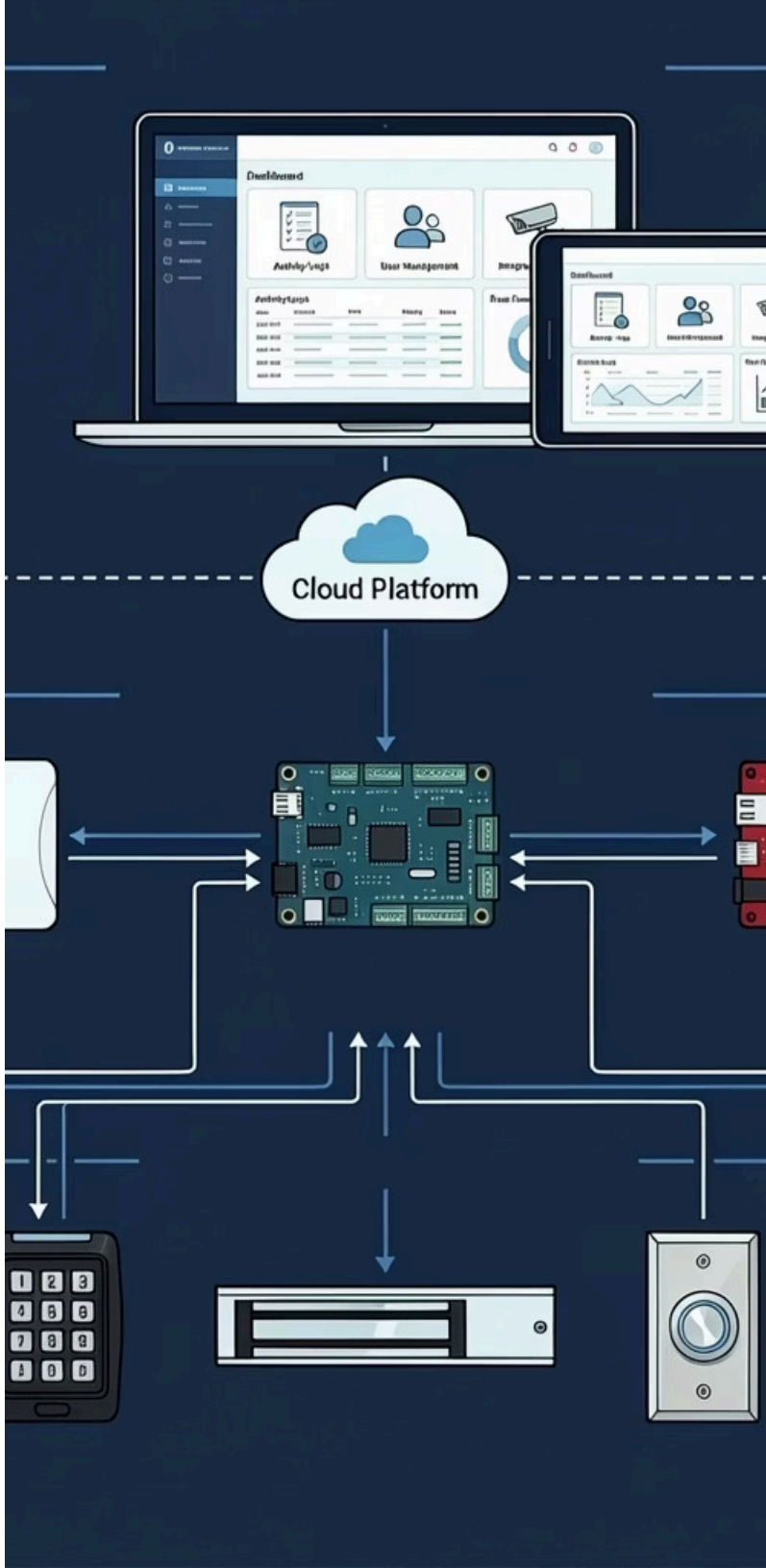
Commercial Access Control Systems Guide

Planning, Installing, and Upgrading Building Access Control Systems

A practical buyer's guide for organizations evaluating access control installation, door security, key card systems, mobile access, turnstiles, and integrated video security.



