BTI Communications Group, Ltd.

Business Security Systems

Southern California | Phoenix | Chicagoland

(800) 435-7284

info@btigroup.com

www.btigroup.com

PHYSICAL SECURITY SELF-ASSESSMENT

Office Security Checklist

A Practical Physical Security Self-Assessment for Safer Workplaces

Version 2026 | BTI Communications Group

How to Use This Checklist

This checklist is designed to help business owners, facilities managers, operations leaders, office managers, and executives conduct a thorough, honest evaluation of their office's physical security environment. Walk through each section during or after a facility walkthrough. Score each item honestly — the goal is to identify gaps, not to achieve a perfect score.

This checklist focuses on:

- Office physical security (doors, locks, perimeter, lighting)
- Access control systems (badges, fobs, RFID cards, readers, credentials)
- Video security (cameras, NVR/DVR/VMS, recording, remote access)
- Alarm systems (intrusion detection, monitoring, dual-path communication)
- Visitor and contractor management
- Connected security system protection and remote access
- Emergency readiness and employee training

Scoring System

Symbol	Rating	What It Means
✅	Good	This item is in place and functioning as expected.
⚠️	Needs Improvement	This item exists but has gaps, inconsistencies, or needs updating.
🔴	Critical Gap	This item is missing, broken, or poses an immediate risk. Prioritize for action.

After completing each section, transfer Critical Gaps and Needs Improvement items to the Office Security Action Plan in Section 8.

Who Should Complete This Assessment

Suggested participants: Facilities Manager, Operations Director, Office Manager, IT/Security Coordinator, or Executive Leadership. A physical walkthrough of the facility is strongly recommended.

Section 1: Building Access & Entry Points

SECTION 1 OF 8

Physical security begins at the perimeter. Every door, window, loading dock, stairwell, and rooftop access point is a potential vulnerability. Walk the exterior and interior of your facility and evaluate each entry point honestly.

Circle one per row: 🟢 Good | 🟡 Needs Improvement | 🔴 Critical Gap

#	Checklist Item	Score
1	The main entrance is visible from a staffed reception desk or monitored camera.	🟢 🟡 🔴
2	Entry doors are equipped with a controlled access method (keycard, fob, intercom, or buzzer).	🟢 🟡 🔴
3	Lobby doors are not propped open or bypassed during business hours.	🟢 🟡 🔴
4	Signage directs all visitors to check in at reception before proceeding.	🟢 🟡 🔴
5	The main entrance has adequate lighting during all hours of operation.	🟢 🟡 🔴
6	All secondary doors (side, rear, service) require a credential to enter from outside.	🟢 🟡 🔴
7	Secondary doors are alarmed or monitored and not routinely propped open.	🟢 🟡 🔴
8	Loading dock and delivery areas have controlled access and are not left unattended when open.	🟢 🟡 🔴
9	Delivery personnel are not allowed to enter the main office without escort.	🟢 🟡 🔴
10	Ground-floor windows are secured with locks and, where appropriate, window sensors.	🟢 🟡 🔴
11	Window coverings or film prevent visibility into sensitive areas from outside.	🟢 🟡 🔴
12	Parking areas are well-lit at night and during early morning/evening hours.	🟢 🟡 🔴
13	Parking lot cameras cover entry/exit points and the full lot where feasible.	🟢 🟡 🔴
14	Visitor and employee parking areas are clearly separated where applicable.	🟢 🟡 🔴
15	Stairwell doors require a credential to re-enter from the stairwell side.	🟢 🟡 🔴
16	Elevator access to sensitive floors is controlled by keycard or floor restriction.	🟢 🟡 🔴
17	Roof access doors are locked, alarmed, and not accessible to unauthorized personnel.	🟢 🟡 🔴
18	All exterior doors use commercial-grade hardware (not residential-grade locks).	🟢 🟡 🔴
19	Door frames, hinges, and strike plates are in good condition with no visible damage.	🟢 🟡 🔴
20	Doors close and latch fully — no doors that fail to latch or self-close properly.	🟢 🟡 🔴

Section 1 Summary

Total Items: 20

✅ Good: ___

⚠️ Needs Improvement: ___

🔴 Critical Gap: ___

Notes / Priority Actions:

_____

_____

_____

Section 2: Access Control & Credential Management

SECTION 2 OF 8

Access control is the backbone of a layered security strategy. It's not enough to have keycards — what matters is how permissions are managed, how quickly credentials are removed when employees leave, and whether access levels reflect actual job roles. Evaluate your credential management practices honestly.

