



Access Control System Validation Checklist

System Overview & Configuration

This section covers initial system setup, configuration reviews, and baseline settings verification.

System Software Version

System Manufacturer

System Architecture Description

Access Control Method

- ☐ Card Reader
- ☐ Biometric (Fingerprint)
- ☐ PIN Code
- ☐ Mobile Credential

Date of Last System Configuration Change

Enter date...

Number of Access Points Controlled

Enter a number...

Network Connectivity

- ☐ Wired
- ☐ Wireless
- ☐ Both

Describe any custom configurations applied to the system.

Write something...

User Management & Roles

Focuses on the creation, modification, and deletion of user accounts and their associated access roles within the logistics environment.

Default User Role Assignment Method

- ☐ Manual
- ☐ Automated (Group Based)
- ☐ Combination

Maximum Number of Users per Role

Enter a number...

Password Complexity Requirements Enforcement?

- ☐ Yes
- ☐ No
- ☐ Partial/Configurable

Last User Role Review Date

Enter date...

Justification for any deviations from Standard User Role Definitions

Write something...

Which User Groups require Two-Factor Authentication?

- ☐ Warehouse Staff
- ☐ Supervisors
- ☐ Receiving Personnel
- ☐ Shipping Personnel
- ☐ Management

User Account Lockout Policy?

- ☐ None
- ☐ Fixed Number of Attempts
- ☐ Configurable

Account Deactivation Process Followed?

Write something...

Access Point Validation

Evaluates the physical access points (doors, gates, loading docks) and their integration with the access control system.

Verify physical location of Access Point: Door A

 [Set My Current Location](#)



Access Point ID Number (e.g., engraved plate)

Enter a number...

Access Point Type (e.g., Door, Gate, Loading Dock)

- ☐ Door
- ☐ Gate
- ☐ Loading Dock
- ☐ Other

Access Control Method (e.g., Card Reader, Biometric, Keypad)

- ☐ Card Reader
- ☐ Biometric (Fingerprint)
- ☐ Keypad
- ☐ Other

Number of Reader Heads Installed

Enter a number...

Notes on Physical Security of Access Point (e.g., damage, obstructions)

Write something...

Access Level Assigned (e.g., Employee, Visitor, Contractor)

- ☐ Employee
- ☐ Visitor
- ☐ Contractor
- ☐ Restricted

Observed Access Point Operation Time (e.g., opening/closing sequence)

Credential Management

Covers card/fob issuance, PIN/biometric enrollment, and procedures for revocation/replacement of credentials.

Number of Active Credentials Issued

Enter a number...

Credential Issuance Process Followed?

- ☐ Yes, documented procedure followed
- ☐ No, deviations occurred
- ☐ Not Applicable

Describe any deviations from the credential issuance procedure.

Write something...

Credential Types Supported?

- ☐ Proximity Cards
- ☐ Fobs
- ☐ PIN Codes
- ☐ Biometrics (Fingerprint)
- ☐ Mobile Credentials

Date of Last Credential Revocation Audit

Enter date...

Number of Revoked Credentials in Last Month

Enter a number...

Describe the procedure for credential replacement (lost/damaged)

Write something...

Credential Revocation Process Verified?

- ☐ Yes, documented procedure followed
- ☐ No, deviations occurred
- ☐ Not Applicable

Audit Trail & Reporting

Verifies the system's ability to accurately record access events and generate reports for security review and compliance.

Audit Log Retention Period (Days)

Enter a number...

Audit Log Storage Location

- ☐ Local Server
- ☐ Cloud Storage
- ☐ Dedicated Security Information and Event Management (SIEM) system

Date of Last Audit Trail Review

Enter date...

Summary of Findings from Last Audit Trail Review

Write something...

Which Event Types are Logged?

- ☐ Card Access
- ☐ PIN Access
- ☐ Biometric Access
- ☐ Door Forced
- ☐ System Override
- ☐ User Account Modification
- ☐ Credential Issuance/Revocation

Report Delivery Method

- ☐ Email
- ☐ Automated Export to SIEM
- ☐ Manual Export

Number of Audit Logs Reviewed During Validation

Enter a number...

Description of any discrepancies found during Audit Trail Validation (if any)

Write something...

Time of last Audit Report Generated

Integration with Logistics Systems

Focuses on how the access control system interacts with other systems like warehouse management (WMS), transportation management (TMS), or security cameras.

Which Logistics Systems are integrated with the Access Control System?

- ☐ Warehouse Management System (WMS)
- ☐ Transportation Management System (TMS)
- ☐ Yard Management System (YMS)
- ☐ Order Management System (OMS)
- ☐ Security Camera System (VMS)
- ☐ None

Describe the data exchanged between the Access Control System and the integrated Logistics System(s).

Write something...

What is the latency (in seconds) for data synchronization between the Access Control System and the integrated Logistics System(s)?

Enter a number...


Is data encryption used during transmission between the Access Control System and the integrated Logistics System(s)?

- ☐ Yes
- ☐ No
- ☐ Partial

Describe the process for handling discrepancies or errors encountered during data integration.

Write something...

Upload integration configuration files (if available).

 Upload File

Does the Access Control System restrict access to Logistics Systems based on user roles and permissions?

- ☐ Yes
- ☐ No
- ☐ Partial

Emergency & Override Procedures

Tests the functionality of emergency access procedures, override capabilities, and fail-safe mechanisms.

Verify emergency unlock procedure documentation exists and is readily available.

☐ Yes

☐ No

☐ N/A

Record response time (seconds) for emergency unlock request.

Enter a number...

Test manual override functionality (e.g., key override).

☐ Successful

☐ Partial Success

☐ Unsuccessful

Describe any issues encountered during manual override testing.

Write something...

Confirm emergency power backup system tested.

☐ Yes

☐ No

☐ N/A

Record timestamp of emergency override activation test.

Document steps taken to revert system to normal operation after emergency override.

Write something...

Were designated personnel properly trained on emergency override procedures?

- ☐ Yes
- ☐ No
- ☐ Partial

Security & Vulnerability Assessment

Identifies potential vulnerabilities and assesses the system's resilience against unauthorized access or manipulation.

Brute-Force Lockout Time (Seconds)

Enter a number...

Encryption Protocol Used (e.g., AES, TLS)

- ☐ AES
- ☐ TLS
- ☐ Other (Specify)

Describe any observed vulnerabilities during penetration testing (if performed).

Write something...


Which of the following potential vulnerabilities are mitigated by the current configuration? (Select all that apply)

- ☐ Default Credentials
- ☐ Unpatched Software
- ☐ Physical Tampering of Readers
- ☐ Lack of Two-Factor Authentication
- ☐ SQL Injection

Firewall configuration: Is access to the Access Control System server(s) restricted to authorized personnel/systems only?

- ☐ Yes
- ☐ No
- ☐ Not Applicable/Unknown

Upload Penetration Testing Report (if applicable)

 Upload File

Date of last vulnerability scan.

Enter date...