

Business Continuity Plan

v5 October 2025



1. Introduction

The purpose of this Business Continuity Plan (BCP) is to ensure that Source can respond effectively to a disruption and continue its critical operations. This plan outlines the procedures and information necessary for the logistics business to recover and maintain operations in the event of an emergency.

2. Objectives

1. Ensure the safety and well-being of all employees
2. Maintain and restore critical business operations and services
3. Minimise the financial impact of disruptions
4. Preserve the company's reputation and customer trust

3. Scope

This BCP covers all operations, services, and locations of Source including but not limited to:

- Warehouse and storage facilities
- Transportation and delivery services
- Customer service and support
- IT and communication systems

4. Business Impact Analysis (BIA)

4.1 Identify Critical Functions

- **Order Processing:** Ensuring orders are received, processed, and dispatched
- **Inventory Management:** Maintaining accurate stock levels and ensuring availability
- **Transportation and Delivery:** Ensuring timely delivery of goods
- **Customer Support:** Addressing customer inquiries and issues
- **IT Systems:** Ensuring systems for tracking, communication, and operations are functional

4.2 Identify Critical Resources

- Personnel
- IT systems and infrastructure
- Communication systems
- Transportation fleet
- Warehousing

4.3 Determine Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)

- Order Processing: RTO - 4 hours, RPO - 30 minutes
- Inventory Management: RTO - 6 hours, RPO - 1 hour
- Transportation and Delivery: RTO - 4 hours, RPO - 1 hour
- Customer Support: RTO - 1 hour, RPO - 15 minutes
- IT Systems: RTO - 2 hours, RPO - 15 minutes



5. Risk Assessment

5.1 Potential Disruptions

- Natural disasters (e.g., floods, earthquakes)
- Cyber-attacks and data breaches
- Power outages
- Transportation accidents
- Pandemics and health crises
- Supply chain disruptions

5.2 Impact Analysis

- **Natural Disasters:** Could lead to physical damage to facilities and delays in operations.
- **Cyber-attacks:** Could result in data breaches, loss of critical data, and operational shutdowns.
- **Power Outages:** Could halt operations and communications.
- **Transportation Accidents:** Could cause delays and damage to goods.
- **Pandemics:** Could lead to workforce shortages and operational restrictions.
- **Supply Chain Disruptions:** Could affect the availability of goods and materials.

6. Mitigation Strategies

- **Natural Disasters:** Implement structural reinforcements, maintain insurance, and develop evacuation plans.
- **Cyber-attacks:** Enhance cybersecurity measures, conduct regular audits, and maintain data backups.
- **Power Outages:** Install backup generators and uninterruptible power supplies (UPS).
- **Transportation Accidents:** Implement stringent safety protocols and maintain insurance.
- **Pandemics:** Develop health and safety protocols, enable remote work, and ensure PPE availability.
- **Supply Chain Disruptions:** Diversify suppliers and maintain safety stock.



7. **Response and Recovery Strategies**

7.1 **Emergency Response Team (ERT)**

- **Team Lead:** Responsible for overall coordination and decision-making.
- **Communication Officer:** Handles internal and external communications.
- **IT Officer:** Ensures the functionality of IT systems.
- **Operations Officer:** Oversees the restoration of logistics operations.
- **Safety Officer:** Ensures the safety and well-being of employees.

7.2 **Communication Plan**

- **Internal Communication:** Use of emails, intranet, and emergency notification systems to keep employees informed.
- **External Communication:** Use of social media, company website, and press releases to inform customers and stakeholders.

7.3 **Recovery Steps**

1. **Assess the Situation:** Determine the extent of the disruption and its impact on operations.
2. **Activate the BCP:** Initiate the response plan and notify the Emergency Response Team.
3. **Ensure Safety:** Ensure the safety of all employees and stakeholders.
4. **Restore Critical Functions:** Prioritize and restore critical operations based on the RTO and RPO.
5. **Communicate:** Maintain clear communication with employees, customers, and stakeholders.
6. **Review and Improve:** After the situation is under control, conduct a post-incident review to identify areas for improvement.

8. **Testing and Maintenance**

- **Regular Testing:** Conduct regular drills and simulations to test the effectiveness of the BCP.
- **Plan Review:** Review and update the BCP annually or when significant changes occur in the business environment.
- **Training:** Provide regular training to employees on their roles and responsibilities during an emergency.

9. **Appendices**

- **Contact List:** Emergency contact information for all key personnel.
- **Resource List:** Inventory of critical resources and suppliers.
- **Maps and Diagrams:** Facility layouts and evacuation routes.

10. **Conclusion**

This Business Continuity Plan is designed to ensure that Source can quickly recover from disruptions and continue to provide critical services to its customers. Regular testing, training, and updates are essential to maintaining the effectiveness of this plan. By following this BCP, Source will be better prepared to handle emergencies and ensure business resilience.