Circle one per row: 🟢 Good | 🟡 Needs Improvement | 🔴 Critical Gap

#	Checklist Item	Score
1	Every employee has an individual credential (badge, fob, or mobile credential) — no shared cards, fobs, PINs, or badges.	🟢 🟡 🔴
2	Temporary contractor and vendor credentials are issued separately and tracked.	🟢 🟡 🔴
3	Temporary credentials are set to expire automatically or are manually deactivated when the engagement ends.	🟢 🟡 🔴
4	Master keys and override codes are limited to authorized personnel only and documented.	🟢 🟡 🔴
5	A current inventory of all issued credentials (cards, fobs, badges) is maintained.	🟢 🟡 🔴
6	Blank or spare credentials are stored securely and not casually available.	🟢 🟡 🔴
7	Terminated employee credentials are deactivated within 24 hours of separation.	🟢 🟡 🔴
8	Lost or stolen RFID cards, fobs, or badges are disabled immediately upon report.	🟢 🟡 🔴
9	Former employee access is confirmed removed — not just deactivated at the door but fully removed from the system.	🟢 🟡 🔴
10	Access levels are role-based — employees can only access areas required for their job.	🟢 🟡 🔴
11	Access permissions are reviewed at least quarterly and updated when roles change.	🟢 🟡 🔴
12	Sensitive areas (server rooms, executive offices, records rooms, cash-handling areas, pharmacies, storage) have additional access restrictions beyond standard employee access.	🟢 🟡 🔴
13	Door schedules are configured so doors lock/unlock automatically at appropriate times.	🟢 🟡 🔴
14	Holiday schedules are reviewed and updated annually.	🟢 🟡 🔴
15	Reader tamper alerts are configured and monitored where supported by the system.	🟢 🟡 🔴
16	Forced-door alerts are configured and monitored where supported.	🟢 🟡 🔴
17	Held-door (door held open too long) alerts are configured where supported.	🟢 🟡 🔴
18	Access control software is managed by a named administrator — not a shared or generic account.	🟢 🟡 🔴
19	Access logs are retained for a minimum of 90 days (or per applicable regulation).	🟢 🟡 🔴
20	Access logs are periodically reviewed for unusual patterns (after-hours access, repeated failed attempts).	🟢 🟡 🔴
21	Access events can be correlated with video footage when an incident occurs.	🟢 🟡 🔴
22	The access control system has been tested within the past 12 months to confirm all doors and readers function correctly.	🟢 🟡 🔴

Section 2 Summary

Total Items: 22

Good: ___ | 🟡 Needs Improvement: ___ | 🔴 Critical Gap: ___

Notes / Priority Actions:

_____

_____

_____

Section 3: Video Security, NVR/DVR/VMS & Camera Coverage

SECTION 3 OF 8

A well-designed video surveillance system serves two critical functions: deterrence and evidence. Cameras placed visibly at entry points, parking areas, and sensitive zones discourage unauthorized activity. Properly maintained recording systems ensure footage is available when incidents occur. Evaluate both camera coverage and recording system health.

