not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation and other necessary utilities should be thoroughly tested in a simulation test.

Validated checklists can provide a reasonable level of assurance for many of these scenarios. Analyse the output of the previous tests carefully before the proposed simulation to ensure the lessons learned during the previous phases are applied.

# Contact lists

Mandatory

## Staff call tree

The flow chart below describes who is responsible for calling who, in the event of an emergency and to keep in contact with staff.

**Note**: It is important that these contact details are kept updated. Also ensure you store these phone numbers in your phone contact list.

| **Contact** | **Work** | **Mobile** | **Home** |
| --- | --- | --- | --- |
| Business Continuity Manager |  |  |  |
| Technical Representative |  |  |  |
| Senior Leadership Team Representative |  |  |  |

## Staff, supplier, and stakeholder contact lists

Guidance: Determine how contact lists for staff, suppliers and other stakeholders will be maintained and where backup copies of these lists will be securely stored.

For example:

The contact lists are kept in a single spreadsheet on the I drive, in the following location:

* I:\\_RECEPTION\_\\_Contact Lists

The file is called:

* Contact Details.xls

<<Insert role>> is responsible for maintaining copies of these contact lists from the respective IT systems.

# Version Information and Changes

Mandatory

Any changes, edits and updates made to the Business Continuity Plan will be recorded here.

It is the responsibility of the Business Continuity Manager to ensure that all existing copies of the Business Continuity Plan are up to date. Whenever there is an update to the Business Continuity Plan, <<Organisation Name>> requires that the version number be updated to indicate this.

| **Version** | **Change Description** | **Reviewed By** | **Approved By** | **Date** |
| --- | --- | --- | --- | --- |
| 1.0 | … | … | … | … |
|  |  |  |  |  |
|  |  |  |  |  |

# Appendix A – Business Impact Analysis approach

Mandatory

Guidance: A Business Impact Analysis (BIA) allows an organisation to understand the resource contingencies required to continue operations in the event of a disruption.

Using the guidelines set out below, document the critical activities and requirements to deliver your key products and services under the relevant headings:

1. List your organisation’s key products and services, in priority order, which if disrupted would have the greatest impact on your organisation:

|  |
| --- |
| **Key Products and Services** |
| 1. |
| 2. |
| 3. |
| 4. |
| 5. |
| 6. |

2. Consider impacts on your organisation’s ability to meet its goals and objectives and the impact on stakeholders such as customers. Refer to the risk assessment (section 3) to identify events that could have an impact on the organisation. Document what the impact would be for:

* + First 24 hours
  + 24 – 48 hours
  + One week
  + Two weeks.

3. Identify the maximum length of time that your organisation can manage a disruption to each of the key products and services without it threatening your organisation’s finances or reputation.

