Aviva Risk Management Solutions

Incident Management and Business Continuity Plan

AVIVA

Business Continuity

Business continuity planning should be regarded as a priority for any business, from SMEs to large organisations. Every year, businesses across the UK face unplanned and unwanted events that may challenge their survival.

Why Business Continuity matters

No matter the cause, the businesses that successfully recover from disruption are those that have:

- Assessed the likely impact of significant events on their business
- Planned their response in advance
- Tested the effectiveness of their plan and revised it where needed
- Invested time, thought and, where necessary, money, to manage risk

Some consequences of disruptions cannot be covered by insurance, such as reputational risk, loss of market share and staff retention. However, a well-developed plan can enable an organisation to identify and minimise the impact of these risks.

Definitions

(Source of Definitions: The Business Continuity Institute)

Incident
Situation that might be, or could lead to, a disruption, loss, emergency, or crisis.

Business Continuity
The capability of an organisation to continue delivery of products or services, at acceptable predefined levels following a disruptive incident.

Business Continuity Management
A holistic management process that identifies potential threats to an organisation, and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience, with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating opportunities.

Business Continuity Plan
Documented procedures that guide an organisation to respond, recover, resume and restore to a pre-defined level of operation following a disruption.

What does a good Business Continuity Plan (BCP) look like?

A good Continuity Plan must have a number of aspects included. One of the main being it should deal with Incident Management, what an organisation must do immediately to deal with an incident, and minimise its impact, and Recovery of the Business, or Business Continuity. This is the part where the resources and activity are prioritised in a Plan to help the business achieve recovery of its customer base and expected market position.

A good BCP will also have buy-in at the top level in an organisation, and budget to put in place Incident Management and Business Continuity/ Recovery features, where required and economical.

The Team(s) put in place, and the persons allocated roles in Incident Management and Business Continuity, should have adequate training to be able to undertake the tasks the roles require, time allowed to do so, and have deputies trained and in place, in case needed.

The BCP will consider six key business elements. Premises, People, Machinery, Suppliers, Data and Communications, and the impact on the organisation, should any of these be unavailable for a period of time due to an incident.

Testing and maintaining the BCP is another key aspect. Ensuring the Plan is assessed on a regular basis, and whenever there is a fundamental change to the business. As well as that regular maintenance, Testing a BCP to ensure it will work as expected when needed will throw up any weaknesses or areas for improvement, whether that's sub-contracting levels, replacing a Team member who has left the business, changing detail around IT and data back-ups, or a number of other aspects.

Incident Management & Business Continuity Plan

> **Note:**
> **The detail in the Blue Areas in this document is purely an example, hints of what a business may need to include, and should be amended, or added to, as necessary.**

Company Name	
Plan Owner	

Plan Objectives

Date of issue	

Date of next review

Plan storage

Incident Management

Definition: Incident

A Situation that might be, or could lead to, a disruption, loss, emergency, or crisis.
(Source: The Business Continuity Institute)

Invoking the Plan

Any member of the Incident Management Team can invoke the Incident Management Plan, should an Incident occur, that would appear to at least have the prospect of interrupting the business' ability to operate, and provide its usual products or services to its customers.

Assembling the Team

The person invoking the Plan will contact the members of the Incident Management Team, and have them meet at one of the Crisis Control Rooms detailed below. Any further staff members required to join the Incident Management Team will be contacted by the IMT using Contact List appended to this Plan.

Grab Bag/ Battle Box

It is strongly advised that all businesses put together a Grab Bag or Battle Box, larger businesses more than one, at separate locations at the premises. One of these should be collected and brought to the Crisis Control Room, by a member of the IMT, as they respond to Plan invocation.

Contents of a Grab Bag or Battle Box should be anything the IMT would need in event of a serious incident/ emergency.

- Site Plan
- Business Continuity Plan
- High Visibility Jackets/ Vests
- Camera
- Torches
- Batteries/ Charging Leads
- Contact Lists
- Payment Facilities, Card, Cheque Book, Bank Details, etc
- Mobile phone and SIM card
- Headed Paper and pens
- Face masks and hand sanitiser

And anything else, business, industry or site specific, that the business would need to assist dealing with an incident.

Crisis Control Room(s)

Location	Contact Detail	Resources Available

Incident Management

The Incident Management Team

The IMT needs to be populated with a variety of persons/ roles within the business, both Managerial and Operational, all with adequate training to perform their individual role, in the event of an incident/ emergency. Deputies should be included and trained in case needed.

