Business Continuity – Solutions Design and Implementation

Effective business continuity planning enables organisations to resume operations swiftly following a disruptive event.

This Loss Prevention Standard is part of a series focused on business continuity and emphasises the critical role of analysing and managing the risks that could threaten recovery from a disruptive event.

Version: 1.0
Date: 28th April 2026

Business Continuity – Solutions Design and Implementation

Introduction

An important step in the Business Continuity lifecycle involves analysing known risks and determining an appropriate risk management approach.

This includes reviewing previously identified risks and highlighting any gaps and single points of failure that could threaten recovery following a disruptive event. Any intolerable risks should be documented and managed under a risk framework.

Compiling actions to mitigate the future impact of potential disruptive events will help increase the resilience of your business.

Note: This Loss Prevention Standard relates to business continuity planning and is focussed on business interruption loss prevention/mitigation and related risk management guidance. It is not intended to address liability exposures. The presumption is that any regulatory requirements relating to business continuity have, or will be, met.

Understanding the Risks

Completing a Solutions Design and Implementation review enables an organisation to convert identified business continuity strategies into practical measures that reduce disruption, safeguard critical activities, and support timely recovery following a disruptive incident.

Without this process, business continuity planning may prove ineffective when required, potentially resulting in prolonged downtime, reputational harm, and increased financial loss, as well as the risk of regulatory non-compliance that may lead to breaches of legal or contractual obligations and potential fines or sanctions.

Business Impact Analysis

A Business Impact Analysis (BIA) can significantly reduce these impacts and strengthen an organisation's ability to recover quickly by examining key business functions and assessing the effect that a disruption may have upon them. Guidance on completing the BIA is provided in the Aviva Loss Prevention Standard **Business Continuity - Business Impact Analysis and Risk Assessment**.

After an organisation has carried out the BIA, the identified risks should be reviewed, with particular emphasis placed on highlighting gaps in recovery capabilities and single points of failure.

Examples of such gaps of points of failure include, but are not limited to:

- A critical product or service taking longer to recover than previously expected, leading to a loss in turnover.
- Losing a critical product or service that creates a greater impact than expected, increasing the amount of time required for recovery.
- Components or activities seen as less important playing a significant role in critical products or services across the organisation, leading to unexpected downtime.
- Highly skilled and experienced employees leaving the organisation without documenting their knowledge or involvement in delivering critical products or services.
- A supplier or third party, that plays a key role in delivering critical products or services, going out of business without any suitable alternatives.

Following this review, organisational representatives should agree on the appropriate mitigation and management actions required to address these risks, which will in turn increase resiliency and lessen the potential impact of disruptive events.

Understanding where the risks lie, and what impact they could have, is critical to the development of a mature business continuity approach.

Managing the Risks

When dealing with any risk, there are a number of alternative approaches an organisation can adopt, depending on the nature of the risk, the chance of the risk occurring (the likelihood), the disruption or effect the risk could have if materialised (the impact), and the amount and type of risk an organisation is willing to take (their risk appetite).

Of these approaches, there are five likely options:

Duplicate

Establish secondary or backup arrangements for critical products and services. This could be a standby server, secondary production line, alternative warehouse site, or multiple factory locations. If the primary production site is disrupted, operations can shift to the backup arrangements.

This approach generally requires the largest investment of time and resources but can result in the quickest recovery time.

Mitigate

Working from identified risks, implement proactive steps to limit the likelihood or impact before disruption occurs. This could be establishing alternative arrangements for replacement machinery or suppliers, exploring outsourcing or external contracting, or establishing a succession planning programme across the organisation.

This is potentially the most effective approach but requires management buy-in and the largest time investment.

Plan

Build reactive recovery scenarios based on the most likely risks, including outlining the actions to take in the event of disruption. This could include detailing contingency plans for the primary production site, failover steps to take during an IT outage, or formalised outsourcing agreements with third party suppliers.

This approach assumes the organisation has sufficient contingency and recovery planning in place to successfully weather disruptions and therefore requires less resource investment but carries greater levels of risk.

Transfer

Engage with third parties to transfer the risk to another organisation or entity. This could involve purchasing insurance to cover business interruption following a disruption or including indemnification clauses in contracts.

This is a common approach but requires a level of regular investment and management buy-in.

Leave Alone

Choose to accept the risk as tolerable and determine that no action is required. Doing nothing is a choice in itself and the organisation may determine the cost of managing the risk is less tolerable than the impact of the risk occurring.

This approach requires the least resources but also carries with it the greatest level of risk.

Each risk management approach should be documented, along with the reasoning, justification, and responsible parties.

Key Actions

- Review previously identified risks, either gathered through Business Impact Analysis or risk management activity.
- After analysing these risks, highlight and document any gaps identified in areas of recovery capability or single points of failure.
- For each identified gap or single point of failure, determine a risk management approach: duplicate, mitigate, plan, transfer, or leave alone.
- Document each approach and assign a responsible owner.
- Review each identified risk and management approach at least once annually or following organisational change.

Checklist

A generic **Solutions Design and Implementation Checklist** is presented in Appendix 1 which can be tailored to your own organisation.

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.

- Business Continuity - **Horizonscan**

For more information please visit: Aviva Risk Management Solutions – Specialist Partners

Sources and Useful Links

- The Business Continuity Institute

Note: Whilst UK standards and legislation are referenced in this document, other international standards and legislation should be referenced where applicable.

Additional Information

Relevant Aviva Loss Prevention Standards include:

- **Business Continuity Planning**
- **Business Continuity – Roles & Responsibilities**
- **Business Continuity – Incident Management Plan**
- **Business Continuity – Communications Plan**
- **Business Continuity – Business Impact Analysis and Risk Assessment**
- **Business Continuity – Policy**

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.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Appendix 1 - Solutions Design Checklist

Location	
Date	
Completed by (name and signature)	

	Checklist	Y/N	Comments
1.	Have the risks previously identified through the Business Impact Analysis been reviewed?		
2.	Have any document gaps related to recovery or single points of failure been highlighted?		
3.	Has a risk management approach (duplicate, mitigate, plan, transfer, or leave alone) been determined for each gap or single point of failure?		
4.	Has each approach been documented and assigned to a responsible owner?		
5.	Has a review schedule been formalised? **Note:** Each risk should be reviewed at least once annually or following organisational change.		
6.	Additional Comments:		

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.

28th April 2026

Version 1.0

ARMSGI4092026