ChecklistGuro

Network Security Audit Checklist

Executive Summary & Scope

Defines the audit's purpose, scope of assessment (networks, systems, data), and intended audience. Includes a high-level overview of findings and recommendations.

Audit Objective Statement

Write something...

Scope Description (Networks, Systems, Data)

Write something...

Number of Locations Included in Audit

Enter a number...

Audit Start Date

Enter date...

Audit End Date (Estimated)

Enter date...

Logistics Business Areas Included

- [ ] Warehousing
- [ ] Transportation (Trucking)
- [ ] Freight Forwarding
- [ ] Supply Chain Management
- [ ] Customs Clearance

Systems within Scope (Select all that apply)

- [ ] TMS (Transportation Management System)
- [ ] WMS (Warehouse Management System)
- [ ] GPS Tracking Systems
- [ ] ERP System
- [ ] Custom APIs

Primary Contact for Audit

Write something...

Brief Overview of Observed Risks (Initial Assessment)

Write something...

Network Infrastructure Assessment

Evaluates the security posture of core network devices (routers, switches, firewalls) and their configurations.

Number of Firewalls in Use

Enter a number...

Firewall Vendor

- [ ] Cisco
- [ ] Palo Alto Networks
- [ ] Fortinet
- [ ] Check Point
- [ ] Other

Summary of Firewall Rule Set Review

Write something...

Current Router Firmware Version (Specify for key routers)

Number of VLANs in Use

Enter a number...

VLAN Security Segmentation Implemented (Select all that apply)

- [ ] PCI DSS Compliance
- [ ] Guest Network Isolation
- [ ] Departmental Isolation
- [ ] Logistics Data Isolation
- [ ] None

Last Router Firmware Update Date (Specify for key routers)

Enter date...

Wireless Network Security

Focuses on the security of wireless networks used for vehicle tracking, warehouse operations, and employee devices.

Number of Wireless Access Points (WAPs)

Enter a number...

Wireless Encryption Protocol in Use

- [ ] WEP
- [ ] WPA
- [ ] WPA2
- [ ] WPA3
- [ ] TKIP
- [ ] AES

Wireless Network Security Protocols Enabled

- [ ] MAC Address Filtering
- [ ] RADIUS Authentication
- [ ] 802.1X Authentication
- [ ] Captive Portal
- [ ] Guest Network Isolation

Wireless Network Authentication Method

- [ ] Open
- [ ] Shared Key
- [ ] RADIUS

Description of Wireless Network Segmentation (e.g., guest, employee, vehicle)

Write something...

Wireless Network Configuration Files (e.g., WAPs, Controller)

Upload File

Last Wireless Network Security Assessment Date

Enter date...

SSID(s) in Use

Write something...

Endpoint Security

Assesses the security of devices connecting to the network, including employee laptops, mobile devices, and IoT devices (e.g., tracking sensors).

Number of Company-Issued Laptops

Enter a number...

Number of Mobile Devices (Company Managed)

Enter a number...

Endpoint Protection Software in Use

- [ ] Microsoft Defender for Endpoint
- [ ] CrowdStrike Falcon
- [ ] Symantec Endpoint Protection
- [ ] Other (Specify in LONG_TEXT)

Specify 'Other' Endpoint Protection Software (if selected above)

Write something...

Security Features Enabled on Endpoints (Select All That Apply)

- [ ] Antivirus
- [ ] Firewall
- [ ] Data Loss Prevention (DLP)
- [ ] Disk Encryption
- [ ] Host-Based Intrusion Prevention System (HIPS)
- [ ] Application Whitelisting

Endpoint Patch Management Process

- [ ] Automated and Centralized
- [ ] Manual and Decentralized
- [ ] Combination of both

Last Patch Management Cycle Completion Date

Enter date...

Describe the process for onboarding new endpoints to the network

Write something...

Data Security & Privacy

Examines the protection of sensitive logistics data, including shipment details, customer information, and route planning.