Role	Responsibilities	Person responsible	Contact details

Incident Management

Incident Management Checklist

Task	Owner	Completed

Business Recovery Plan

When looking at Recovery of the business there are Six key areas to consider. **People, Premises, Data, Communications, Machinery & Equipment** and **Suppliers.** The detail included is what can, or needs to be done, to reduce the impact of an incident, and get an efficient recovery to a pre-defined position.

People

Looking at Key personnel and skills availability

Recovery Plan	Person Responsible	Status

Business Recovery Plan

Premises

Looking at the impact to the business Premises, and activity to recover.

Recovery Plan	Person Responsible	Status

Business Recovery Plan

Data and Information Security

Looking at the security of data, especially sensitive data, support, and the backing-up and storage of data etc.

Recovery Plan	Person Responsible	Status

Business Recovery Plan

Communications

Looking at activity to maintain a level of communications with staff, Customers, suppliers, Insurers and other stakeholders.

Recovery Plan	Person Responsible	Status

Business Recovery Plan

Machinery, Equipment and Utilities

Looking at alternatives, and essential activity, should an incident mean machinery etc on site is put out of action.

Recovery Plan	Person Responsible	Status

Business Recovery Plan

Suppliers

Looking at the impact on the business of loss of supply from key supplier(s), and the work-arounds possible to safeguard ability to provide usual level of products and/or services to Customers.

Recovery Plan	Person Responsible	Status

Business Recovery Plan

Exercising and Maintaining the Business Continuity Plan

Regular Plan maintenance is essential, at least six-monthly. This should ensure that the Plan is up to date, Team members correct, Contact details accurate, any Recovery Assistance relied on in the Plan is still viable. Checking the detail within the BCP for accuracy. This maintenance should also be done whenever there is a fundamental change in the way the business operates. New machinery, different product range, new location, change in Incident Management Team Leadership or roles.

Testing or Exercising the BCP as follows:

Type	Process	Participants

Exercise Log

Date	Type of Exercise	Report completed	Plan revised

Business Recovery Plan

Priorities and Recovery Strategy

For each Priority, there should be a Maximum Tolerable Period of Disruption assessed and a Recovery Time Objective set.

Maximum Tolerable Period of Disruption: The time it would take for adverse impacts, which might arise as a result of not providing a product or service, to become unacceptable.

Recovery Time Objective: The period of time following an incident within which a product or activity must be resumed, or resources must be recovered

In short, the period of time following which customers would go elsewhere, and a strategy to recover key areas, before that happens. *(Source of definitions: The Business Continuity Institute.)*

Planning recovery to get to a necessary level of service, or provision of product, to Customers, is key. If what a business does for its clients is not available, the longer that situation continues the more likely the customers will need to go elsewhere. Assessing that Maximum Tolerable Period of Disruption, and setting a strategy to recover services before that time (Recovery Time Objective) arrives is essential.

The priorities could be large contracts, dominant product lines, an essential machine or production line, trained staff for key roles, any number of key aspects to a business. Recovering or replacing these before loss of custom is where assessment of alternatives to do so, is key.

For example, a key CNC Machine will take 6 months to obtain from manufacturer in Italy. Clearly customers will need what a business normally produces for them a lot sooner than 6 months time, to supply to their own clients, and will likely look to another business to provide it quite quickly. If a business can arrange sub-contracting of production within a reasonable period they are far more likely to retain that customer, whilst awaiting the CNC Machine from manufacturer.

Example:

Priority	Recovery Time Objective	Strategy to Achieve RTO

Business Recovery Plan

Any activity in the Recovery Strategy must be agreed or contracted so it can be relied upon, for example an agreement with a sub-contractor to take on production. All must be **tested** to ensure they would ensure intended service levels, by the time required.

Assessing these priorities will give a business the option to Act Now, and put in place, a second production line for example, to build in resilience. Plan to Act, and arrange something that can be activated in the event of an emergency, sub-contracting at agreed levels, or a set number of desks in a Disaster Recovery facility, for example. The third option being to Provide Alternatives, assessing what the business would need to do. This may be where a number of easily obtained alternatives exist, or the cost of putting in place mitigating features now, would out-weigh the possible financial impact of an incident.

ASSESS	PLAN	TEST

Contact Lists

Staff contacts

Name	Position	Phone	Email

Emergency Contact List

	Company	Contact Name	Phone	Email

Contact Lists

Critical Suppliers Contact List

Company	Supply	Contact Name	Phone	Email

Key Customers Contact List

Company	Contact Name	Phone	Email

Other Stakeholders

Stakeholder	Company	Contact Name	Phone	Email

Sources:
The Business Continuity Institute

Please Note
This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise and Aviva recommend that you obtain specific advice relevant to the circumstances.

Further Information
Aviva Risk Management Solutions   https://www.aviva.co.uk/risksolutions/