Circle one per row: 🟢 Good | 🟡 Needs Improvement | 🔴 Critical Gap

#	Checklist Item	Score
1	All primary entry and exit points are covered by at least one camera with a clear, unobstructed view.	🟢 🟡 🔴
2	Cameras at entrances are positioned to capture a clear face image of individuals entering.	🟢 🟡 🔴
3	The lobby, reception area, and waiting areas are covered by camera.	🟢 🟡 🔴
4	Parking lots and exterior areas are covered with sufficient resolution to identify vehicles and individuals.	🟢 🟡 🔴
5	Loading docks, service entrances, and delivery areas are covered by camera.	🟢 🟡 🔴
6	Hallways leading to sensitive areas (server rooms, executive offices, cash-handling areas) are covered.	🟢 🟡 🔴
7	Camera placement has been reviewed to eliminate blind spots in high-risk areas.	🟢 🟡 🔴
8	Cameras are mounted at appropriate heights and angles — not easily defeated by hats, hoods, or obstructions.	🟢 🟡 🔴
9	Camera lenses are clean and free of dust, spider webs, or obstructions.	🟢 🟡 🔴
10	Camera housings are intact with no visible damage, vandalism, or tampering.	🟢 🟡 🔴
11	All cameras produce a clear, usable image — no cameras with persistent blur, distortion, or black screens.	🟢 🟡 🔴
12	Low-light or night-vision capable cameras are installed in areas with limited lighting (parking lots, exterior doors).	🟢 🟡 🔴
13	Camera resolution is sufficient to support investigations — faces and license plates are identifiable where required.	🟢 🟡 🔴
14	The NVR, DVR, VMS server, or recording appliance is located in a locked room or secured cabinet.	🟢 🟡 🔴
15	Recording is confirmed active — all cameras are recording and no channels show a loss of signal.	🟢 🟡 🔴
16	Recording retention meets business requirements (minimum 30 days recommended; 90 days for sensitive areas).	🟢 🟡 🔴
17	Storage health is monitored — failed or degrading drives are identified and replaced promptly.	🟢 🟡 🔴
18	Date, time, and camera names displayed on recorded footage are accurate and meaningful enough to support investigations.	🟢 🟡 🔴
19	System health alerts (drive failure, camera loss, recording failure) are configured and sent to the right personnel.	🟢 🟡 🔴
20	Firmware and software for the NVR/DVR/VMS are current and updated on a regular schedule.	🟢 🟡 🔴
21	The recording system administrator account is named, unique, and not shared among multiple users.	🟢 🟡 🔴
22	Default passwords on the NVR/DVR/VMS have been changed from factory settings.	🟢 🟡 🔴
23	Recorded footage can be exported in a format usable for law enforcement, insurance claims, or HR investigations.	🟢 🟡 🔴
24	The process for exporting footage is documented and at least one person on staff knows how to perform it.	🟢 🟡 🔴

Section 3 Summary

Total Items: 24

Good: ___ | 🟡 Needs Improvement: ___ | 🔴 Critical Gap: ___

Notes / Priority Actions:

_____

_____

_____

Section 4: Alarm Systems, Monitoring & Dual-Path Communication

SECTION 4 OF 8

A professionally monitored alarm system is one of the most reliable layers of physical security — but only if it is properly configured, regularly tested, and supported by reliable communication paths. A critical requirement for any business alarm system is dual-path communication: the ability to transmit alarm signals over both internet and cellular so that a cut cable or internet outage does not silence your alarm.