BTI Communications Group, Ltd.
Serving California • Illinois • Arizona • National Multi-Site • Select International
www.btigroup.com | info@btigroup.com

Executive Summary

Commercial access control has evolved from a simple door lock replacement into one of the most strategically significant technology decisions a facility or enterprise organization can make. The systems deployed today govern who enters your building, which zones they can access, at what times, using what credential, and how that activity can be logged, reviewed, and reported when the system is configured for that purpose. These are not peripheral concerns — they are core to your security posture, operational continuity, and regulatory standing.

The decision to replace mechanical keys with electronic access control touches every department: security, IT, HR, legal, operations, and finance. When designed, installed, administered, and maintained correctly, access control can reduce key-management risk, lower re-keying exposure, accelerate incident investigation, and create useful access records when logging, retention, and reporting are configured correctly. When poorly designed or under-scoped, access control can create a false sense of security, introduce network risk, and make future inspection, audit, service, or remediation work more difficult and expensive.

BTI Communications Group is a licensed access control installation provider with deep expertise across physical security, IT infrastructure, cybersecurity, VoIP, intercoms, and compliance-supporting documentation when included in scope. We serve California, Illinois, and Arizona, with strong deployment experience in healthcare, industrial, logistics, commercial office, and multi-site environments. This guide reflects BTI's front-line experience across commercial deployments and is designed to help your organization make better decisions — regardless of which platform or vendor you ultimately select.

BTI directly serves California, Illinois, and Arizona and supports national deployments through properly licensed local contractors, subcontractors, and project partners where required. For select international projects, BTI can assist with access control planning, manufacturer coordination, remote project support, and deployment coordination when local regulations, product availability, and qualified in-country resources support the scope.

What This Guide Covers

- How to evaluate access control by door, not just by software platform
- How to choose the right locks, readers, credentials, and turnstiles
- Why duty cycle, speed, and throughput matter in healthcare, industrial, office, and logistics environments
- How to compare cloud, on-prem, and hybrid access control platforms
- How access control can support compliance evidence, privacy reviews, and cyber insurance documentation when designed, configured, and documented for that purpose
- How BTI can integrate access control with video, intercom, IT, cybersecurity, VoIP, and managed support when those services are in scope

Design-First Approach

System design begins at the door opening, not inside software. Hardware compatibility, life safety codes, and traffic volume drive every downstream decision.

Platform-Fit Design

BTI evaluates major platforms and hardware ecosystems objectively. We recommend systems based on fit, supportability, integration needs, lifecycle requirements, and the client's operating environment.

Converged Security Model

Access control, video surveillance, alarms, intercoms, IT, VoIP, and cybersecurity can be planned as a coordinated system when those disciplines are part of the project scope.

Documentation-Driven Delivery

BTI scopes documentation requirements during project planning and provides closeout documentation, as-builts, service records, and compliance-supporting artifacts when included in the project scope or service agreement.

How to Use This Guide
Use this guide to understand the major design decisions behind a commercial access control system before requesting a proposal. It can help your team prepare for a site survey, compare platform options, identify compliance or documentation needs, and avoid under-scoped door hardware, credential, integration, or service decisions.

What Is a Commercial Access Control System?

A commercial access control system is a technology infrastructure that electronically governs, monitors, and logs entry and exit at physical openings — doors, gates, turnstiles, elevators, parking barriers, and server room enclosures. Unlike a mechanical lock and key, an access control system grants or denies access based on verified identity credentials, programmed schedules, zone rules, and real-time event conditions. Access transactions can be time-stamped, user-attributed, and retained in system logs when logging and retention are configured for that purpose.

Modern systems consist of several integrated hardware and software layers that work together to enforce access policy. Understanding these layers is essential before evaluating any specific platform or hardware ecosystem.

