



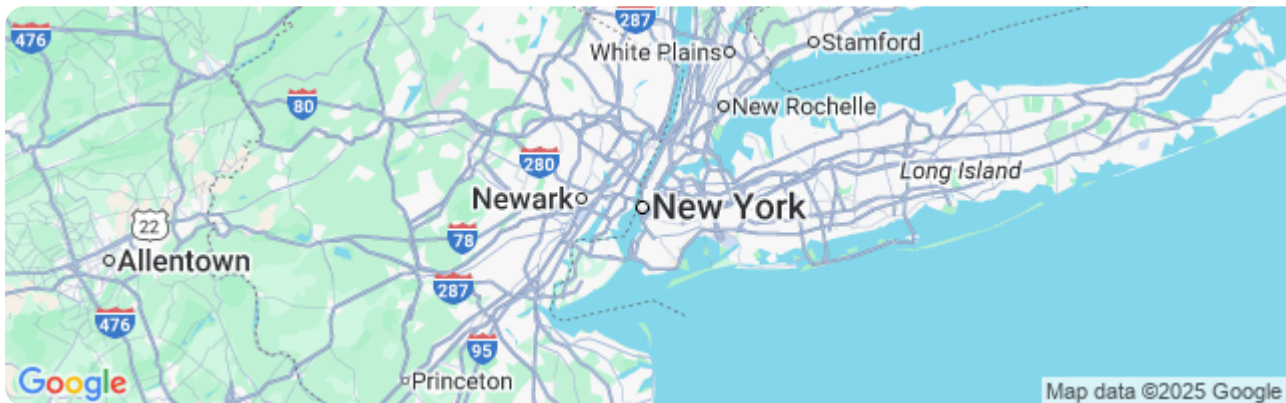
Supply Chain Security Risk Checklist

Physical Security Assessments

Evaluates physical access controls and security measures at key facilities.

Warehouse/Facility Location

 [Set My Current Location](#)



Perimeter Security (Fencing, Walls)

- ☐ Adequate & Maintained
- ☐ Needs Improvement
- ☐ Not Present

Number of Security Cameras

Enter a number...

Last Perimeter Security Inspection Date

Enter date...

Description of Access Control System (Card Readers, Biometrics)

Write something...

Visitor Management Protocol

- ☐ Formal System in Place
- ☐ Informal Process
- ☐ No Defined Process

Site Security Layout Diagram

 Upload File

Cybersecurity Risk Management

Assesses cybersecurity posture across the supply chain, including data protection and system vulnerability.

Last Penetration Test Score

Enter a number...

Current Security Framework (e.g., NIST, ISO 27001)

- ☐ NIST CSF
- ☐ ISO 27001
- ☐ Other

Summary of Recent Cybersecurity Incidents

Write something...


Security Controls Implemented (Select all that apply)

- ☐ Firewalls
- ☐ Intrusion Detection/Prevention Systems
- ☐ Endpoint Detection and Response (EDR)
- ☐ Multi-Factor Authentication (MFA)
- ☐ Data Encryption (at rest and in transit)
- ☐ Vulnerability Scanning

Date of Last Security Awareness Training

Enter date...

Upload Latest Vulnerability Scan Report

 Upload File

Supplier Risk Profiling

Identifies and prioritizes suppliers based on security risk factors and geographic location.

Supplier Risk Score (1-10)

Enter a number...

Geographic Region of Supplier

- ☐ North America
- ☐ Europe
- ☐ Asia
- ☐ South America
- ☐ Africa
- ☐ Oceania

Criticality to Supply Chain

- ☐ High
- ☐ Medium
- ☐ Low

Supplier's Security Certification(s) (e.g., ISO 27001, SOC 2)

Write something...

Last Risk Assessment Date

Enter date...

Supplier Tier (e.g., Tier 1, Tier 1.5, Tier 2)

- ☐ Tier 1
- ☐ Tier 1.5
- ☐ Tier 2
- ☐ Tier 2+

Supplier Security Questionnaire

 Upload File

Contractual Security Requirements

Reviews supplier contracts to ensure adequate security clauses and liability provisions are in place.

Security Breach Notification Timeline Defined?

- ☐ Yes, defined in contract
- ☐ No, not defined
- ☐ Needs Clarification

Penalties for Security Breaches (Value)

Enter a number...


Description of Security Audit Rights Granted to Company

Write something...

Data Encryption Requirements Specified?

- ☐ Yes, specified
- ☐ No, not specified
- ☐ Needs Clarification

Attach Contractual Security Addendum (if applicable)

 Upload File

Last Contract Review Date

Enter date...

Specific Security Standards Referenced in Contract (e.g., ISO 27001, SOC 2)

- ☐ ISO 27001
- ☐ SOC 2
- ☐ NIST Cybersecurity Framework
- ☐ Other (Specify in Long Text)

Transportation Security

Evaluates security measures during transportation of goods, including tracking, route optimization, and theft prevention.

