

Business Impact Analysis

DEFINITION- Business impact analysis (BIA) is an essential component of an organisation's [business continuance](#) plan; it includes an exploratory component to reveal any vulnerabilities, and a planning component to develop strategies for minimising risk. The result of analysis is a business impact analysis report, which describes the potential risks specific to the organisation studied. One of the basic assumptions behind BIA is that every component of the organisation is reliant upon the continued functioning of every other component, but that some are more crucial than others and require a greater allocation of funds in the wake of a disaster. For example, a business may be able to continue more or less normally if the cafeteria has to close, but would come to a complete halt if the information system crashes.

As part of a [disaster recovery plan](#), BIA is likely to identify costs linked to failures, such as loss of cash flow, replacement of equipment, salaries paid to catch up with a backlog of work, loss of profits, and so on. A BIA report quantifies the importance of business components and suggests appropriate fund allocation for measures to protect them. The possibilities of failures are likely to be assessed in terms of their impacts on safety, finances, marketing, legal compliance, and quality assurance. Where possible, impact is expressed monetarily for purposes of comparison. For example, a business may spend three times as much on marketing in the wake of a disaster to rebuild customer confidence.



associated with the priorities for the business functions,

between business units and dependencies with key external suppliers and agencies, minimum resources required to perform the activities, and vital records needed to support the activities.



In our experience in assisting clients to implement their BC and DR plans, the [Business Impact Analysis](#) phase is often the most challenging phase to implement. Here, GMH will assist clients to analyse potential business impact catalogue of threats; so as to define recovery and resumption of critical recovery timeframes, dependencies

Description

It is often said that the first step in a sensible business continuity process is to consider the potential impacts of each type of problem. The argument is that you cannot properly plan for a disaster if you have little idea of the likely impacts on your business/organisation of the different scenarios.

This is undoubtedly the case, yet it is surprising how many organisations bypass this initial step in the continuity process.

WHAT IS BIA?

Business impact analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various (unavailability) events or incidents

It is common for the impacts resulting from other types of incident (such as breach of loss of data integrity or confidentiality) to be simultaneously explored, but this need not be the case. However, there are certainly advantages to undertaking a comprehensive and wider focused business impact and risk analysis exercise.

The business impact analysis is intended to help you understand the degree of potential loss (and various other unwanted effects) which could occur. This will cover not just direct financial loss, but other issues, such as reputational damage, regulatory effects, etc.

Business Continuance

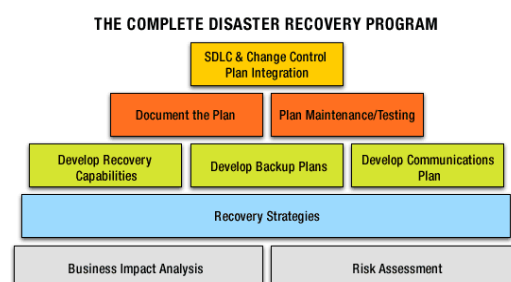
DEFINITION- Business continuance (sometimes referred to as *business continuity*) describes the processes and procedures an organisation puts in place to ensure that essential functions can continue during and after a disaster. Business continuance planning seeks to prevent interruption of mission-critical services, and to re-establish full functioning as swiftly and smoothly as possible.

Although business continuance is important for any enterprise, it may not be practical for any but the largest to maintain full functioning throughout a disaster crisis. According to many experts, the first step in business continuity planning is deciding which of the organisation's functions are essential, and apportioning the available budget accordingly. Once the crucial components are identified, [failover](#) mechanisms can be put in place. New technologies, such as [disk mirroring](#) over the Internet, make it feasible for an organisation to maintain up-to-date copies of data in geographically dispersed locations, so that data access can continue uninterrupted if one location is disabled.

According to a recent Gartner Group document, a business continuance plan should include: a [disaster recovery plan](#), which specifies an organisation's planned strategies for post-failure procedures; a *business resumption plan*, which specifies a means of maintaining essential services at the crisis location; a *business recovery plan*, which specifies a means of recovering business functions at an alternate location; and a *contingency plan*, which specifies a means of dealing with external events that can seriously impact the organisation. Business continuance has become an increasingly common area of concern since the September 2001 World Trade Centre disaster, in which an unforeseen incident created a sudden and severe threat to crucial functions for a number of companies.

Disaster Recovery Plan

DEFINITION- A disaster recovery plan (DRP) - sometimes referred to as a business continuity plan (BCP) or business process contingency plan (BPCP) - describes how an organisation is to deal with potential disasters. Just as a disaster is an event that makes the continuation of normal functions impossible, a disaster recovery plan consists of the precautions taken so that the effects of a disaster will be minimised and the organisation will be able to either maintain or quickly resume mission-critical functions. Typically, disaster recovery planning involves an analysis of business processes and continuity needs; it may also include a significant focus on disaster prevention.



[Ask your questions about disaster recovery at ITKnowledgeExchange.com](http://ITKnowledgeExchange.com)

Disaster recovery is becoming an increasingly important aspect of enterprise computing. As devices, systems, and networks become ever more complex, there are simply more things that can go wrong. As a consequence, recovery plans have also become more complex. According to Jon William Toigo (the author of *Disaster Recovery Planning*).

