Loss Prevention Standards

Business Impact Analysis

Introduction

The Business Continuity Institute, and the International Standard ISO 22301, define Business Impact Analysis (BIA) as follows:

"*The process of analysing business functions and the effect that a business disruption may have upon them.*"

It also considers the Business Continuity requirements resulting.

To understand the effect of a disruption the business needs to understand:

- What are the key business and service objectives of the organisation?
- What are the key products and services required to meet these objectives?
- What are the processes required to provide these products and services?
- What resources and activities are required to provide these processes?
- Effect over time. When do these objectives need to be met by?

The BIA looks at each product, service, process and activity within the organisation, understands its significance, and determines the impact over time if it were disrupted.

It will document interdependencies and single source of supply/single point of failure. Once this is understood an estimate of impact over time can be made, and as a result a **Maximum Tolerable Period of Disruption** can be assessed, and as a result a **Recovery Time Objective**.

This will lead to an organisation having decisions to assess whether to improve situations they find unacceptable:

- **Accept:** if cost of measures to mitigate the risk, or impact, outweigh the likely effect, a business might decide its uneconomic to do anything. The occurrence could be so unlikely, or the impact is assessed as likely to be minimal, the business would accept the situation as it is
- **Improve:** the BIA could identify a significant single point of failure; a machine, or supplier, etc., that if lost would see a dramatic impact on business immediately. The business could decide to improve the situation immediately, putting in place duplication, etc.
- **Plan:** the impact of a disruption could be considerable, but rather than spend on improvements now, the business may decide to formalise arrangements that would go into operation immediately an incident causing a disruption occurs, to minimise its impact. Sub-contracting or reciprocal arrangements, generator supplier, duplicate raw material supplier, etc.

Definitions

These definitions are stated in the [Business Continuity Institute's Good Practice Guidelines](#), and the International Standard.

Risk
The effect of uncertainty on objectives.

Threat
A potential cause of an unwanted incident, which can result in harm to individuals, the environment or the community.

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

Maximum Tolerable Period of Disruption (MTPD)
The time it would take for adverse impacts, which might arise as a result of not providing a product or service, or performing an activity, to become unacceptable (sometimes also referred to as Maximum Acceptable Outage).

AVIVA

Recovery Time Objective (RTO)
The period of time following an incident within which a product or service must be resumed, an activity must be resumed, or resources recovered.

What are the Stages of Business Impact Analysis?

Stage 1: Initial BIA

The initial BIA is undertaken to set scope and framework for the BIAs to follow. It should recommend on products and services that can be grouped together to simplify information collection and analysis. It will also need to agree the impacts to be considered, for example, financial and reputational. It should consider the impact over time of failing to deliver products and services, and as a result estimate a Maximum Tolerable Period of Disruption.

It should consider the processes that deliver the products and services, and the owner of each of these processes. Additionally, it should also list any products, services, processes or activities excluded from the BIA, and the reasons for this.

This would then provide a framework for the BIAs to follow.

Stage 2: Products and Services BIA

The purpose of a products and services BIA is to identify and prioritise products and services and determine the organisation's business continuity requirements at a strategic level.

It should detail the potential impact on products or services, of any fundamental changes in the business. It should analyse the products and services and document the impact on the business of not being able to deliver them.

It should then follow on to fine tune the Maximum Tolerable Period of Disruption for each product or service or set group thereof.

Stage 3: Processes BIA

The purpose of the processes BIA is to determine the process or processes required for the delivery of the prioritised products and services.

This part of the BIA can be left out by less process driven businesses, who can move straight from the products and services to the activities BIA.

The dependencies for the processes that deliver the prioritised products and services must be identified. This could be across many departments, inter-department or organisation-wide, and dependencies need to be documented.

Identify how disruption to processes would impact the ability to provide the prioritised products and services and ascertain the point at which the impact becomes unacceptable (MTPD). Consideration must also be given to lead times for restoring processes, and in the recovery process after an incident, capacity and backlogs and their impact.

The result of this analysis should be setting of relevant Recovery Time Objective(s) for the processes.

Stage 4: Activities BIA

The purpose of the activities BIA is to identify and prioritise the activities which deliver the most urgent products and services, and determine the resources required for the continuity of these activities.

The activity BIA is where an organisation would gather and assess information relating to the resources required to support the activities which support achieving the organisation's strategic objectives.

This BIA looks at the people, information and data, buildings and work environment, IT systems, transport, finance, partners and sub-contractors, and suppliers, needed to undertake the activities that support the processes.

The Recovery Time Objective, and how the business will achieve recovery at that point is the main focus of the activity BIA, and consideration needs to be given to other activities that may need to be done to support that, such as clearing backlogs.

The outcomes from this BIA would be the MTPD and RTO for each activity, which will give a clear timetable, and from this a list of the resources required to achieve recovery by the RTO.

Recovery Point Objective needs to be considered and set at this stage. This is the point at which the IT and information used by an activity must be restored to enable the activity to operate on resumption.

Stage 5: Risk and Threat Assessment

The final part of the BIA is a threat assessment and recognising the threats to the day to day operation of the business. A lot of businesses have a Risk Register, which can be of great assistance in this part of the process.

List the known threats to the business, both internal and external. Then estimate the impact level of the threat should it turn into an incident. Following on from that, assess the likelihood of that threat becoming an actual incident. To assist in this process a Likelihood vs Severity table can be produced, similar to the example below:

Likelihood

Highly Likely	🟨	🟨	🟥	🟥	🟥
	🟨	🟨	🟥	🟥	🟥
Possible	🟩	🟨	🟨	🟥	🟥
	🟩	🟩	🟨	🟨	🟨
Very Unlikely	🟩	🟩	🟩	🟨	🟨
	Minimal		*Medium*		*Catastrophic*

<div align="center">Severity</div>

Using a table like the above, plot the assessed threats to the business, to help prioritise those with greatest impact on the business. Threats can be from a number of areas; fire, smoke, contamination, flood, supplier, pandemic, industry, weather, loss of power, denial of access, terrorism, product recall, reputation, etc.

Threat analysis is the process of evaluating threats and uses risk assessment techniques to identify unacceptable concentrations of risk to activity, and single points of failure.

Once threats are identified and plotted, acting on them to move them away from the top right corner (worst cases) towards acceptability is the next step.

When Should Business Impact be Completed?

The process needs buy-in at the top level, and once the first full BIA is completed it should be reviewed at least annually if the business remains unchanged. Any change to the business, key staff, process change, new machinery, change of supplier, etc., would mean changing and updating the BIA immediately. Changes, however small, could lead to difficulties in protecting against, or recovering from, an incident causing a disruption.

Additional Information

Further risk management information can be obtained from Aviva Risk Management Solutions

Please Note
This document contains general information and guidance and is not and should not be relied on as specific advice. 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. AVIVA accepts no responsibility or liability towards any person who may rely upon this document.