

# Business Continuity – Step 3: Communications Plan

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

This Loss Prevention Standard is part of a series focussed on business continuity and emphasizes the critical role of communications planning to help ensure a timely and effective response and recovery.

# Business Continuity – Step 3: Communications Plan

## Introduction

Unplanned disruptions, such as those caused by fires, escape of water incidents, etc., can have serious consequences for businesses.

A well-managed Communications Plan can however significantly reduce the impact and enhance the organisation's ability to recover quickly.

This document explores the key aspects of communications planning and outlines the essential activities required, providing guidance on those key actions.



**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

Loss events can occur without warning. Having clear and concise communication plans can help manage the immediate disruptive event help reduce the impact and scale of any business interruption losses.

Common risks/exposures/issues include, but are not limited to:

- **Reputational Damage.** Poor communication during a disruptive event, including a perceived lack of empathy or failure to acknowledge the situation, can damage relationships with customers, suppliers, and other stakeholders.
- **Financial Loss.** Uncoordinated responses can result in delayed or ill-informed decision-making, leading to significantly higher losses.
- **Extended Downtime.** Fractured messaging can result in miscommunication and delays when dealing with internal or external recovery teams.
- **Regulatory Non-Compliance.** Many industries are highly regulated and require organisations comply with strict legal and regulatory communication requirements relating to disruptions.
- **Reduced Recovery Capability.** If critical teams or individuals are not kept up to date during a disruptive event, this could lead to further delays and greater overall impact.

## Managing the Risks

### Incident Management Plan

An Incident Management Plan helps ensure disruptive incidents or events requiring intervention are accurately assessed and the appropriate response is determined.

Refer to the Aviva Loss Prevention Standard **Business Continuity - Incident Management Plan** for further guidance.

### Communications Plan

A Communications Plan is essential for ensuring timely, clear and considered communication with interested parties and stakeholders.

The plan should assign the following tasks to an individual role or team:

- Advising senior management on the communications strategy.
- Developing communication materials intended for internal and external audiences.
- Monitoring and liaising with the media.
- Engaging with social media.
- Updating the website with relevant information and guidance.
- Reviewing and logging incoming communications.
- Briefing the spokesperson(s) before any external statement.

Effective communication plans should:

- Identify the information likely to be required from interested parties, such as customers, suppliers, and employees.
- Include pre-written templates for statements addressing the above information.
- Provide general questions and answers that apply to most situations.
- Contain a pre-written description of the company's background and operations for public distribution.
- Develop a dedicated external webpage for communicating with staff during emergency situations.

Consideration should be given to the following:

**Centrally Agreed.** All communications issued during a disruptive incident should be approved and managed by a named team or individual, previously determined and agreed.

- Communication procedures should be documented, including how to coordinate and implement throughout the organisation.
- These procedures should also include any additional approvals or authorisations required.

**Messaging Strategy.** Establish a consistent tone for communications to ensure messages are accurate, relevant and clearly communicated.

- Language should be appropriate for the target audience, and communications should be honest and transparent, whilst respecting necessary confidentiality.

**Holding Messages.** Holding messages should be prepared for various potential scenarios relevant to your organization. Examples include loss of premises, product recall, offensive actions by an employee, lawsuits, workplace injuries, customer service issues, or system outages.

- These may need to be sent at very short notice. To prepare for this, internal and external holding messages should be prepared in readiness.
- These templates should also outline any approvals or authorisations required before messages are sent.

**Organisational Alignment.** All communications should align with the organisation's beliefs, culture, and values.

- The media may extract information directly from an organisation's website or social media at any time, particularly during a disruptive event. This content should not contradict any communications sent during a disruptive event.

**Contact Details.** Both internal and external contact details should be stored securely and be readily available during a disruptive event.

## Key Actions

- Allocate specific communication responsibilities to named teams or roles.
- Set a messaging strategy and agree the tone for communications.
- Determine what information would be required during a disruption and prepare templates for potential scenarios.
- Create internal and external holding messages and agree what level of disruption will activate different holding messages.
- Store all necessary internal and external contact details in easily accessible and secure locations.

## Appendices

A generic Communications Plan Checklist is presented in Appendix 1 which can be tailored to your own organisation.

Example Holding messages are provided within Appendix 2.

## 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 - Seven Steps to Business Continuity**
- **Business Continuity - Step 1: Roles & Responsibilities**
- **Business Continuity - Step 2: Incident Management Plan**
- **Business Continuity - Step 4: Business Impact Analysis and Risk Assessment**
- **Business Continuity - Step 5: Solutions Design and Implementation**
- **Business Continuity - Step 6: Policy**
- **Business Continuity - Step 7: Test and Exercise Plan**
- **Supply Chain Risk Management**

To find out more, please visit [Aviva Risk Management Solutions](#) or speak to one of our advisors.

Email us at [riskadvice@aviva.com](mailto: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 – Communications Plan Checklist

Location	
Date	
Completed by (name and signature)	

	Communication Plan	Y/N	Comments
1.	Has a named team or individual been pre-approved to issue communications during a disruptive incident?		
2.	Are communication procedures documented, and do they include coordination and implementation steps across the organisation?		
3.	Has a messaging strategy been established, ensuring consistent tone for all communications?		
4.	Has a holding message or template been created for internal interested parties?		
5.	Has a holding message or template been created for external interested parties?		
6.	Has authority been delegated to a specific person who approves communications?		
7.	Have websites and/or social media content been reviewed to ensure there is no contradiction of official communications during a disruptive event?		
8.	Has a separate external webpage or messaging group that can be used for staff communication in emergency situations been developed?		
9.	Are the contact details of internal and external interested parties stored securely?		
10.	Are internal and external contact details readily available during a disruptive event?		
11.	Additional Comments:		

## Internal Example Holding Message

We are aware of a disruptive incident currently affecting [specific area/process/system]. Our team is actively assessing the situation and working to resolve it as quickly as possible.

At this time, we do not have full details to share, but please be assured that updates will follow as soon as more information becomes available.

In the meantime:

- Continue normal operations where possible.
- Do not speculate or share unverified information externally.
- Direct any questions to [designated contact/team].

Thank you for your cooperation and understanding.

## External Example Holding Message

We are currently experiencing an unexpected issue affecting [specific service/product/operation]. Our team is actively investigating and working to resolve the situation as quickly as possible.

At this stage, we do not have full details to share, but please be assured we are prioritising this matter and will provide further updates as soon as more information becomes available.

In the meantime:

If you have urgent concerns, please contact [designated contact or support channel]. We appreciate your patience and understanding while we work to restore normal operations.

Thank you for your continued support.

## **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.

15<sup>th</sup> May 2026

Version 1.1

ARMSGI3592025

Aviva Insurance Limited, Registered in Scotland Number SC002116. Registered Office: Pitheavlis, Perth PH2 0NH.  
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.