Data Encryption at Rest Compliance

- [ ] Fully Compliant
- [ ] Partially Compliant
- [ ] Not Compliant

Data Encryption in Transit Compliance

- [ ] Fully Compliant
- [ ] Partially Compliant
- [ ] Not Compliant

Describe the data classification scheme in use (e.g., Public, Confidential, Restricted).

Write something...

Approximate number of customer records processed annually.

Enter a number...

Which data privacy regulations apply to the organization? (Select all that apply)

- [ ] GDPR
- [ ] CCPA
- [ ] HIPAA
- [ ] Other (Specify in LONG_TEXT)

Describe data retention policies and procedures. How long is data stored?

Write something...

Upload a copy of the data privacy policy (if available).

Upload File

Date of last data privacy impact assessment (DPIA).

Enter date...

Access Control & Identity Management

Reviews user access rights, authentication mechanisms, and account management practices.

Multi-Factor Authentication (MFA) Implementation

- [ ] Fully Implemented for All Users
- [ ] Partially Implemented (Specific Roles)
- [ ] Not Implemented

Password Complexity Policy Enforcement

- [ ] Strict Policy Enforced (Length, Complexity, Rotation)
- [ ] Moderate Policy Enforced
- [ ] Weak or No Policy

Account Lockout Threshold (Failed Login Attempts)

Enter a number...

Privilege Access Management (PAM) Practices

- [ ] Least Privilege Principle Applied
- [ ] Regular Privilege Access Reviews Performed
- [ ] Just-in-Time (JIT) Privilege Elevation
- [ ] Centralized PAM Solution in Place

Last User Access Review Date

Enter date...

Description of User Onboarding/Offboarding Procedures

Write something...

Centralized Identity Provider (IdP) Usage

- [ ] Using Centralized IdP (e.g., Azure AD, Okta)
- [ ] Using Local User Accounts
- [ ] Hybrid Approach

Incident Response & Business Continuity

Evaluates the organization's ability to detect, respond to, and recover from security incidents and disruptions to logistics operations.

Estimated Recovery Time Objective (RTO) in Hours

Enter a number...

Estimated Recovery Point Objective (RPO) in Hours

Enter a number...

Describe the current Incident Response Plan (IRP)

Write something...

Which departments are involved in the incident response process?

- [ ] IT
- [ ] Legal
- [ ] Operations
- [ ] Public Relations
- [ ] Executive Management

Last Incident Response Plan Review Date

Enter date...

Summarize recent simulated incident response exercises (drills) and findings.

Write something...

Communication methods used during an incident (choose one)

- [ ] Email
- [ ] Phone Calls
- [ ] SMS
- [ ] Dedicated Incident Communication Platform

Upload a copy of the Business Continuity Plan (BCP)

Upload File

Vendor Risk Management

Focuses on the security practices of third-party vendors providing critical logistics services (e.g., transportation management systems, GPS tracking providers).

Vendor Security Questionnaires Completed?

- [ ] Yes
- [ ] No
- [ ] In Progress

Number of Vendors Audited Annually

Enter a number...

Summary of Vendor Risk Assessment Methodology

Write something...

Security Controls Verified in Vendor Agreements (Select all that apply)

- [ ] Data Encryption at Rest
- [ ] Data Encryption in Transit
- [ ] Multi-Factor Authentication
- [ ] Regular Security Audits
- [ ] Incident Response Plan
- [ ] Business Continuity Plan
- [ ] Data Breach Notification Procedures

Date of Last Vendor Security Audit

Enter date...

Vendor Security Audit Reports Reviewed?

- [ ] Yes
- [ ] No
- [ ] N/A

Description of Vendor's Data Retention Policies

Write something...

Physical Security & Network Access Points

Considers the physical security of network infrastructure, data centers, and access control to network resources.

Are network rooms/server rooms physically secured?

- [ ] Yes, with access control system
- [ ] Yes, with locks and monitoring
- [ ] No, lacking physical security
- [ ] Unsure

What type of access control is implemented?

- [ ] Biometrics (fingerprint, retinal scan)
- [ ] Keycard/Proximity Card
- [ ] Combination Lock
- [ ] None
- [ ] Manual Logbook

Number of network access points (routers, switches, firewalls) exposed without physical barriers?