4.You should now set a point in time at which each of your key products or services would need to be resumed in the event of a disruption (this may also link with your Disaster Recovery Plan).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Considerations for increasing your organisation’s resilience** | | | | |
| * **PEOPLE** | * **PREMISES** | * **PROCESSES** | * **PROVIDERS** | **PROFILE** |
| **Key Staff:**  What staff do you require to carry out your key functions? | **Buildings:**  What locations do your department’s key functions operate from? (Primary site, alternative premises) | **IT:**  What IT is essential to carry out your key functions? | **Reciprocal Arrangements:**  Do you have any reciprocal agreements with other organisations? | **Reputation:**  Who are your key stakeholders? |
| **Skills / Expertise / Training:**  What skills / level of expertise is required to undertake key functions? | **Facilities:**  What facilities are essential to carry out your key functions? | **Documentation:**  What documentation / records are essential to carry out your key functions, and how are these stored? | **Contractors / External Providers:**  Do you tender key services out to another organisation? If so - to whom and for what? | **Legal Considerations:** What are your legal, statutory and regulatory requirements? |
| **Minimum Staffing Levels:**  What is the minimum staffing level with which you could provide some sort of service? | **Equipment / Resources:**  What equipment / resources are required to carry out your key functions? | **Systems and Communications:**  What systems and means of communication are required to carry out your key functions? | **Suppliers:**  Who are your priority suppliers and whom do you depend on to undertake your key functions? | **Vulnerable Groups:**  Which vulnerable groups might be affected if your organisation fails to carry out key functions? |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **BIA Proforma for your organisation** | | | | |
| * **PEOPLE** | * **PREMISES** | * **PROCESSES** | * **PROVIDERS** | * **PROFILE** |
| **Key Staff:** | **Buildings:** | **IT:** | **Reciprocal Arrangements:** | **Reputation:** |
| **Skills / Expertise / Training:** | **Facilities:** | **Documentation:** | **Contractors / External Providers:** | **Legal Considerations:** |
| **Minimum Staffing Levels:** | **Workstations:** | **Systems and Communications:** | **Suppliers:** | **Vulnerable Groups:** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Considerations for increasing your organisation’s resilience** | | | | |
| * **PEOPLE** | * **PREMISES** | * **PROCESSES** | * **PROVIDERS** | * **PROFILE** |
| **Key Staff:**  Can staff be contacted out of hours?  Could extra capacity be built into your staffing to assist you in coping during an incident? | **Buildings:**  Could you operate from more than one premise?  Could you relocate operations in the event of a premise being lost or if access to the premise was denied? | **IT:**  Is data backed-up and are back-ups kept off site?  Do you have any disaster recovery arrangements in place? | **Reciprocal Arrangements:**  Do you have agreements with other organisations regarding staffing, use of facilities in the event of an incident? | **Reputational Damage:**  How could reputational damage to your organisation be reduced?  How could you provide information to staff and stakeholders in an emergency (e.g. press release)? |
| **Skills / Expertise / Training:**  Could staff be trained in other roles?  Could other members of staff undertake other non-specialist roles, in the event of an incident? | **Facilities:**  Are any of your facilities multi-purpose?  Are alternative facilities available in the event of an incident? | **Documentation:**  Is essential documentation stored securely (e.g., fire proof safe, backed-up)?  Do you keep copies of essential documentation elsewhere? | **Contractors / External Providers:**  Do you know of alternative contractors or are you reliant on a single contractor?  Do your contractors have contingency plans in place?  Could contractors be contacted in the event of an incident? | **Legal Considerations:**  Do you have systems to log decisions; actions; and costs, in the event of an incident? |
| **Minimum Staffing Levels:**  What is the minimal staffing level required to continue to deliver your key functions at an acceptable level?  What measures could be taken to minimise impacts of staff shortfalls? | **Equipment / Resources:**  Could alternative equipment / resources be acquired in the event of an incident / disruption?  Could key equipment be replicated or do manual procedures exist? | **Systems and Communications:**  Are your systems flexible?  Do you have alternative systems in place (manual processes)?  What alternative means of communication exist? | **Suppliers:**  Do you know of suitable alternative suppliers?  Could key suppliers be contacted in an emergency? | **Vulnerable Groups:**  How could vulnerable groups be contacted / accommodated in the event of an incident? |

**Using Business Impact Analysis to build a plan:**

|  |  |  |
| --- | --- | --- |
|  | **BIA**  Identifies your requirements for continuing your key functions. | **BCP**  Documents how your requirements identified in the BIA can be achieved. |
| **PEOPLE** | * Key Staff * Key Skills * Expertise / competence required * Minimum staffing levels required to continue / recover key functions. | * Notification / invocation procedure / protocol * Management structure for dealing with an incident * Information and advice to staff (response procedures) * Key staff / contact list (including out of hours details) * Multi skill training in key areas * Reciprocal Arrangements to cover staff short falls * Home working * Staff welfare issues. |
| **PREMISES** | * Key facilities * Key Equipment * Key Resources * Specialist Equipment * Security / restrictions * Alternative sites * Alternative facilities. | * Loss / damage assessment * Site security * Relocation arrangements / protocol * Inventories of equipment/ resources and details of how to recover these * Salvage, site clearance and cleaning arrangements. |
| **PROCESSES** | * Key processes * Critical periods * Key IT systems / applications * Key documentation / data * Record keeping requirements * Key communication requirements. | * Action cards for recovery of key processes * Checklists * Copies / Back-ups / safe storage (recovery procedure) * Contingency procurement arrangements * Documented manual procedures * Data recovery procedures. |
| **PROVIDERS** | * Key dependencies (supply and receipt) * Key suppliers * Key contractors / service providers / suppliers * Reciprocal arrangements in place with other organisations. | * Contact details for key providers / contractors / suppliers / support services * Alternative suppliers (required for key functions) * Alternative providers (required for key functions) * Alternative contractors (required for key functions) * Resilience capability of suppliers / provider / contractors to business disruption * Third party business continuity arrangements. |
| **PROFILE** | * Key stakeholders * Legal / statutory / regulatory requirements * Vulnerable groups. | * Communication strategy / plan / procedures * Stakeholder liaison (regulator, clients, unions) * Media liaison * Public information / advice * Notification of at risk groups / alternative care arrangements. |