Business Continuity – Step 2: Incident Management Plan

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

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

Version: 1.1
Date: 15th May 2026

Business Continuity – Step 2: Incident Management Plan

Introduction

Unplanned disruptions, such as fires or water escape incidents, can have serious consequences for businesses.

However, a well-managed incident response can significantly reduce the impact and enhance the organization's ability to recover quickly.

This document explores two key aspects of incident response and outlines the essential activities required, providing guidance on those key actions and timings.

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, but having clear incident management plans can help manage the immediate disruptive event, which can significantly reduce the impact and scale of business interruption losses.

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

- **Extended Downtime.** Without clear incident management planning, recovery may be delayed, leading to prolonged disruption.
- **Financial Loss.** Uncoordinated responses can result in slow or poor decision making and errors, and significantly higher losses.
- **Reduced Recovery Capability.** Delays may negatively impact recovery efforts, slowing down the return to normal operations.
- **Reputational Damage.** Delays in returning to normal operations can damage relationships with customers, suppliers and other stakeholders.
- **Regulatory Non-Compliance.** Many industries require documented and tested incident management plans. Poor management may lead to breaches of legal or regulatory obligations, resulting in fines or sanctions.

Managing the Risks

Definitions

- An **Incident** is defined as an event that can be, or could lead to, a disruption, loss, emergency or crisis.
- **Incident Management** is the immediate process by which an organization responds to and controls an incident using response procedures or plans.
- **Business Continuity** is the capability of an organization to continue the delivery of products and services within acceptable time frames at a predefined capacity during a disruption.
  Source (The Business Continuity Institute)

Incident Response Team

Ensure that key roles and responsibilities are allocated, and the team are appropriately trained at regular intervals.

Refer to the Aviva Loss Prevention Standard **Business Continuity – Step 1: Roles and Responsibilities** for further guidance.

Incident Management

Many incidents will be addressed promptly with little disruption and without the need to invoke an Incident Management Plan (IMP). However, in the event of more significant incident or event requiring intervention, the deployment of the incident management team, and wider business continuity teams, should follow a formal process, to include, but not limited to:

- Assessing if the site of the incident can be re-entered.
  - ✓ Establishing a command centre with appropriate resources, which may need to be remote if site access is not permitted.
- Assembling the Incident Management team.
- Assessing the incident and determining the response.
- Implementing the IMP and/or other recovery measures or plans.

Incident Management Plan

The IMP outlines how the business will respond to and manage loss events or disruptive incidents to minimise impact and ensure a prompt recovery. The plan should include:

Incident Classification

- The criteria for categorizing incidents (e.g. minor, major, critical) should be outlined.
- Impact thresholds for activating different levels of response.

Incident Detection and Reporting

- Procedures for identifying and reporting incidents.
- Channels for internal and external reporting.
- Initial notification protocols.

Incident Response Procedures

- Step-by-step actions for immediate containment, mitigation, and stabilization.
- Coordination with emergency services if applicable.

Resource Management

- Access to emergency resources (e.g. backup systems, alternate sites).
- Contact lists for vendors, partners, and support teams.

Documentation and Logging

- Incident log template.
- Requirements for recording actions, decisions, and communications.

Recovery and Restoration

- Procedures for restoring operations and services.
- Criteria for transitioning from response to recovery.
- Dependencies and prioritization of recovery activities.

Command Centre

One key aspect of Incident Management is designating a suitable command centre, particularly if the buildings or location would be affected by the incident and become unavailable. Suitable alternatives include:

- Another building at the location unaffected by the incident.
- Another branch, or location.
- Rented accommodation.
- A key customer or supplier premises.
- A director's house in the immediate aftermath.
- A hotel meeting room, etc.
- A remote platform, where connectivity is available.

The Command Centre will need adequate space, telecoms, internet connectivity, furniture, whiteboards and stationery.

Incident Management Plan Closure

An Incident Management Plan Closure Checklist is a tool used to ensure all necessary actions have been completed before formally closing an incident and transitioning back to normal operations. It helps validate that the response and recovery efforts were effective, documentation is complete, and any lessons learned are captured. Steps include:

Confirm Resolution

- All affected systems, services, and processes are fully restored.
- Recovery Time Objective (RTO) and Recovery Point Objective (RPO) have been met.
- Stakeholders confirm that operations are back to normal.