System Component	Function	Common Examples
Access Control Panel / Controller	Processes credentials, enforces access rules, stores event logs locally	Kantech controllers, Software House controllers, Avigilon ACM controllers, Mercury-based controllers where applicable
Credential Reader	Reads card, fob, mobile, PIN, or biometric identity	HID Signo readers, OSDP readers, mobile credential readers, smart card readers
Door Hardware	Physically secures or releases the door upon valid credential	Magnetic locks, electric strikes, electrified mortise locks
Request-to-Exit (REX)	Allows free egress without credential presentation	PIR motion sensors, push bars with REX contacts
Door Position Switch (DPS)	Monitors door open/closed state; triggers alarms on forced or propped doors	Recessed magnetic contacts
Access Control Software / Platform	Manages users, schedules, policies, reports, and system configuration	Kantech, Software House, Avigilon Alta, Avigilon Unity / ACM, Brivo, RS2 / ACRE, Alarm.com for Business, YourSix
Network Infrastructure	Connects panels, readers, and cameras to servers and cloud	PoE switches, VLANs, fiber backbone
Power Supply / UPS	Provides conditioned power and backup during outages	Altronix, Securitron
Video Integration Layer	Correlates access events with video clips for incident review	Avigilon video, Axis cameras and intercoms, Milestone (video platform integration only)
Identity / HR Integration	Synchronizes user provisioning and de-provisioning with HR systems	Active Directory, Workday, BambooHR connectors

A properly designed access control system starts at the door, not in the software. Hardware compatibility with door frame type, fire rating, life safety codes, and traffic volume must be resolved before platform selection begins.

Why Businesses Replace Keys with Electronic Access Control

Mechanical key systems have fundamental structural limitations that create compounding operational and security risk over time. Every time an employee is terminated, a key is lost, or a contractor relationship ends, organizations face an unresolvable problem: they cannot verify whether their physical space is still secure. Re-keying costs accumulate, access cannot be time-restricted, and there is no audit trail for any door event. These are not theoretical risks — they represent real liability exposure that regulators, insurers, and auditors increasingly scrutinize.

Electronic access control can greatly reduce the re-keying cycle by allowing credentials to be deactivated in software. Credentials can be deactivated in software when the system is properly administered. Access schedules can be enforced automatically — for example, a cleaning crew's badge can be limited to authorized access windows when schedules are configured and maintained, and access attempts outside that window can be logged when reporting is configured. Time-sensitive contractor access can be provisioned with automatic expiration when the platform and workflow support it. Access control systems can record door events such as valid entry, denied entry, forced door, and propped door activity with user identity, timestamp, and door location when those features are configured and retained.

Depending on the organization, access control may help reduce manual security workload, support stronger insurance discussions, and accelerate incident investigation through event-log correlation with video. For multi-site organizations, centralized credential management can provide operational efficiency that is difficult to achieve with mechanical key systems.

Reduce Re-Keying Exposure

Deactivate credentials from software when the system is properly administered. This can greatly reduce locksmith visits, hardware changes, and re-keying delays across supported doors and sites.

Time-Based Access Enforcement

Program access by day, time, holiday schedule, and user group. Cleaning crews, contractors, and vendors can be limited to authorized access windows when schedules are configured and maintained.

Configurable Audit Trails

Door transactions can be logged with user identity and timestamp when logging is configured and retained. Report exports can support incident response, internal reviews, insurance requests, and compliance documentation when reporting and retention are configured for that purpose.

Centralized Multi-Site Management

Manage credentials, policies, and reports across multiple locations from a single platform where the architecture supports it. A strong fit for enterprise, healthcare networks, and industrial campuses.

Access Control Use Cases by Industry

Access control requirements vary significantly by vertical market. A warehouse loading dock faces entirely different design constraints than a hospital medication room or a financial institution's trading floor. Understanding industry-specific use cases is essential for designing a system that aligns with operational workflows, regulatory requirements, and physical security risk profiles.

Healthcare

- Staff entrances, pharmacies, medication rooms, behavioral health areas, server rooms, and visitor management
- Access logs can support compliance evidence when configured and retained for that purpose
- Video, intercom, nurse call, or related integrations may be appropriate depending on workflow and scope

Commercial Office & Multi-Tenant

- Lobby turnstiles, elevator floor access, executive suites, after-hours access, visitor workflows, and tenant separation
- Mobile credentials and cloud administration may simplify management across sites and tenants
- User experience, aesthetics, and accessibility should be balanced with security

Industrial & Logistics

- Shift-change entrances, loading docks, equipment yards, contractor access, vehicle gates, and controlled production areas
- Turnstile throughput, anti-passback, durability, and serviceability are critical design factors
- Access control should be designed around peak traffic, not only average daily use

Data Centers & IT Facilities

- Server rooms, cages, MDF/IDF rooms, network closets, and privileged areas
- Strong credential controls, video verification, visitor logs, and access reviews may support SOC 2, ISO, PCI, cyber insurance, or internal controls when in scope
- Integration with IT identity, ticketing, and security operations may be appropriate for mature environments

Related BTI Resource

Not sure where your facility stands today? BTI's Commercial Security Self-Assessment Checklist can help leadership teams evaluate physical security gaps before planning access control, video surveillance, alarms, intercoms, or managed security upgrades. This checklist is a useful starting point — it does not replace a professional site survey.

