Security Review Checklist

A practical assessment tool for access control, video surveillance, visitor management, intercoms, networking, monitoring, and long-term system support.

Use this checklist to identify gaps before they become risk points. Mark each item as In Place, Needs Review, or N/A, then use the scoring and action-plan pages to prioritize next steps.

Assessment Details

Organization / Facility:	
Site Address / Area:	
Reviewer:	
Date:	
Primary Security Goal:	

How to Use This Checklist

1	Walk the site and review the real workflow: entrances, doors, visitor paths, service areas, restricted rooms, cameras, intercoms, and network closets.
2	Mark each item as In Place, Needs Review, or N/A. Use the notes column to identify owner, priority, and next action.
3	Score each section on the summary page and choose the top five improvements to address first.

Recommended scoring: 0 = Not in place, 1 = Informal or inconsistent, 2 = In place, 3 = Strong, documented, and reviewed regularly.

1. Facility Profile and Security Goals

Review Item	In Place	Needs Review	N/A	Notes / Owner / Priority
The main entrances, staff entrances, service doors, gates, and restricted areas have been identified.				
The current security goals are documented: safety, accountability, loss prevention, compliance, uptime, or response.				
The site has a current list of security contacts, administrators, vendors, and support responsibilities.				
Security procedures reflect how people actually move through the facility each day.				
Multi-site, campus, or remote-building requirements have been reviewed where applicable.				
Known pain points are documented, such as propped doors, missed video, visitor bottlenecks, or system downtime.				

2. Access Control and Credentials

Review Item	In Place	Needs Review	N/A	Notes / Owner / Priority
Users have individual credentials instead of shared cards, shared codes, or generic logins.				
Former employees, contractors, vendors, and temporary users are removed promptly.				
Access levels match roles, departments, schedules, and authorized areas.				
Temporary access is limited by time, location, and business need.				
Credential types are reviewed: cards, fobs, mobile credentials, biometric options, or PINs.				
Administrative permissions are limited to approved users and reviewed regularly.				
Door schedules, holidays, unlock periods, and exception rules are documented.				
Access control reports can be generated for investigations, audits, or operational review.				

3. Doors, Entrances, Exits, and Restricted Areas

Review Item	In Place	Needs Review	N/A	Notes / Owner / Priority
Each controlled door has an assigned purpose and risk level.				
Main entrances have a clear process for staff, visitors, vendors, and after-hours access.				
Service doors, delivery doors, loading areas, and employee entrances are included in the plan.				
Restricted spaces are identified, such as IT rooms, records rooms, medication rooms, labs, or storage areas.				
Door-held-open and forced-door events are monitored, routed, and reviewed.				
Emergency exits and fire-code requirements are understood before access rules are changed.				
Staff know what to do when a door alarm, held-open event, or access denial occurs.				
Outdoor gates, parking areas, yards, and remote entry points are reviewed where applicable.				

4. Video Surveillance and VMS

Review Item	In Place	Needs Review	N/A	Notes / Owner / Priority
Camera placement supports a clear security purpose, not just broad coverage.				
Important access points have useful video context: entrances, lobbies, gates, and restricted doors.				
Video quality is adequate for the intended purpose, such as overview, recognition, or investigation.				
Lighting, glare, low light, wide dynamic range, and obstruction issues have been reviewed.				
Video retention needs are documented and aligned with policy and storage capacity.				
Users know how to search, export, and review footage when needed.				
Video analytics are considered where they can reduce missed events or improve response.				
Privacy-sensitive areas and signage requirements are considered.				

5. Visitor, Vendor, and Contractor Management

Review Item	In Place	Needs Review	N/A	Notes / Owner / Priority
Visitors are checked in consistently through a documented process.				
Visitor identity, host, purpose, arrival time, and departure are recorded where needed.				
Vendor and contractor access is time-limited and tied to approved work.				
Temporary badges, QR codes, credentials, or escorted-access procedures are controlled.				
After-hours visitor, delivery, and contractor procedures are documented.				
Visitor records can be reviewed during investigations, audits, or emergency events.				
Reception or front-desk staff understand approval, denial, and escalation procedures.				
Emergency visibility includes visitors, contractors, vendors, and non-employees where practical.				

6. Smart Intercoms and Entry Communication

Review Item	In Place	Needs Review	N/A	Notes / Owner / Priority
Main entrances, remote doors, gates, and delivery points have appropriate communication tools.				
Staff can see, speak with, and verify people before releasing a door where required.				
Remote unlock rules are documented and limited to authorized users.				
Intercoms are placed at a practical height and location for users and visitors.				
After-hours intercom routing is documented and tested.				
Video intercom activity supports visitor management and access control workflows.				
Failed calls, missed calls, and unanswered entry requests are reviewed if they create risk.				

