Edition 1 – released October 2025

Cargo Operations Contingency Planning Framework

Guidance document

Executive Summary

In cargo operations, robust contingency plans are crucial for ensuring safety and business continuity. This document outlines a strategic framework to mitigate risks, safeguard resources and minimise operational downtime. By proactively preparing for potential disruptions and defining clear response strategies, organizations can enhance resilience and maintain service reliability. The scope of this guidance is limited to non-sector-based enterprise governance and best practices. Implementation of specific regional or national civil aviation regulations concerning business continuity and emergency management is not included or referenced.

Purpose of a Contingency Framework

The primary purpose of a contingency framework is to ensure uninterrupted operations during unexpected disruptions. This involves minimising downtime, protecting critical resources and maintaining effective communication with employees, customers and stakeholders.

General Principles for All Stakeholders

Contingency framework is to be embedded in the Quality Management System. To ensure the effectiveness of contingency planning across the air cargo supply chain, stakeholders should adhere to the following principles:

a. **Proactive Preparation:** Identify potential risks and implement preventative measures before disruptions occur.

b. **Response and Recovery:** Outline clear and proactive procedures and roles and responsibilities to facilitate quick recovery to normal operations, with minimal disruption

c. **Collaboration:** Engage with other stakeholders, including airlines, ground handlers, freight forwarders and regulators, to ensure alignment and interoperability of contingency plans.

d. **Customization:** Tailor contingency plans to address the unique risks and operational requirements of the specific organization.

e. **Risk Assessment and mitigation:** Conduct regular comprehensive risk assessments to identify vulnerabilities and prioritize contingency measures and keep risk registry updated

f. **Compliance:** Ensure plans meet all relevant regulatory, safety and security standards as outlined by IATA and local authorities.

g. **Flexibility:** Design plans that are adaptable to a variety of disruption scenarios, enabling rapid response to both anticipated and unforeseen events.

h. **Testing and Training:** Conduct regular drills and simulations and provide regular training to employees on contingency procedures to ensure preparedness and effective implementation during disruptions.

Continuous Improvement: Review and update contingency plans regularly based on lessons learned from drills, incidents, or changes in operational conditions.

Contingency framework

a. **Focus:** Addresses specific risks or scenarios that may disrupt normal operations.
b. **Preparation:** Developed in advance and may require ongoing updates and revisions.

c. **Scope**: Covers a wide range of potential scenarios and events such as, but are not limited to power outages, cyber-attacks or supply chain disruptions
d. **Response Time**: Typically implemented after a contingency event occurs and may have a longer lead time.

Key Objectives:

a. **Operational Continuity**: Ensure seamless and continued operations during disruptions.

b. **Resource Protection**: Safeguard physical, digital, and human assets that are critical to operations, and reputation of the organization.

c. **Stakeholder Communication**: Ensure timely, regular and transparent communication with all relevant parties.

d. **Rapid Recovery:** Enable a swift return to normal operations while minimizing impact on customers and productivity.

Scenarios to be considered – Risks

While not exhaustive, this contingency framework covers a wide range of possible disruptions, including:

a. **Technology Failures**: Computer systems, messaging platforms and cargo management disruptions.

b. **Cybersecurity Threats to enterprise systems (non-aviation infrastructure)**: Data breaches and ransomware attacks.

c. **Workforce Shortages**: Absenteeism or lack of skilled personnel.

d. **Security or safety incidents such as a terrorist attack or aircraft accident**

e. **Facility Disruptions**: Partial or complete unavailability of critical facilities.

f. **External Factors**: Industrial actions, environmental events, geopolitical events, economic/trade wars or blocked access to facilities.

Core Strategies:

To mitigate the impact of these scenarios, organizations should adopt the following strategies:

a. **Risk Assessments:** Conduct regular assessments to identify vulnerabilities and prioritize resources for the most significant risks.

b. **Risk Mitigation:** Ensure residual risks identified during risk and vulnerability assessment are appropriately mitigated

c. **Alternative Solutions, Redundancy and Backups**: Identifying temporary facilities, rerouting logistics and securing emergency resources. Establishing and implementing alternative systems, secure data backups, and identifying temporary operational solutions.

d. **Employee Training and Cross-Functionality**: Train and equip staff to handle diverse roles and ensure their readiness for contingency scenarios.

e. **Crisis Communication**: Developing a clear and robust plan for internal and external communications to keep all stakeholders informed.

f. **Continuous Improvement**: Conduct post-incident reviews to enhance future preparedness and refine contingency measures.

