



Cargo Security Plan Review Checklist

Plan Scope and Objectives

Verifies the plan clearly defines the scope of cargo covered, associated risks, and the overall objectives for cargo security.

Describe the types of cargo covered by the plan (e.g., high-value goods, hazardous materials, perishable items).

Write something...

Define the geographical scope of the plan (e.g., specific countries, regions, or trade lanes).

Write something...

Estimated annual volume of cargo handled (units/weight/value).

Enter a number...

Does the plan include cargo transported via all relevant modes (e.g., road, rail, sea, air)?

☐

Yes

☐

No

☐

Partially

Summarize the overall security objectives of the cargo security plan.

Write something...

Does the plan specifically address security concerns related to theft?

☐ Yes

☐ No

Does the plan specify consequences for security breaches?

☐ Yes

☐ No

Risk Assessment

Evaluates the thoroughness and accuracy of the risk assessment process, considering potential threats and vulnerabilities.

Describe the methodology used for risk identification.

Write something...

Estimated Value of Cargo (USD)

Enter a number...

Primary Cargo Risk Category (e.g., Theft, Damage, Contamination)

- ☐ Theft
- ☐ Damage
- ☐ Contamination
- ☐ Loss
- ☐ Tampering

Potential Threat Actors Considered (Select all that apply)

- ☐ Criminal Organizations
- ☐ Disgruntled Employees
- ☐ Terrorist Groups
- ☐ Opportunistic Thieves
- ☐ Natural Disasters

Detail the potential impact of the highest-rated risks.

Write something...

Risk Score (Scale of 1-10, 10 being highest)

Enter a number...

Risk Assessment Review Date

Security Measures - Personnel

Reviews security protocols related to personnel, including screening, training, background checks, and access control.

Background Checks Conducted?

- ☐ Yes
- ☐ No
- ☐ Partial (Specify)

Number of Personnel Trained in Security Awareness

Enter a number...

Describe Personnel Security Training Content

Write something...

Which of the following security clearances are required for relevant personnel?

- ☐ Tier 1
- ☐ Tier 2
- ☐ Tier 3
- ☐ None
- ☐ Other (Specify)

Are Access Controls Implemented?

- ☐ Yes
- ☐ No
- ☐ Partial (Specify)

Last Personnel Security Training Date

Enter date...

Describe procedures for monitoring personnel activity.

Write something...

Security Measures - Physical

Examines physical security measures at origin, transit points, and destination, such as fencing, lighting, and surveillance.

Perimeter Fence Height (meters)

Enter a number...

Number of Security Cameras

Enter a number...

Lighting Types Installed

- ☐ LED
- ☐ Halogen
- ☐ Motion Sensor
- ☐ Floodlights


Type of Access Control System

- ☐ Keypad
- ☐ Biometric
- ☐ Card Reader
- ☐ Guard Station

Describe Physical Security Vulnerabilities Identified & Mitigation Plans

Write something...

Physical Security Layout Diagram

 Upload File

Are Security Guards Present?

☐ Yes

☐ No

Location of Main Gate

 [Set My Current Location](#)



Security Measures - Technology

Assesses the use of technology for cargo tracking, monitoring, and security, including GPS, RFID, and alarm systems.

GPS Tracking System in Use?

- ☐ Yes
- ☐ No
- ☐ Partial/Limited Use

What technologies are used for cargo monitoring?

- ☐ RFID
- ☐ IoT Sensors (Temp, Humidity, Shock)
- ☐ Video Surveillance
- ☐ Geofencing
- ☐ Tamper Detection Devices


Number of cameras covering key loading/unloading zones

Enter a number...

Describe the alert system in place for detecting security breaches (e.g., geofence violations, tamper alerts)

Write something...

Upload relevant screenshots or documentation of technology interfaces

 Upload File

Is the technology integrated with other security systems?

- ☐ Yes
- ☐ No
- ☐ Limited Integration

Encryption Level used for data transmission (scale of 1-10)

Enter a number...

Security Measures - Transportation

Evaluates the security protocols in place during transportation, including route planning, vehicle security, and driver training.

Driver Background Checks Conducted?

