



Supply Chain Cybersecurity & Data Protection Checklist 2026

Network Security & Perimeter Defense

Ensuring robust firewalls, intrusion detection systems (IDS), and secure access controls are active across all supply chain nodes.

Implemented Perimeter Security Controls

- ☐ Next-Generation Firewall (NGFW)
- ☐ Intrusion Prevention System (IPS)
- ☐ Virtual Private Network (VPN) for Remote Access
- ☐ Network Segmentation (VLANs)
- ☐ DDoS Protection Services

Last Firewall Configuration Audit Date

Security Gateway IP Address Range

Description of Identified Network Vulnerabilities

Write something...

Upload Recent Network Penetration Test Report

 Upload File

IT Security Officer Verification

Third-Party & Vendor Risk Management

Verifying the cybersecurity maturity and data handling protocols of external suppliers, partners, and logistics providers.

Vendor Risk Tier

- ☐ Critical (Direct Access to Core Systems)
- ☐ High (Handles Sensitive Data)
- ☐ Medium (Limited Data Access)
- ☐ Low (No Digital Integration)

Security Certifications Verified

- ☐ ISO 27001
- ☐ SOC2 Type II
- ☐ GDPR Compliance
- ☐ NIST Cybersecurity Framework
- ☐ Cyber Essentials

Vendor Cybersecurity Audit Report

 Upload File

Last Security Assessment Date

Enter date...

Identified Vulnerabilities & Mitigation Plan

Write something...

Auditor Verification Signature

Access Control & Identity Management

Implementing Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC) for all users accessing SCM software and databases.

MFA Implementation Status

- ☐ Fully Implemented
- ☐ Partially Implemented
- ☐ Not Implemented

Authorized User Roles Verified

- ☐ Warehouse Manager
- ☐ Procurement Officer
- ☐ Logistics Coordinator
- ☐ Third-Party Vendor
- ☐ System Administrator

Last Access Audit Date

Enter date...

Identity Provider (IdP) Name

Write something...

Description of Access Revocation Procedure

Write something...

Security Officer Verification

Data Encryption & Integrity

Standardizing encryption protocols for data at rest and data in transit, specifically for sensitive shipping, billing, and proprietary product information.

Encryption Standard Implemented

- ☐ AES-256
- ☐ RSA-2048
- ☐ TLS 1.3
- ☐ Other

Data States Protected

- ☐ Data at Rest
- ☐ Data in Transit
- ☐ Data in Use

Last Encryption Key Rotation Date

Encryption Protocol Documentation Summary

Write something...

Upload Encryption Certificate/Audit Proof

 Upload File

Data Protection Officer Verification

Endpoint & IoT Device Security

Securing connected hardware, including warehouse scanners, GPS trackers, automated picking robots, and IoT-enabled sensors.

Connected Devices Under Audit

- ☐ Handheld Scanners/RF Terminals
- ☐ Automated Guided Vehicles (AGVs)
- ☐ IoT Temperature/Humidity Sensors
- ☐ GPS Tracking Units
- ☐ Warehouse Security Cameras
- ☐ RFID Gates/Readers

Device Firmware Update Status

- ☐ Up to date
- ☐ Pending Update
- ☐ Outdated/Critical Vulnerability

Last Security Patch Deployment Date

Enter date...

Identified Vulnerabilities or Unsecured Devices

Write something...

Device Inventory & Configuration Report

 Upload File

IT Security Officer Verification

Incident Response & Disaster Recovery

Developing and testing protocols for rapid response to ransomware, data breaches, and system outages within the supply chain ecosystem.

Last Incident Response Drill Date

Enter date...

Identified Vulnerability Types

- ☐ Ransomware Attack
- ☐ Data Breach
- ☐ DDoS Attack
- ☐ Unauthorized Access
- ☐ Physical Hardware Theft

Incident Recovery Action Plan Summary

Write something...

Disaster Recovery Plan Document

 Upload File

Current Recovery Time Objective (RTO) Status

- ☐ Within Target
- ☐ At Risk
- ☐ Exceeding Limit

IT Security Manager Approval

Employee Training & Security Awareness

Conducting regular phishing simulations and cybersecurity training for staff handling logistics and procurement data.

Last Training Completion Date

Enter date...

Training Modules Completed

- ☐ Phishing Awareness
- ☐ Password Management & MFA
- ☐ Secure Data Handling
- ☐ Social Engineering Defense
- ☐ Incident Reporting Procedures

Number of Staff Trained in Last 12 Months

Enter a number...

Summary of Identified Training Gaps

Write something...

Training Attendance Logs/Certificates

 Upload File

Compliance Officer Verification

Compliance & Regulatory Alignment

Ensuring all digital processes adhere to global standards such as GDPR, SOC2, and industry-specific data protection regulations.

Applicable Regulatory Frameworks

- ☐ GDPR (General Data Protection Regulation)
- ☐ SOC2 Compliance
- ☐ ISO/IEC 27001
- ☐ CCPA (California Consumer Privacy Act)
- ☐ HIPAA (for Healthcare Supply Chain)
- ☐ C-TPAT (Customs-Trade Partnership Against Terrorism)

Last Compliance Audit Date

Enter date...

Compliance Certification Documents

 Upload File

Regulatory Gap Analysis Summary

Write something...

Compliance Status

- ☐ Fully Compliant
- ☐ Partial Compliance
- ☐ Non-Compliant
- ☐ Under Review

Compliance Officer Verification

Continuous Monitoring & Auditing

Establishing automated logs and periodic security audits to detect anomalies in supply chain data flows.

Last Audit Completion Date

Enter date...

Audit Frequency

- ☐ Weekly
- ☐ Monthly
- ☐ Quarterly
- ☐ Annually

Security Monitoring Tools in Use

- ☐ SIEM (Security Information and Event Management)
- ☐ Endpoint Detection and Response (EDR)
- ☐ Vulnerability Scanners
- ☐ Network Traffic Analyzers

Identified Vulnerabilities & Observations

Write something...

Upload Recent Audit Report

 Upload File

Compliance Officer Verification

< Previous

> Next

✓ Finish

 **Generate Sample Report**