Mode of Transportation

- ☐ Truck
- ☐ Rail
- ☐ Sea
- ☐ Air

Average Shipment Value (USD)

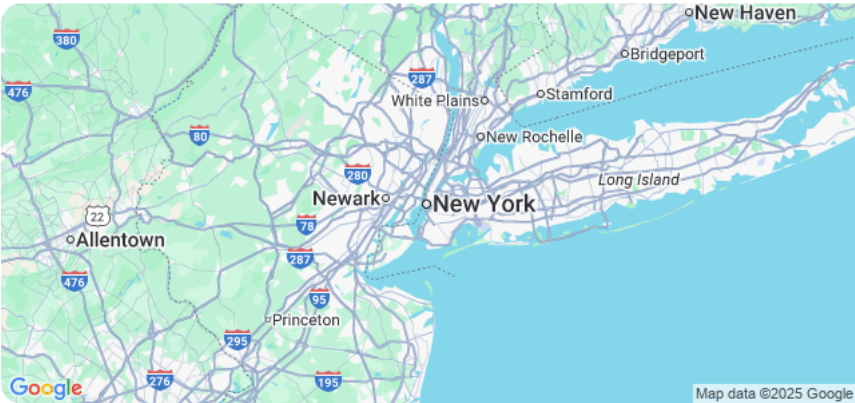
Enter a number...

Security Measures Implemented (Select All That Apply)

- ☐ GPS Tracking
- ☐ Tamper-Evident Seals
- ☐ Security Escorts
- ☐ Cargo Insurance
- ☐ Route Optimization

Primary Transportation Hub Location

 Set My Current Location



Last Security Audit Date

Enter date...

Transportation Security Plan Document

 Upload File

Carrier Security Rating

- ☐ Excellent
- ☐ Good
- ☐ Fair
- ☐ Poor

Incident Response Planning

Examines the preparedness for security incidents, including detection, containment, and recovery procedures.

Describe the incident response team composition and roles.

Write something...

Estimated time to activate the Incident Response Plan (in minutes).

Enter a number...

Primary communication method for incident notification (e.g., Email, Phone, SMS)

- ☐ Email
- ☐ Phone
- ☐ SMS
- ☐ Dedicated Platform

Date of last Incident Response Plan test/simulation

Enter date...

Outline steps for identifying and classifying security incidents.

Write something...

Potential incident types covered by this plan (Select all that apply)

- ☐ Malware Infection
- ☐ Data Breach
- ☐ Supply Chain Disruption
- ☐ Cyberattack (e.g., Ransomware)
- ☐ Natural Disaster
- ☐ Theft/Loss of Equipment

Describe the process for containing and eradicating incidents.

Write something...

Target Recovery Time Objective (RTO) - In hours.

Business Continuity & Disaster Recovery

Reviews plans to maintain operations during disruptions, including alternate sourcing and facility backups.

Estimated Downtime Tolerance (Hours)

Enter a number...

Last Disaster Recovery Test Date

Enter date...

Summary of Recovery Procedures

Write something...

Critical Systems Covered by DR Plan

- ☐ ERP System
- ☐ Warehouse Management System
- ☐ Order Management System
- ☐ Transportation Management System
- ☐ Customer Relationship Management (CRM)

Backup Location Type

- ☐ Cold Site
- ☐ Warm Site
- ☐ Hot Site
- ☐ Cloud-Based Backup

DR Plan Documentation

 Upload File

Next DR Plan Review Date

Enter date...

Compliance & Regulatory Checks

Verifies adherence to relevant security regulations and industry standards.

Relevant Regulations (e.g., GDPR, C-TPAT)

- ☐ GDPR
- ☐ C-TPAT
- ☐ ISO 27001
- ☐ SOC 2
- ☐ Other (Specify)

Last Compliance Audit Date

Enter date...

Audit Score (if applicable)

Enter a number...

Summary of Findings from Last Compliance Audit

Write something...

Third-Party Certification Status

- ☐ Certified
- ☐ Pending Certification
- ☐ Not Applicable

Compliance Documentation (e.g., Certificates, Audit Reports)

 Upload File

Data Security & Privacy

Assesses controls for protecting sensitive data shared with and by suppliers.

Data Encryption at Rest?

- ☐ Yes
- ☐ No
- ☐ Partial/Unclear

Data Encryption in Transit?

- ☐ Yes
- ☐ No
- ☐ Partial/Unclear

Number of Data Breaches in Past Year?

Enter a number...

Details of Data Breaches (if any)

Write something...

Data Privacy Frameworks Adhered To?

- ☐ GDPR
- ☐ CCPA
- ☐ HIPAA
- ☐ Other (Specify in LONG_TEXT)

If 'Other' selected for Data Privacy Frameworks, please specify.

Write something...

Data Retention Policy in Place?

- ☐ Yes
- ☐ No
- ☐ Partial/Unclear

Last Data Privacy Impact Assessment Date

Enter date...

Employee Security Awareness

Evaluates training and awareness programs for employees and suppliers regarding security risks and best practices.

Have you received security awareness training in the last 12 months?

- ☐ Yes
- ☐ No
- ☐ Not Applicable

Which security topics have you been trained on?

- ☐ Phishing Awareness
- ☐ Password Security
- ☐ Data Handling
- ☐ Physical Security
- ☐ Social Engineering

How confident are you in identifying a phishing email (1-10, 10 being very confident)?

Enter a number...

Describe a recent security incident you were involved in (if any).

Write something...

Are you aware of the company's reporting procedures for security incidents?

- ☐ Yes
- ☐ No
- ☐ Unsure

Date of last security awareness training completion.

Enter date...