Loss prevention standards

Business Continuity

Unexpected interruption to business can be caused by a range of events. Organisations that recover successfully will already have a detailed Business Continuity Plan and recovery procedures in place.

Business Continuity

Introduction

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. It can also be used as a differentiator when competing for business. The following steps outline an approach that can be adapted for use by most organisations.

Setting Policy

It's crucial to create a policy that sets out the scope and intentions of your business continuity programme. It should be short, clear and concise and include roles and responsibilities, along with a set of minimum agreed standards. The complexity of the policy will depend on the size and complexity of your organisation. Setting the policy at a senior level will help embed business continuity in day-to-day activities and your organisation's culture.

External Influences

Every business will have a number of external influences that can affect its mission-critical process and functions, such as government departments, regulators, competitors, trade bodies and pressure groups. It is important to identify these at an early stage and take their influence into account.

Appointing a Business Continuity Team

Developing and implementing a plan is best completed as a team. The business continuity team should be made up of managers and staff, along with deputies to cover for illness and holidays, who are able to work effectively in challenging circumstances. Between them, the team should have a good understanding of business operations and processes, legal, finance, HR, IT, premises, publicity, health and safety, and fire and security precautions.

When choosing team members, remember that you will need individuals outside the team to manage the parts of the business that have not been affected by the disruption. A co-ordinator of appropriate seniority and authority should be appointed to lead the team and to decide when it is necessary to invoke the Business Continuity Plan.

It's important to ensure that the team has a common understanding of the company's primary business objectives at the outset. This can avoid disputes over priorities later in the planning proess.

Creating a Business Continuity Plan (BCP)

Once a business continuity team has been appointed, they can follow this five-step process to create a BCP:

Step 1: Service Levels

First, the business must understand its desired level of service – what it aims to deliver to its customers and stakeholders every day – and its minimum acceptable service – the essential service it must provide to avoid immediate permanent loss of custom and to fulfil its primary contractual obligations.

The plan will detail how the organisation will get from their minimum service level to their desired service level in the shortest possible time.

The 'Maximum Tolerable Period of Disruption' is 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 (Business Continuity Institute).

Step 2: Risk Analysis

Risk analysis is the process of recognising the risks the business faces (risk mapping), understanding what the consequences of these risks occurring would be (business impact analysis) and putting protection and mitigation measures in place (risk reduction).

The Horizon Scan 2015 Survey Report, published by the Business Continuity Institute (BCI) in conjunction with the British Standards Institution, listed the top threats to organisations as:

1. Cyber attacks
2. Unplanned IT and communications outages
3. Data breach
4. Interruption to utility supply
5. Supply chain disruption
6. Security incidents
7. Adverse weather
8. Human illness
9. Fire
10. Acts of terrorism

Other risks that businesses may face include:

- Environmental impact including flood and pollution
- Theft and vandalism
- Industrial relations
- Pandemics

The business should consider what effects these risks would have on:

- Each premises, in whole or in part
- IT equipment and data
- Machinery and plant
- Vehicles used by the business
- Public utility supplies, such as electricity, gas, water and telecommunications
- Premises of a major supplier

It is also useful to assess the supply chain for weaknesses at this stage. The assessment should clarify who the key suppliers are, and what the effect would be on the business should any supplier suffer a major incident and supply be interrupted. It may also involve arranging duplicate or alternative suppliers.

Understanding available capacity within the organisation or group should also be a consideration when determining how to mitigate and respond to an incident.

Step 3: Emergency Action Planning

The Emergency Action Plan should be implemented by the business continuity team in the immediate aftermath of any incident. Decide how the business would deal with issues such as:

- Personnel
- Immediate damage limitation
- Site security
- Damage assessment and salvage
- Invoking emergency arrangements such as IT and workplace recovery contracts
- Maintaining an incident recovery log to record details of actions, losses identified and expenses incurred
- Communication with the media, stakeholders, suppliers and important customers
- Deciding which members of the team will be responsible for which actions

Remember to consider where the team will assemble, as key premises may be damaged or access be denied following an incident.

Step 4: Business Recovery Planning

The business continuity team should prepare a business recovery procedure, stating how the business would deal with issues such as:

- Implementing alternative working practices, such as utilising available capacity within the group or subcontracting
- Identifying and equipping temporary premises, perhaps using second-hand machinery so the business can relocate
- Monitoring the progress of the reinstatement work at the damaged premises, ensuring it progresses as planned and that equipment is ordered at the appropriate time
- Maintaining contact with customers and trying to win back any lost business as capacity improves
- Keeping the disaster/incident recovery log up to date by recording details of actions, losses identified and expenses incurred

Step 5: Testing and Maintaining the BCP

The BCP plan needs to be tested to ensure it is robust and operates as planned. Testing can also highlight any gaps in the plan, increase awareness within the organisation, and develop teamwork within the business continuity team.

Testing can take the form of a desktop exercise simulating a particular incident, a discussion-based exercise, or a full live test to check on how the response would work – all valuable ways of assessing both the plan and the organisation's resilience. All areas of the organisation, including IT, HR, production, sales, and transport should be involved in testing to demonstrate how an incident in one area could impact on other sections of the company.

It's recommended that testing is undertaken at least annually, and whenever there are any changes to the organisation, such as amendments to operations, premises, machinery and processes, changes to key suppliers, mergers and acquisitions. Even small changes to the business can have a big impact on the business continuity plan's operation and effectiveness.

For further guidance, see the Aviva Loss Prevention Standard Business Continuity Plan – Testing and Maintenance.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services via our network of Specialist Partners who are reputable companies offering agreed discounted rates for Aviva customers.

For more information please visit:

Aviva Risk Management Solutions – Specialist Partners

Useful Sources and Links:

- Continuity Central
- Disaster Recovery Journal
- Disaster Resource Guide

Additional Information

Relevant Aviva Loss Prevention Standards include:

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

To find out more, talk to our advisors or vist Aviva Risk Management Solutions.

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

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

Appendix - Definitions

Definitions

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 they might cause, and which provides a framework for building organisational resilience with an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

Business Continuity Policy
Intentions and direction of an organisation as formally expressed by senior management.

Business Continuity Plan
Documented procedures that guide organisations to respond, recover, and restore to a predefined level of operation following disruption.

Business Continuity Management Programme
Ongoing management and governance process, supported by senior management, to implement and maintain business continuity management.

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.

06/10/20 V1.3

Aviva Insurance Limited, Registered in Scotland Number 2116. Registered Office: Pitheavlis, Perth PH2 0NH.
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.