Conduct Post-Incident Review (PIR)

- PIR meeting scheduled and conducted with relevant stakeholders.
- Timeline of events is reviewed and validated.
- Key decisions and actions are evaluated.
- Successes and challenges are identified.

Document Lessons Learned

- Lessons learned are documented and approved.
- Recommendations for improvement are captured.
- Plans, procedures and related documents are updated.

Communicate Closure
- Final incident summary is prepared.
- Closure is communicated to all relevant stakeholders.
- Executive summary is shared with leadership.

Close Incident in Tracking System
- Incident ticket or record is updated with final status.
- All documentation (PIR, logs, communications) is attached.
- Closure date and responsible person details are recorded.

Initiate Corrective Actions
- Action items are assigned with owners and deadlines.
- Follow-up mechanisms are in place to track progress.
- Improvements are integrated into future response plans.

Archive Records
- All incident-related documents are securely stored.
- Records are accessible for audit, compliance, or training.

Key Actions

- Allocate roles and responsibilities and provide suitable training.
- Produce an Incident Management Plan.
- Provide regular training including staged incident response training.
- Compile a list of suitable command centres.
- Formalise incident closure review procedures.

Appendices

A generic **Incident Management Checklist** and **Incident Report and Decision Log** are presented in Appendices 1 and 2 which can be tailored to your own organization.

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 3: Communications 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 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 – Incident Management Checklist

	Activity	IMT Responsibilities	Owner	Completed
1	Start Action Log	'Commander' / IMT Leader Business Recovery Role		
2	Account for Staff (Whereabouts and Well-being)	Security / Site Safety / Personnel		
3	Dispatch Facilities Team Member to site	Command Centre		
4	Liaise with Emergency Services/ Identify Salvage	Emergency Services Liaison		
5	Identify and assess damage	Premises & Facilities Role		
6	Identify disrupted activities	'Commander'		
7	Secure damaged Building/ Asset	Security/Site Safety Premises & Facilities		
8	Review critical functions list in BCP	Business Recovery		
9	Identify appropriate recovery and response	'Commander'		
10	Decide on a course of action and allocate duties	Command Centre / 'commander'		
11	Communicate details to staff	Personnel (HR) - Employee & Agency Supplier		
12	Communicate details to stakeholders	Communications – Operational Customers		
13	Prepare media statement and communication strategy	Communications - Media		
14	Convene operational recovery teams	Command Centre		
15	Inform Insurance Company / Broker	Business Recovery		
16	Set up helpline / communicate updates	Communications - Media		
17	Ensure adequate resources to man phonelines	Personnel (HR)		
18	Availability of IT system and phones at relevant location/command centre.	IT		
19	Update the Board and other stakeholders	'Commander' / Communications - Media		
20	Contact Customers and Suppliers	Communications - Operational		
21	Arrange a Debrief	Command Centre		
22	Review Incident Management Plan and reassess priorities	'Commander' / Business Recovery		

Appendix 2 – Incident Report and Decision Log

This form should be used for recording initial incident details along with the proposed course of action. A fresh form may be required as the situation becomes clearer and at periodic intervals. In doing so, the organisation can learn from the incident and take actions to prevent re-occurrence.

Incident Report Form	
Completed by :	
Contact number:	
Date/Time of Incident:	
Date/Time Completed:	
Comments	
Incident Description: • Type of incident. • Cause (if known). • Location of incident.	
Initial assessment of impact to the business/ damage to physical assets: • People. • Buildings. • Plant and equipment. • Utilities. • Telecoms/ IT. • Environment. • Reputation. • Other.	
Proposed course of Action (refer to other reports to be completed): • Incident Response. • Safety of Personnel. • Salvage of Assets. • Communication. • Recovery.	
Anticipated period of interruption.	

Decision Log		
Date/Time	Issue	Action Taken

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.

15th May 2026

Version 1.1

ARMSGI3512025