Circle one per row: 🟢 Good | 🟡 Needs Improvement | 🔴 Critical Gap

#	Checklist Item	Score
1	All primary entry doors are protected by door contacts that trigger when opened.	🟢 🟡 🔴
2	Motion sensors are installed in key interior areas (lobbies, hallways, server rooms, storage areas).	🟢 🟡 🔴
3	Glass-break sensors are installed on ground-floor windows in applicable areas.	🟢 🟡 🔴
4	Panic buttons are installed at reception, executive offices, or other high-risk locations.	🟢 🟡 🔴
5	All alarm zones are correctly labeled in the panel and match the physical layout of the facility.	🟢 🟡 🔴
6	There are no bypassed zones that have been left bypassed without documented justification.	🟢 🟡 🔴
7	⚠️ **CRITICAL:** The alarm system uses dual-path communication — both internet/broadband AND cellular backup — so alarm signals transmit even if one path fails.	🟢 🟡 🔴
8	Cellular backup is active, confirmed operational, and billed correctly on the monitoring account.	🟢 🟡 🔴
9	The monitoring center has confirmed receipt of both communication paths.	🟢 🟡 🔴
10	Alarm communication has been tested within the past 12 months to verify signals reach the monitoring center.	🟢 🟡 🔴
11	The alarm panel has a functioning battery backup that has been tested within the past 12 months.	🟢 🟡 🔴
12	Battery backup duration is sufficient to maintain alarm operation during a power outage.	🟢 🟡 🔴
13	The alarm panel shows no persistent trouble conditions, faults, or error indicators.	🟢 🟡 🔴
14	The alarm system is monitored 24/7 by a professional central monitoring station.	🟢 🟡 🔴
15	The monitoring center has current dispatch instructions, including after-hours contacts and verified response preferences.	🟢 🟡 🔴
16	The call list and escalation contacts at the monitoring center are current and accurate.	🟢 🟡 🔴
17	The monitoring center knows which law enforcement jurisdiction to contact for this location.	🟢 🟡 🔴
18	Every authorized user has a unique alarm code — no shared codes among multiple employees.	🟢 🟡 🔴
19	Alarm codes are removed promptly when employees leave or roles change.	🟢 🟡 🔴
20	A current list of authorized alarm users and their codes is maintained and reviewed at least annually.	🟢 🟡 🔴
21	Door contacts, motion sensors, glass-break sensors, and panic buttons are tested at least annually.	🟢 🟡 🔴
22	A written record of the most recent alarm test is on file, including date, technician, and results.	🟢 🟡 🔴

⚠️ **Dual-Path Communication Note:**
If your alarm system communicates only over your internet connection, a cut cable, router failure, or internet outage can prevent alarm signals from reaching your monitoring center. Cellular backup ensures your alarm can still communicate even when your primary internet path is unavailable. Ask your alarm provider to confirm your communication path configuration.

Section 4 Summary

Total Items: 22

Good: ___ | 🟡 Needs Improvement: ___ | 🔴 Critical Gap: ___

Notes / Priority Actions:

_____

_____

_____

Section 5: Visitor Management & Contractor Control

SECTION 5 OF 8

Visitors — including clients, vendors, contractors, maintenance personnel, delivery drivers, and job candidates — represent a unique security challenge. Unlike employees, visitors are often unfamiliar with your facility, may not understand your security expectations, and may have access to areas they should not. A consistent, documented visitor management process reduces risk and creates accountability.

Circle one per row: 🟢 Good | 🟡 Needs Improvement | 🔴 Critical Gap

#	Checklist Item	Score
1	All visitors are required to check in at reception before proceeding into the facility.	🟢 🟡 🔴
2	Visitor identification (government-issued ID) is verified at check-in for all non-routine visitors.	🟢 🟡 🔴
3	Visitors are issued a visible visitor badge that is worn at all times while in the facility.	🟢 🟡 🔴
4	Visitor badges are dated and time-stamped so they cannot be reused on a different day.	🟢 🟡 🔴
5	Visitor badges are collected at check-out and not allowed to leave the building.	🟢 🟡 🔴
6	Visitors are escorted by an employee at all times — they are not allowed to move freely through the facility unaccompanied.	🟢 🟡 🔴
7	Visitors are not allowed access to sensitive areas (server rooms, executive offices, records rooms, storage) without specific authorization.	🟢 🟡 🔴
8	Employees are trained to challenge or report unescorted visitors or unfamiliar individuals in restricted areas.	🟢 🟡 🔴
9	Contractors and vendors are pre-approved before arriving on site.	🟢 🟡 🔴
10	Contractor access is limited to the specific areas required for their work.	🟢 🟡 🔴
11	Contractors working after hours are accompanied by an authorized employee or their access is specifically documented and approved.	🟢 🟡 🔴
12	Contractor credentials (temporary badges, access cards) are collected or deactivated immediately upon completion of work.	🟢 🟡 🔴
13	Vendor and contractor access to security systems (cameras, alarm panels, access control) is supervised and logged.	🟢 🟡 🔴
14	Deliveries are received at a designated area — delivery personnel do not enter the main office unescorted.	🟢 🟡 🔴
15	Unexpected or unscheduled deliveries are verified before acceptance.	🟢 🟡 🔴
16	A visitor log is maintained (electronic or paper) recording name, company, purpose, host employee, time in, and time out.	🟢 🟡 🔴
17	Visitor logs are retained for a minimum of 90 days.	🟢 🟡 🔴
18	Visitor logs can be produced for law enforcement, HR investigations, or insurance claims when needed.	🟢 🟡 🔴
19	Visitor logs are accessible during an evacuation so all visitors can be accounted for at the assembly point.	🟢 🟡 🔴
20	Reception staff know the procedure for visitors during a lockdown, shelter-in-place, or emergency evacuation.	🟢 🟡 🔴