Download the Commercial Security Self-Assessment Checklist

Door-by-Door Access Control Design

One of the most common and costly mistakes in access control deployment is treating a building as a uniform set of openings and applying a single hardware specification across all doors. In practice, every door opening has a unique combination of traffic volume, fire rating requirements, life safety obligations, structural characteristics, and security classification that must be evaluated individually. A door-by-door design process is the foundation of a system that will perform reliably, meet code, and support future expansion.

The door-by-door review begins with a physical survey of every opening under consideration. For each door, the designer should review and document the door material and frame type, existing hardware, fire and smoke rating, hinge configuration, door width and weight, the latch mechanism currently in use, whether the opening is on a life safety egress path, and the expected peak traffic volume. This information helps determine which electrified lock type is appropriate, which reader mounting position is feasible, and whether the existing door frame can support the required hardware without modification.

Access control designers also classify each opening by security zone. A lobby entrance, an IT server room, a pharmacy dispensary, and a break room may represent very different security tiers with different credential requirements, audit logging expectations, and alarm response procedures. Zone classification helps shape software policy design as well as hardware selection.

Door Type	Typical Hardware	Life Safety Note	Security Tier	Common Industries
Main Building Entrance	Mag lock + REX + DPS	Free egress requirements should be reviewed for the opening, occupancy, hardware type, local code, and AHJ interpretation	Medium-High	All
Server / IT Room	Electrified mortise or multi-point lock	Check occupancy egress rules	High	Office, Data Center, Healthcare
Pharmacy / Drug Storage	Electric strike + deadbolt + audit reader	DEA or controlled-substance requirements may apply	Very High	Healthcare
Loading Dock / Shipping	Electric strike or mag lock on personnel door; gate operator on vehicle gate	Egress-compliant REX	Medium	Industrial, Logistics
Stairwells	Electric strike; may require card-in-only	Egress requirements should be reviewed by opening and AHJ	Low-Medium	Office, Healthcare, Multi-Tenant
Executive Suite	Electrified mortise or electronic deadbolt	Standard egress	High	Office, Financial
Break Room / Low-Security Interior	Electronic deadbolt or keypad lock	Standard	Low	All
Elevator Floor Access	Floor relay module + reader in cab	Fire recall and elevator requirements should be reviewed with the elevator contractor and AHJ	Variable	Multi-Tenant, Hotel, Healthcare

Door Hardware for Access Control Systems

Door hardware is the physical execution layer of any access control system. It is the component that actually holds the door closed, releases it upon a valid credential, and returns it to a secured state. The selection of the wrong hardware type for a given application is one of the most common sources of system failure, life safety violations, and post-installation remediation costs. Hardware decisions should be reviewed against the door type, frame construction, fire and smoke rating, latch requirements, and applicable local building codes.

The four primary electrified lock types used in commercial access control each have distinct advantages, limitations, and appropriate applications. Understanding the functional differences is essential before specifying hardware for any opening.

Hardware Type	How It Works	Best Applications	Key Limitations
Electromagnetic Lock (Mag Lock)	Energized coil holds armature plate with 600–1,200 lb holding force. Power off = door releases.	Glass doors, aluminum frames, high-security vestibules	Often requires REX, DPS, and fire alarm interface review; no mechanical latch
Electric Strike	Replaces mechanical strike; releases latch remotely. Mechanical latch remains engaged until credential.	Hollow metal doors, retrofit applications, stairwells	Frame modification may be required; fail-safe vs. fail-secure selection should be reviewed
Electrified Mortise Lock	Full mortise lockset with electric latch or deadbolt retraction. High security and ADA-capable.	Executive suites, server rooms, high-security interior doors	Higher cost; requires proper door prep; heavier installation
Electrified Cylindrical Lock	Standard cylindrical lockset with electric credential control. Lower cost option.	Interior low-medium security doors, retrofit projects	Lower holding force; less suitable for exterior high-traffic openings
Electronic Deadbolt	Motorized deadbolt with credential reader integrated or remote	Low-traffic interior offices, break rooms, storage	Not suitable for high-traffic; slower cycle time
Electromechanical Panic Hardware	Panic bar/exit device with electric latch retraction or dogging	Fire egress doors requiring access control on approach side	Free egress requirements should be reviewed for the opening, occupancy, hardware type, local code, and AHJ interpretation

