Loss prevention standards

Business Impact Analysis

Disruption impacts each business function differently. To understand which impacts are most significant, a business impact analysis should be completed to look at the potential risks of disruption across the business.

Business Impact Analysis

Introduction

The Business Continuity Institute and the International Standard ISO 22301 define Business Impact Analysis (BIA) as: '*The process of analysing business functions and the effect that a business disruption may have upon them*'.

It also considers the aligned Business Continuity requirements.

Key Questions

To understand the effect of disruption, the organisation needs to understand:

- What are the key business and service objectives of the business?
- 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?
- When do these objectives need to be met by?

The Business Options

The BIA looks at each product, service, process and activity within the organisation to understand its significance and determine the impact over time if it were disrupted. It also documents interdependencies and any single sources of supply or point of failure. Once this is understood an estimate of impact over time can be made, a Maximum Tolerable Period of Disruption can be assessed, and a Recovery Time Objective then defined.

The organisation then needs to assess whether to improve situations they find unacceptable. Decisions can align to the following options:

- Accept – if an occurrence is unlikely, its impact minimal, or the cost of measures to mitigate the risk outweighs its impact, the business might decide not to do anything, and will accept the situation as it is
- Improve – the BIA could identify a significant single point of failure; a machine, supplier, etc. that if lost would see a dramatic impact on business. The business could decide to improve the situation immediately, putting in duplication, etc.
- Plan – the impact of disruption could be considerable, but rather than spend on improvements now, the business may decide to formalise arrangements that would go into operation after a disruption, to minimise its impact., such as sub-contracting or reciprocal arrangements, generator supplier, duplicate raw material supplier, etc.

The Business Impact Analysis

Stage 1: Initial BIA

Purpose: To set the scope and framework for the BIA to follow.

Process:

1. Recommend products and services that can be grouped together to simplify information collection and analysis
2. Agree the impacts to be considered, for example financial and reputational
3. Consider the impact over time of failing to deliver products and services and estimate a Maximum Tolerable Period of Disruption
4. Consider the processes, and owners of these processes, that deliver products and services
5. List any products, services, processes or activities excluded from the BIA, and the reasons for this

Stage 2: Products and Services BIA

Purpose: To identify and prioritise products and services and determine the organisation's business continuity requirements at a strategic level.

Process:

1. Detail the potential impact of any fundamental changes in the business on its products or services
2. Analyse products and services and document the impact of not being able to deliver them
3. Fine-tune the Maximum Tolerable Period of Disruption for each product or service

Stage 3: Processes BIA

Purpose: To determine the process or processes required to deliver the prioritised products and services. This stage can be skipped by less process-driven businesses, who can move straight from the products and services to the activities BIA.

Process:

1. Identify and document the dependencies for the processes that deliver the prioritised products and services. This could be across many departments, inter-department or organisation-wide
2. Identify how disruption to processes would impact the ability to provide the prioritised products and services and ascertain the point at which this impact becomes unacceptable (MTPD)
3. Consider lead times for restoring processes, the recovery process after an incident, capacity and backlogs
4. Set relevant Recovery Time Objectives for the above processes

Stage 4: Activities BIA

Purpose: To identify and prioritise the activities that deliver the most urgent products and services, and determine the resources required for the continuity of these activities.

Process:

1. Analyse the people, information and data, buildings and work environment, IT systems, transport, finance, partners and sub-contractors, and suppliers needed for the activities that support the processes
2. The Recovery Time Objective, and how the business will achieve recovery at that point is the main focus of the Activity BIA, so consider other activities that may need to be undertaken to support this, such as clearing backlogs
3. Determine the Maximum Tolerable Period of Disruption and Recovery Time Objective for each activity, which will provide a clear timetable, and from this a list of resources required to achieve recovery
4. Consider and set the Recovery Point Objective – 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

Purpose: To recognise 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. Threat analysis is the evaluation of threats and the use of risk assessment techniques to identify unacceptable concentrations to risk activity and single points of failure.

Process:

1. List the known threats to the business, both internal and external
2. Estimate the impact level of a threat, should it turn into an incident
3. Assess the likelihood of that threat becoming an actual incident
4. Plot assessed threats to the business on a Likelihood vs. Severity table (see table below) to help prioritise those with greatest impact on the business. Threats can be from a number of areas such as fire, smoke, contamination, flood, supplier, pandemic, industry, weather, loss of power, denial of access, terrorism, product recall, reputation, etc.
5. Once threats are identified and plotted, acting on them to move them away from the right-hand corner (worst cases) towards acceptability is the next step

Likelihood

Highly Likely					
Possible					
Very Unlikely					
	Minimal		Medium		Catastrophic

Severity

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).

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.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services at preferential rates via our network of Specialist Partners.

For more information please visit:

Aviva Risk Management Solutions – Specialist Partners

Additional Information

Relevant Loss Prevention Standards include:

- Business Continuity
- Business Continuity Plan – Testing and Maintenance
- Business Interruption – Indemnity Period and Maximum Indemnity Period
- Business Interruption – Committed Costs

To find out more, please visit Aviva Risk Management Solutions or speak to one of our advisors.

Email us at riskadvice@aviva.com or call 0345 366 6666.*

*Calls may be recorded and/or monitored for our joint protection.

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.

17/08/21 V1.1