This document serves as a guide for preventive recommendations, and quickly activating contingency measures, prioritizing critical functions, maintaining operations as long as possible and recovering from disruptions effectively. By proactively addressing potential risks and assigning clear roles and responsibilities, the organization can enhance its resilience and ensure uninterrupted service delivery to its customers.

Scenarios to be considered - Risks

1. **Technology Failures**: Disruptions to computer systems, messaging platforms, cargo management systems and warehouse automation.
    a. **Backup Systems:** Regularly back up all critical data and systems. Use both on-site and off-site backups to ensure data is safe even if one location is compromised.
    b. **Redundant Systems:** Implement redundant systems that can take over if the primary system fails. This includes servers, network equipment and communication tools. Conduct regular testing of redundant systems.
    c. **Software and Hardware Failures:** Address potential issues proactively with regular maintenance and updates.
2. **Cybersecurity Threats**: Data breaches and ransomware attacks.
    a. **Cybersecurity Measures:** Use firewalls, antivirus software and regular security audits to protect against cyber threats. Train employees on cybersecurity best practices.
    b. **Alternative Communication Channels:** Have alternative communication methods such as satellite phones, radios, or secure messaging apps in case primary systems fail.
    c. **Employee Training:** Train employees on recognizing phishing and other cyber threats.
3. **Workforce Shortages**: Absenteeism or lack of qualified personnel. Epidemic and/or industrial actions.
    a. **Cross-Training Employees:** Ensure that employees are trained to handle multiple roles so operations can continue smoothly even if key personnel are absent.
    b. **Temporary Staffing Agencies:** Maintain relationships with staffing agencies that can provide temporary workers at short notice.
    c. **Remote Work Capabilities:** Equip employees with tools and access for remote work, including laptops, VPN access and collaboration software.
    d. **Industrial Actions Negotiation:** Have a strategy for negotiating with unions or employee groups to resolve disputes quickly.
4. **Facility Disruptions**: Partial or complete unavailability of critical facilities.
    a. **Alternative Work Locations:** Identify and prepare alternative locations for the temporary relocation of operations.

   b. **Mobile Units:** Use mobile units or temporary structures if the main facility is unusable.
   c. **Insurance Coverage:** Ensure insurance policies cover damage to facilities and provide for business interruption.
5. **External Factors**: 3rd Industrial actions or blocked access to facilities.
   a. **Alternative Transportation Routes:** Identify and communicate alternative routes for employees, suppliers and customers.
   b. **Local Partnerships:** Partner with local businesses or organizations to use their facilities or resources temporarily.
   c. **Environmental Disruptions:** Plan for natural disasters and other environmental risks.

Crisis management

a. **Initiation:** Designate a person or team responsible for initiating the contingency plan. This could be a senior manager or a dedicated crisis management team. Clearly define the role of each person in the team.
b. **Communications:** Maintain an updated emergency contact list.
c. **Staff Notification:** Develop a clear process for informing staff about the activation of a contingency plan. This could include emails, text messages, or an internal communication platform.
d. **Customer Communication:** Plan how to inform customers about potential disruptions. This could include email notifications or updates on your website.
e. **Communication Plan:** Use predefined templates for urgent messages and maintain open lines of communication via multiple channels.
f. **Internal Experts:** Identify internal subject matter experts who can provide the necessary knowledge and skills to address the situation. Ensure they are available and briefed on their roles.

Recovery and Resumption

Steps for Recovery:

a. Assess damage and operational capacity.
b. Prioritize resource protection and resumption of critical operations.
c. Monitor and evaluate the effectiveness of recovery measures.

Post-Incident Review:

a. Analyse root causes and response effectiveness.
b. Update contingency plans based on lessons learned.
c. Conduct training to address gaps identified.

IATA recommends that all stakeholders in cargo operations develop their own tailor-made contingency plans. These plans should align with the specific risks, operational requirements and regulatory obligations of each organization. By proactively preparing for disruptions, stakeholders can collectively strengthen the resilience of the cargo supply chain and ensure uninterrupted service delivery.

For additional guidance on crisis and emergency management related planning, stakeholders are recommended to take reference from

- IATA Airport Handling Manual (AHM 620) and
- IATA Emergency Response Best Practices Handbook (ERP).
- Crisis communications and Reputation Management post COVID guidelines
- Integrated Risk and Resilience Management Manual
- IATA SeMS Manual
- IATA Cybersecurity Supply Chain Oversight Guidance Material (CSCOGM)

END