- ☐ Yes
- ☐ No
- ☐ N/A - Driver Provided by Carrier

Vehicle Security Measures Implemented:

- ☐ GPS Tracking
- ☐ Alarm System
- ☐ Tamper-Evident Seals
- ☐ Vehicle Inspection Records Maintained
- ☐ Secure Cab Access

Route Selection Process:

- ☐ Pre-determined Routes Used
- ☐ Dynamic Route Planning Based on Risk
- ☐ Route Selection Documentation Available

Maximum Vehicle Speed Limit

Enter a number...

Driver Training Records Summary

Write something...

Vehicle Seal Integrity Checks?

- ☐ Yes, at origin and destination
- ☐ Yes, at destination only
- ☐ No
- ☐ N/A – Seals Managed by Carrier

Last Route Risk Assessment Review Date

Enter date...

Typical Route Start/End Points

 [Set My Current Location](#)



Incident Response Plan

Reviews procedures for responding to security incidents, including reporting, investigation, and recovery.

Describe the procedure for initial incident reporting (who to contact, what information to provide).

Write something...

Estimated timeframe (in hours) for first responders to arrive at the incident location.

Enter a number...

Who is responsible for coordinating the investigation?

- ☐ Security Manager
- ☐ Law Enforcement
- ☐ Insurance Provider
- ☐ Legal Counsel

Check all actions to be taken immediately upon discovering a security breach.

- ☐ Secure the scene
- ☐ Notify authorities
- ☐ Document the incident
- ☐ Contain the loss
- ☐ Preserve evidence

Date of last incident response plan test/exercise.

Enter date...

Describe the procedure for notifying stakeholders (customers, insurance, etc.).

Write something...

Who is authorized to communicate with the media regarding an incident?

- ☐ Company Spokesperson
- ☐ Legal Counsel
- ☐ Security Manager
- ☐ No external communication

Communication & Reporting

Verifies communication protocols for sharing security information between stakeholders and reporting incidents.

Primary Communication Method for Security Alerts:

- ☐ Email
- ☐ Phone
- ☐ SMS/Text Message
- ☐ Secure Messaging App

Who needs to be notified of security breaches?

- ☐ Logistics Manager
- ☐ Security Team
- ☐ Law Enforcement
- ☐ Shipping Partner
- ☐ Customer

Average Response Time to Security Alerts (minutes):

Enter a number...

Describe the process for reporting suspicious activity:

Write something...

Date of last communication protocol review:

Enter date...

Reporting system in place?

☐ Yes

☐ No

Upload Contact List for Security Reporting:

 Upload File

Plan Review & Update

Confirms a process exists for regularly reviewing and updating the cargo security plan based on changing threats and vulnerabilities.

Date of Last Plan Review

Enter date...

Review Frequency (in months)

Enter a number...

Summary of Changes Made During Last Review

Write something...

Areas of Plan Reviewed/Updated

- ☐ Risk Assessment
- ☐ Personnel Security
- ☐ Physical Security
- ☐ Technology Security
- ☐ Transportation Security
- ☐ Incident Response
- ☐ Communication Procedures

Justification for any deviations from the standard review frequency

Write something...

Review Outcome

- ☐ Plan Approved
- ☐ Plan Requires Minor Revisions
- ☐ Plan Requires Major Revisions
- ☐ Plan Rejected

Name of Reviewer

Write something...

Reviewer Signature

Compliance & Regulations

Ensures the plan complies with applicable legal and regulatory requirements (e.g., C-TPAT, customs regulations).

Is the plan compliant with C-TPAT requirements?

- ☐ Yes
- ☐ No
- ☐ Not Applicable

Does the plan address relevant customs regulations (e.g., import/export controls)?

- ☐ Yes
- ☐ No
- ☐ Review Required

Specify relevant country-specific regulations addressed in the plan.

Write something...


Record the last C-TPAT validation date (if applicable).

Enter a number...

Date of last regulatory compliance review.

Enter date...

Upload supporting documentation for regulatory compliance (e.g., certifications, permits).

 Upload File

Select all applicable regulatory frameworks:

- ☐ Customs-Trade Partnership Against Terrorism (C-TPAT)
- ☐ ISO 28000
- ☐ PIB (Port Inspectorate Business)
- ☐ Other (Specify in Long Text)

If 'Other' selected above, specify framework.

Write something...