7. Network and Infrastructure Readiness

Review Item	In Place	Needs Review	N/A	Notes / Owner / Priority
Security devices are mapped, including cameras, panels, readers, intercoms, switches, access points, and servers.				
PoE capacity, port availability, cabling quality, and power requirements are reviewed.				
Network segmentation, VLANs, firewall rules, and remote access methods are documented where applicable.				
Wireless bridges, access points, and remote buildings have reliable coverage and monitoring.				
The organization avoids risky shortcuts such as unmanaged port forwarding or undocumented public exposure.				
Network health, uptime, and device status can be monitored or supported remotely where appropriate.				
Backup power, surge protection, and critical-device recovery procedures are considered.				
The network is treated as part of the security system, not as background infrastructure.				

8. Monitoring, Alerts, and Response

Review Item	In Place	Needs Review	N/A	Notes / Owner / Priority
Alerts are routed to the right people, not simply generated without ownership.				
Critical events are defined, such as forced door, held-open door, camera offline, intrusion, or after-hours activity.				
Response procedures explain who verifies the event, who responds, and when escalation is required.				
Live monitoring or guard response is considered for sites with after-hours or high-risk activity.				
False alarms are reviewed so the system remains trusted and useful.				
Emergency scenarios are discussed, including lockdowns, evacuations, resident safety, or critical access needs.				
Staff training is current and practical for daily users, not only administrators.				

9. Reporting, Accountability, and Administration

Review Item	In Place	Needs Review	N/A	Notes / Owner / Priority
Access control, visitor, video, and system health reports are reviewed on a regular schedule.				
Reports support real questions: who entered, what happened, when it happened, and what response followed.				
User permissions are reviewed for administrators, managers, front desk users, guards, and support staff.				
Audit trails are available for important changes, door events, and user activity.				
Policies exist for record retention, privacy, evidence handling, and report access.				
Security procedures are documented enough that new staff can follow them.				
The system can support compliance, insurance, operational, or internal review requirements where applicable.				

10. Maintenance, Lifecycle, and Support

Review Item	In Place	Needs Review	N/A	Notes / Owner / Priority
Firmware, software, license status, and supported product versions are reviewed.				
A maintenance plan exists for cameras, readers, controllers, intercoms, servers, switches, and credentials.				
Backup procedures are documented for databases, configurations, video settings, and access rules.				
Old devices, unsupported software, weak passwords, and inactive users are identified for cleanup.				
Support contacts and escalation pathways are known by administrators and facility leadership.				
The organization has a plan for growth, new doors, new cameras, new sites, or additional integrations.				
Security reviews are scheduled before problems become incidents.				

Score Summary and Priority Planning

Use this page to convert the checklist into action. Sections with low scores, repeated "Needs Review" items, or unclear ownership should be prioritized first.

Checklist Section	Score 0-3	Top Gap / Concern	Priority
1. Facility Profile & Security Goals			
2. Access Control & Credentials			
3. Doors, Entrances, Exits, & Restricted Areas			
4. Video Surveillance & VMS			
5. Visitor, Vendor, & Contractor Management			
6. Smart Intercoms & Entry Communication			
7. Network & Infrastructure Readiness			
8. Monitoring, Alerts, & Response			
9. Reporting, Accountability, & Administration			
10. Maintenance, Lifecycle, & Support			

Top Five Security Improvements

#	Improvement	Owner	Target Date	Status
1				
2				
3				
4				
5				

30 / 60 / 90 Day Action Plan

Timeline	Recommended Focus	Actions / Notes
Next 30 Days	Address urgent risks, remove old credentials, document key contacts, and review critical doors or cameras.	
Next 60 Days	Improve workflows, reporting, visitor processes, alert routing, and network visibility.	
Next 90 Days	Plan upgrades, training, maintenance routines, multi-site standards, and long-term support needs.	

Need Help Reviewing Your Security Environment?

PMT Security supports organizations and integrators with access control, video surveillance, visitor management, smart intercoms, cloud-managed networking, live guard monitoring, and integrated physical security solutions.

Access Control
Review doors, credentials, access levels, schedules, reports, and administrator permissions.

Video Surveillance & VMS
Review camera placement, event verification, retention, search tools, and investigation workflows.

Visitor Management
Review visitor, vendor, contractor, temporary access, check-in, and emergency visibility workflows.

Networking & Support
Review PoE, cabling, switches, wireless, remote support, firmware, backups, and lifecycle planning.

Ready to move from security questions to a clearer action plan?

Visit PMTSecurity.com or contact PMT Security. USA: +1 727-786-1900 | Canada: +1 647-999-4644

Discuss access control, video surveillance, visitor management, intercoms, networking, and integrated security solutions for your facility.