Section 5 Summary

Total Items: 20

Good: ___ | 🟡 Needs Improvement: ___ | 🔴 Critical Gap: ___

Notes / Priority Actions:

_____

_____

_____

Section 6: Connected Security System Protection & Remote Access

SECTION 6 OF 8

Your physical security systems — cameras, NVRs, DVRs, access control software, alarm panels, and remote viewing platforms — are themselves networked devices that require proper configuration and access management. This section evaluates whether those systems are protected from unauthorized access, properly maintained, and managed with the same discipline as the physical security they support.

Circle one per row: 🟢 Good | 🟡 Needs Improvement | 🔴 Critical Gap

#	Checklist Item	Score
1	NVR, DVR, VMS, and recording appliance administrator accounts are named and unique — not shared among multiple users.	🟢 🟡 🔴
2	Default factory passwords on all NVR/DVR/VMS devices have been changed.	🟢 🟡 🔴
3	Former employees and former vendors no longer have administrative access to recording systems.	🟢 🟡 🔴
4	Firmware and software on NVR/DVR/VMS platforms are current and updated on a regular schedule.	🟢 🟡 🔴
5	System health alerts (drive failure, camera loss, recording interruption) are configured and routed to the right personnel.	🟢 🟡 🔴
6	Remote access to cameras, NVRs, DVRs, and VMS platforms is limited to authorized, named users only.	🟢 🟡 🔴
7	Remote viewing uses secure, vendor-supported access methods — not open ports, unsecured shortcuts, or unmanaged workarounds.	🟢 🟡 🔴
8	Cameras are not unnecessarily exposed to the public internet.	🟢 🟡 🔴
9	Former employees, former vendors, and former contractors have been removed from all remote viewing access.	🟢 🟡 🔴
10	Mobile app users with remote camera access are reviewed at least annually.	🟢 🟡 🔴
11	Remote access to video systems is documented — the business knows who can view live or recorded footage remotely.	🟢 🟡 🔴
12	Access control software is managed by named administrator accounts — not shared or generic logins.	🟢 🟡 🔴
13	Default passwords on access control software and hardware have been changed from factory settings.	🟢 🟡 🔴
14	Former employees and former vendors no longer have administrative access to the access control system.	🟢 🟡 🔴
15	Access control software is updated on a regular schedule.	🟢 🟡 🔴
16	Audit logs within the access control system are retained and periodically reviewed.	🟢 🟡 🔴
17	A current inventory of all RFID cards, fobs, and mobile credentials is maintained.	🟢 🟡 🔴
18	Blank or unissued credentials are stored securely and not casually accessible.	🟢 🟡 🔴
19	Reader firmware is current where updates are available and supported.	🟢 🟡 🔴
20	Alarm system installer/dealer codes are managed — default or shared installer codes have been changed or are controlled by the monitoring provider.	🟢 🟡 🔴
21	Vendor and technician remote access to alarm panels, access control systems, or camera systems is documented and limited to active service relationships.	🟢 🟡 🔴
22	When a vendor relationship ends, their remote access to all security systems is confirmed removed.	🟢 🟡 🔴

Section 6 Summary

Total Items: 22

Good: ___ | 🟡 Needs Improvement: ___ | 🔴 Critical Gap: ___

Notes / Priority Actions:

_____

_____

_____

Section 7: Emergency Response & Employee Training

SECTION 7 OF 8

Physical security technology is only as effective as the people who use it. Employees who know how to respond to emergencies, report suspicious activity, follow visitor procedures, and use security systems correctly are a critical layer of your overall security posture. Evaluate your emergency readiness and training practices honestly.

