

Business Continuity & Disaster Recovery

The world we live in is an ever changing world. You need to be prepared. A well planned and tested Business Continuity Plan (BCP) will ensure that your business is prepared. Every business can experience a serious incident that can prevent it from continuing normal business operations, and this can happen at any time. The scope to these incidents can range from a flood or explosion to a serious computer malfunction or information security incident. Every business has the potential to recover from such incidents in the minimum amount of time possible provided they have a tried and tested Business Continuity Plan. This recovery process requires careful preparation and planning.

ASDF can simplify and support the development and testing of a well structured and coherent plan which will enable you to recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts normal business operations. The objective is to ensure that your business survives major interruption.

ASDF Defines Business Continuity and Disaster Recovery:

The differences between "Disaster Recovery Plans" and "Business Continuity Plans" are not clear-cut in actual usage. Different companies and people sometimes use these terms differently and, at times, interchangeably.

Technically the "Business Continuity Plan" refers to the means by which loss of business may be avoided. Business recovery planning (BRP) is a superset of DRP and is recovery of all aspects of your business following a loss from a disaster. The "Business Continuity Plan" defines the business requirements for continuity of operations. It defines the business requirements for a "Disaster Recovery Plan".

Technically, the "Disaster Recovery Plan" deals with the restoration of computer systems with all attendant software and connections to full functionality under a variety of damaging or interfering external conditions. Disaster recovery planning (DRP) refers to IT operations and the recovery of IT following a loss from a disaster.

In daily practice Business Continuity often refers to disaster recovery from a business point-of-view, or dealing with simple daily issues, such as a failed disk, failed server or DB, possibly a bad communications line. It is often referred to as the measure of lost time in an application, possibly a mission critical application.

In daily practice Disaster Recovery often refers to major disruption, such as a flooded building, fire or earthquake disrupting an entire installation. The issue of Business Continuity certainly arises when Disaster Recovery is required.

Below is a summary of the various phases of a Business Continuity Plan which ASDF professionals adhere to:

1 - Initiating the project

It is imperative that the BCP process is initiated. This involves undertaking a range of project initiation and project organization activities.

The first phase of the Business Continuity Plan includes a couple of steps that need to be adhered to before the development of the plan:

- Project Initiation Activities
- Project Organization

2 - Assessing Business Risk and Impact of Potential Emergencies (Business Impact Analysis & B.I.A)

The second phase involves reviewing the different types of emergencies that can arise and assessing the risks to the various business processes

A key part of the BCP Process is the assessment of the potential risks to the business which could result from disasters or emergency situations. It is necessary to consider all the possible incidents and the impact each may have on a company's ability to continue to deliver its normal business services.

It is necessary to assess the criticality of a company's business processes and to determine the impact and consequences of loss of service or a reduction in normal customer service levels.

Of particular importance when considering business risks and the impact of potential emergencies is the disruption to, and availability of, IT services and communications. The level of dependency that most organizations have on IT and communications systems and the nature of customer services which are often on a 24/7 basis, has meant that it is essential that organizations are able to keep their IT networks and communications systems operational at all times. The

following areas will be covered:

- Emergency Incident Assessment
- Business Risk Assessment
- IT and Communications
- Other Existing Disaster Recovery Procedures
- Premises Issues

3 - Preparing for a Possible Emergency

The third phase involves the identification of back-up and recovery strategies to mitigate the effects of an emergency.

It is necessary to take steps to minimize the effects of potential emergencies. The underlying objective of this phase is to identify ways of preventing an emergency from turning into a disaster for the organization. The focus is on business activities that are key to the continued viability of the business. The following areas will be dealt with extensively:

- Back-up and Recovery Strategies
- Key BCP Personnel and Supplies
- Key Documents and Procedures

4 - Disaster Recovery Phase

The fourth phase involves the development of procedures to be followed by a Disaster Recovery team where human life is at risk.

A critical part of handling any serious emergency situation is in the management of the Disaster Recovery Phase. By definition, the Disaster Recovery Phase is likely to involve, to a significant degree, external emergency services. The priority during this phase is the safety and well being of the employees and other involved persons, the minimization of the emergency itself, the removal or minimization of the threat of further injury or damage and the re-establishment of external services such as power, communications, water etc. A significant task during this phase is also the completion of Damage Assessment Forms.

In addition to the emergency services, the Disaster Recovery Phase may involve different personnel depending upon the type of emergency and a Disaster Recovery Team will be nominated according to the requirements of each specific crisis. The following key areas will be covered:

- Handling the Emergency Situation
- Notification and Reporting During Disaster Recovery Phase

5 - Business Recovery Phase

The fifth phase is the main phase from a business perspective and involves developing detailed procedures for the recovery of the business.

The Business Recovery Phase will either follow directly on from the Disaster Recovery Phase or will be directly initiated after a serious emergency incident affecting normal business operations which does not need a Disaster Recovery Phase.

The Business Recovery Phase involves the restoration of normal business operations after an unexpected event which has disrupted all or part of the business process. From a business perspective, this is the most critical phase of the whole BCP. The efficiency and effectiveness of the procedures contained within this section could have a direct bearing on the organization's ability to survive the emergency. The following areas will be covered:

- Managing the Business Recovery Phase
- Business Recovery Activities

6 - Testing Business Recovery Process

The sixth phase involves the detailed testing of the Business Recovery Phase set in reasonably authentic emergency situations.

The ability of the BCP to be effective in emergency situations can only be assessed if rigorous testing is carried out in realistic conditions. The BCP testing phase contains important verification activities which should enable the plan to stand up to most disrupted events.

The BCP should be tested within a realistic environment which means simulating conditions which would be applicable in an actual emergency. It is also important that the tests should be carried out by the persons who would be responsible for those activities in a crisis. The following areas will be covered:

- Planning the Tests
- Conducting the Tests

7 - Training Staff in the Business Recovery Process

The seventh phase covers the training of all employees in the procedures to effectively manage the business recovery process.

All staff should be trained in the business recovery process. This is particularly important when the procedures are significantly different from those pertaining to normal operations. This training may be integrated with the training phase or handled separately.

The training should be carefully planned and delivered on a structured basis. The training should be assessed to verify that it has achieved its objectives and is relevant for the procedures involved. The following areas will be covered:

- Managing the Training Process
- Assessing the Training

8 - Keeping the Plan Up-To-Date

The BCP must be regarded as a dynamic document and be kept up to date to reflect all changes to business processes and employee structure.

Products and services change and also their method of delivery. The increase in technological based processes over the past ten years, and particularly within the last five, have significantly increased the level of dependency upon the availability of systems and information for the business to function effectively. These changes are likely to continue and probably the only certainty is that the pace of change will continue to increase. It is necessary for the BCP to keep pace with these changes in order for it to be of use in the event of a disruptive emergency. This phase deals with updating the plan and the managed process which should be applied to this updating activity. The following area is covered:

- Maintaining the BCP