Enter a number...

Describe visitor access procedures to network areas.

Write something...

Are cabling closets locked?

- [ ] Yes
- [ ] No
- [ ] Partially (some closets locked)
- [ ] Not applicable

Upload a diagram of network room layout.

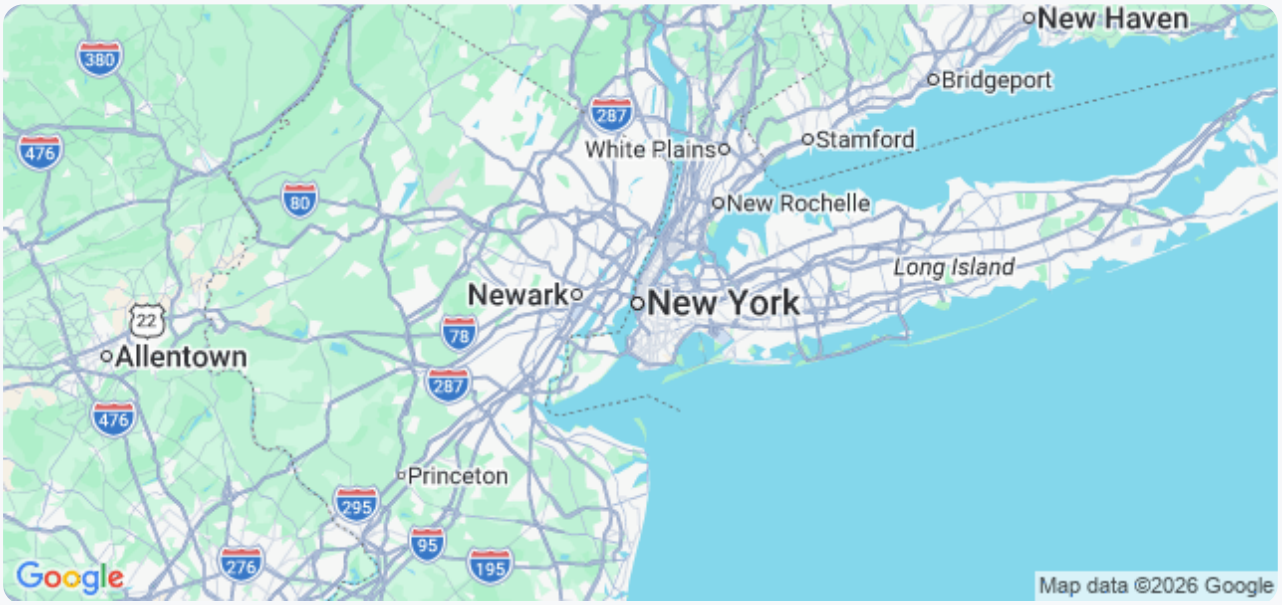
Upload File

Is there video surveillance of network areas?

- [ ] Yes, and recordings are retained
- [ ] Yes, but recordings are not retained
- [ ] No
- [ ] Unsure

Location of primary network infrastructure (e.g., server room, main router)

Set My Current Location



Log Management & Monitoring

Reviews logging practices and the ability to monitor network activity for suspicious behavior and security events.

Number of Security Logs Generated Daily

Enter a number...

Centralized Logging System in Use?

- [ ] Yes
- [ ] No
- [ ] Partial

Description of Log Retention Policy (duration, storage location, disposal method)

Write something...

Which Log Sources are Currently Monitored?

- [ ] Firewalls
- [ ] Routers
- [ ] Servers
- [ ] Endpoint Devices
- [ ] Intrusion Detection/Prevention Systems
- [ ] Applications
- [ ] Cloud Services

Are Logs Encrypted at Rest?

- [ ] Yes
- [ ] No
- [ ] Partial

Time Required to Review Logs for Anomalies

Enter time...

Describe the process for responding to log-generated alerts.

Write something...

Are Log Alerts Integrated with an Incident Response System?

- [ ] Yes
- [ ] No