Circle one per row: 🟢 Good | 🟡 Needs Improvement | 🔴 Critical Gap

#	Checklist Item	Score
1	A written emergency response plan exists and is accessible to all employees.	🟢 🟡 🔴
2	The plan covers evacuation, shelter-in-place, lockdown, and active threat response.	🟢 🟡 🔴
3	Emergency exits are clearly marked, unobstructed, and known to all employees.	🟢 🟡 🔴
4	A designated assembly point for evacuations is established and communicated to all staff.	🟢 🟡 🔴
5	Employees know the difference between evacuation, shelter-in-place, and lockdown procedures.	🟢 🟡 🔴
6	Employees know how and where to report security incidents, suspicious behavior, or safety concerns.	🟢 🟡 🔴
7	A process exists for documenting and escalating security incidents internally.	🟢 🟡 🔴
8	Employees are encouraged to report concerns without fear of retaliation.	🟢 🟡 🔴
9	Employees know what to do when the intrusion alarm activates during business hours.	🟢 🟡 🔴
10	Employees know the location and proper use of panic buttons in the facility.	🟢 🟡 🔴
11	Front desk and reception staff have a clear protocol for handling threatening or suspicious individuals.	🟢 🟡 🔴
12	Employees have received training on lockdown procedures appropriate for the facility.	🟢 🟡 🔴
13	Doors in the facility can be locked from the inside quickly in a lockdown scenario.	🟢 🟡 🔴
14	Employees know not to open doors for unknown individuals during a lockdown, even if the individual claims to be law enforcement (verify through a window or intercom first).	🟢 🟡 🔴
15	A current emergency contact list is posted or accessible to all employees.	🟢 🟡 🔴
16	Employees know who to call internally and externally (building management, security, law enforcement) in an emergency.	🟢 🟡 🔴
17	The facility has a method to communicate with all employees simultaneously during an emergency (PA system, mass notification, group text, or similar).	🟢 🟡 🔴
18	Evacuation drills are conducted at least annually and results are documented.	🟢 🟡 🔴
19	New employees receive security orientation covering badge procedures, visitor escort policy, and emergency procedures.	🟢 🟡 🔴
20	Security training is refreshed at least annually for all staff.	🟢 🟡 🔴

Section 7 Summary

Total Items: 20

Good: ___ | 🟡 Needs Improvement: ___ | 🔴 Critical Gap: ___

Notes / Priority Actions:

_____

_____

_____

Section 8: Office Security Action Plan

→ SECTION 8 OF 8

Use this section to consolidate the gaps you identified throughout this assessment into a prioritized action plan. For each Critical Gap or Needs Improvement item, record the details below. Transfer items from each section's summary notes to this plan.

Gap / Issue	Location or System	Recommended Action	Owner	Priority	Target Date	Status
_______________	_______________	_______________	_______________	_______________	_______________	_______________
_______________	_______________	_______________	_______________	_______________	_______________	_______________
_______________	_______________	_______________	_______________	_______________	_______________	_______________
_______________	_______________	_______________	_______________	_______________	_______________	_______________
_______________	_______________	_______________	_______________	_______________	_______________	_______________
_______________	_______________	_______________	_______________	_______________	_______________	_______________
_______________	_______________	_______________	_______________	_______________	_______________	_______________
_______________	_______________	_______________	_______________	_______________	_______________	_______________
_______________	_______________	_______________	_______________	_______________	_______________	_______________
_______________	_______________	_______________	_______________	_______________	_______________	_______________
_______________	_______________	_______________	_______________	_______________	_______________	_______________
_______________	_______________	_______________	_______________	_______________	_______________	_______________