For example, fifteen or twenty years ago if there was a threat to systems from a fire, a disaster recovery plan might consist of powering down the [mainframe](#) and other computers before the sprinkler system came on, disassembling components, and subsequently drying circuit boards in the parking lot with a hair dryer. Current enterprise systems tend to be too large and complicated for such simple and hands-on approaches, however, and interruption of service or loss of data can have serious financial impact, whether directly or through loss of customer confidence.

Appropriate plans vary from one enterprise to another, depending on variables such as the type of business, the processes involved, and the level of security needed. Disaster recovery planning may be developed within an organisation or purchased as a software application or a service. It is not unusual for an enterprise to spend 25% of its information technology budget on disaster recovery.

Nevertheless, the consensus within the DR industry is that most enterprises are still ill-prepared for a disaster. According to the Disaster Recovery site, "Despite the number of very public disasters since 9/11, still only about 50 percent of companies report having a disaster recovery plan. Of those that do, nearly half have never tested their plan, which is tantamount to not having one at all."

Business Continuity Management Consulting Services

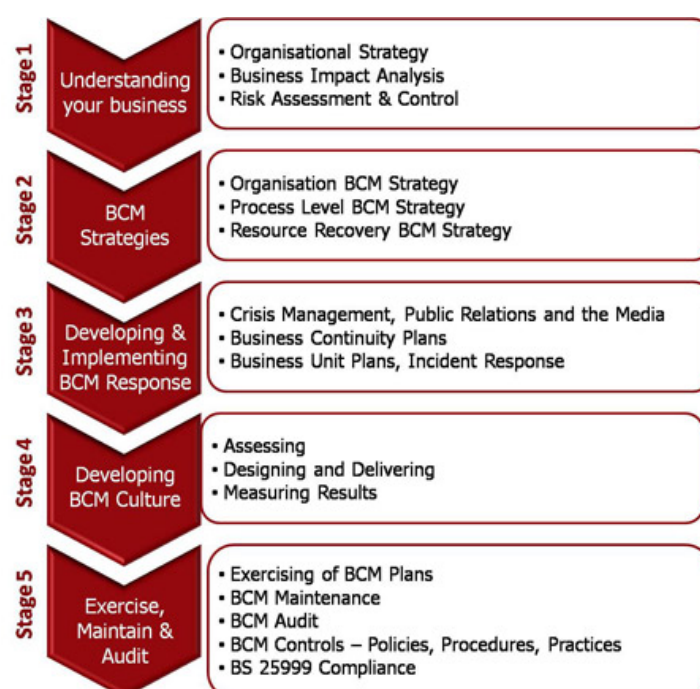
CBA Consulting Business Continuity Management offers a range of consulting services that assist organisations in implementing Business Continuity Programmes that safeguard the interests of their key stakeholders, by managing to build resilience and the capability for effective responses to potential impacts that may threaten the organisation.

These services are aimed to assist organisations to effectively develop and implement a BCM policy, BCM strategies and BCM Plans.

BCM Programme Implementation Support

Our approach to BCM implementation support is based on the principles of the British Standard Institute's Publicly Available Specification – BS 25999.

The implementation approach involves the following phases:



Business Impact Analysis

The Business Impact Analysis (BIA) is the foundation upon which the whole BCM process is built. BIA services assist organisations to identify, quantify and qualify the business impacts of a loss, interruption or disruption of business processes on an organisation and provide the data from which appropriate continuity strategies can be determined.

The BIA identifies mission-critical areas and business processes that are crucial to the survival of business and then analyses financial and operational impact to business if these processes are interrupted as a result of a disaster. Overall, the BIA raises senior management's awareness of undesirable consequences and potential operational risk and helps to justify the need for a business continuity plan.

The BIA helps organisations to:

- Obtain an understanding of the organisation's most critical objectives, the priority of each and the timeframes for resumption of the unscheduled interruption.
- Inform a management decision on Maximum Tolerable Outage for each function
- Provide the resource information from which an appropriate recovery strategy can be determined / recommended
- Outline dependencies that exist both internally and externally to achieve critical objectives

Information Security Management Consulting Services

Information Security Consulting services provide a structured, practical, results-oriented approach that assists organisations in all aspects of developing, implementing or managing an Information Security Management System (ISMS).

Covering the full lifecycle of Information Security Management, our consulting services can include creating policies and standards, achieving ISO 27001 compliance. CBA Consulting can also support your organisation through full or partial outsourcing of your ISMS.

With extensive experience in developing security management systems in both private and public sector organisations. Some of the key activities we're able to address include:

- Reviews of existing policies and procedures against industry best practice
- Risk assessment and change control procedures
- Definition of security policies and standards
- Achieving compliance with ISO 27001
- Security incident reporting processes and response strategy
- Building a security culture within an organisation through awareness and training
- Monitoring internal compliance to security policies
- Maintaining corporate compliance to regulatory or legislative requirements
- Recruitment, training and mentoring of ISMS staff
- Outsourcing of your ISMS