Overall Assessment Summary

Section	Total Items	🟢 Good	🟡 Needs Improvement	🔴 Critical Gap
Section 1: Building Access & Entry Points	20	___	___	___
Section 2: Access Control & Credential Management	22	___	___	___
Section 3: Video Security, NVR/DVR/VMS & Camera Coverage	24	___	___	___
Section 4: Alarm Systems, Monitoring & Dual-Path Communication	22	___	___	___
Section 5: Visitor Management & Contractor Control	20	___	___	___
Section 6: Connected Security System Protection & Remote Access	22	___	___	___
Section 7: Emergency Response & Employee Training	20	___	___	___
TOTAL	**150**	___	___	___

🗺️ Ready to Turn This Assessment Into a Professional Plan?

BTI uses System Surveyor — the leading digital platform for collaborative security system design — to create accurate floor plans, device layouts, and professional proposals during a virtual or on-site assessment with one of our engineers.

During a free System Surveyor walkthrough, a BTI security engineer will:

- Map your facility on a live digital floor plan
- Place cameras, access control readers, alarm sensors, and other devices visually
- Identify gaps and coverage areas in real time
- Generate an accurate, itemized Bill of Materials automatically
- Share the design with you for review and approval before any equipment is purchased

This process is transparent, collaborative, and obligation-free. You see exactly what you're getting before installation begins.

What You See in System Surveyor

Why It Matters

Need Help Evaluating or Upgrading Your Office Security?

Schedule a Free System Surveyor Assessment with a BTI Security Engineer

If your checklist reveals gaps in access control, cameras, alarms, visitor management, or connected systems, BTI can help. Schedule a free virtual site walkthrough with a BTI security engineer using our System Surveyor digital design platform. We'll review your assessment, map your facility, and deliver clear recommendations — no obligation, no pressure.

Discover Commercial Security Solutions from BTI

What Happens During a Free System Surveyor Assessment?

Step 1 — We Review Your Assessment

Share your completed checklist with a BTI engineer. We'll identify your highest-priority gaps before the walkthrough begins.

Step 2 — We Map Your Facility

Using System Surveyor, we create a live digital floor plan of your space and place cameras, access control readers, alarm sensors, and other devices visually — so you can see the proposed system before anything is installed.

Step 3 — You Receive a Clear Proposal

We generate an accurate, itemized Bill of Materials and a written proposal. You review, ask questions, and decide — no pressure, no obligation.

BTI Communications Group

Business Security Systems

📞 (800) 435-7284

✉️ info@btigroup.com

🌐 www.btigroup.com

Serving Southern California | Phoenix | Chicagoland

Disclaimer

This checklist is provided by BTI Communications Group, Ltd. as a general reference tool to help business owners, facilities managers, operations leaders, and executives begin an informed conversation about their office physical security environment.

This document is intended as a starting point for self-assessment only. It does not constitute professional security advice, a formal security audit, a risk assessment, or a compliance evaluation. The items contained in this checklist are general in nature and may not reflect the specific requirements, regulations, or conditions applicable to your facility, industry, or jurisdiction.

Every facility is different. Security needs vary based on building type, occupancy, location, industry, regulatory environment, and risk profile. The findings from this self-assessment should be reviewed and evaluated by a qualified, licensed security professional before any security decisions, purchases, or system changes are made.

BTI Communications Group, Ltd. recommends that all businesses consult with a state-licensed security systems contractor or qualified physical security professional when evaluating, designing, installing, or modifying security systems. Licensing requirements for security contractors vary by state. BTI is licensed in Illinois, Arizona, and California.

This checklist does not create any warranty, guarantee, or representation regarding the security of any facility. BTI Communications Group, Ltd. assumes no liability for security incidents, losses, or damages arising from the use or non-use of this checklist or any information contained herein.

BTI Communications Group, Ltd.
Business Security Systems
Southern California | Phoenix | Chicagoland
(800) 435-7284 | info@btigroup.com | www.btigroup.com