⚠ Electrified hardware on fire-rated openings should be reviewed for listing, door rating, egress, fire alarm interface, and AHJ requirements before specification or installation. Improper hardware selection or installation can create life-safety, inspection, warranty, or code issues. Confirm requirements with the AHJ and qualified code professionals before finalizing hardware.

Fail-Safe vs. Fail-Secure Locks

The fail-safe versus fail-secure decision is one of the most consequential hardware choices in access control design, and it is one of the most frequently misunderstood by organizations specifying their first system. Getting this wrong can result in life safety violations, fire code failures, regulatory findings, or — in the opposite direction — an unlocked building during a power outage when you need it most secured. The decision must be made door-by-door, not as a blanket policy.

A **fail-safe** lock releases when power is removed. Fail-safe behavior may be required or expected for certain controlled openings depending on egress requirements, hardware type, occupancy, local code, and AHJ interpretation. A **fail-secure** lock remains locked when power is removed. This behavior is appropriate for high-security areas where maintaining containment during a power failure is more important than convenience — and should not be applied to required egress paths without qualified life-safety review and AHJ approval where required.

Characteristic	Fail-Safe	Fail-Secure	Design Implication
Power loss behavior	Door unlocks / opens freely	Door remains locked	Determines backup power requirements
Life safety egress	Often required or expected on egress paths; verify by opening and AHJ	Generally not appropriate on required egress paths without qualified review and approval	Verify AHJ and applicable life-safety requirements
Fire alarm integration	Often required depending on hardware, code, and AHJ review	May require fire alarm release or shunt wiring depending on hardware, occupancy, and AHJ review	Fire alarm interface may be required depending on hardware, occupancy, and AHJ
Security posture during outage	Lower — door is accessible	Higher — door stays locked	Backup power should be evaluated for critical openings
Typical applications	Main entrances, stairwells, lobby doors, corridors	Server rooms, vaults, pharmacies, evidence rooms	Zone classification drives selection
ADA compliance impact	Door opens freely — no ADA issue	May require power assist or accessible hardware depending on ADA and project requirements	Plan for ADA operator integration
Battery backup requirement	May be needed to maintain access control during outages	Intrinsic during outage — but consider access needs	Plan backup power for critical panels and openings where needed

⊗ Fail-secure hardware should not be applied to required egress paths without qualified code review, life-safety review, and AHJ approval where required. Egress requirements vary by opening, occupancy, hardware type, local code, and AHJ interpretation.

Hardware Durability, Duty Cycle & High-Traffic Openings

Not all electrified door hardware is rated for the same volume of cycles. A device rated for 100,000 actuations per year installed on a door that sees 500,000 actuations annually will fail prematurely, generate service calls, and ultimately cost more than specifying the correct hardware at the outset. Duty cycle is a specification that appears in hardware datasheets but is rarely discussed in sales conversations — which means it falls on the facility team and the access control designer to enforce it during specification review.

High-traffic openings include main building entrances, lobby turnstile bypass lanes, cafeteria access points, hospital corridor doors, and any door used by shift workers during peak entry and exit windows. These openings often require higher-duty hardware with high-cycle ratings, robust latch mechanisms, and — in many cases — door closers and openers that can handle the mechanical stress of continuous operation. The access control panel powering these openings should also be sized with appropriate power supplies and surge protection to handle the higher switching frequency.

Opening Classification	Annual Cycles (Est.)	Recommended Hardware Grade	Typical Maintenance Consideration
High-Traffic (Main Entrance, Cafeteria, Lobby)	250,000 – 1,000,000+	ANSI Grade 1 commercial, heavy-duty rated	Often quarterly for high-use openings when in scope
Medium-Traffic (Office Suite, Break Room)	50,000 – 250,000	ANSI Grade 1 commercial	Often semi-annual when in scope
Low-Traffic (Server Room, Storage, Executive)	Under 50,000	ANSI Grade 1 or 2	Often annual when in scope
Exterior High-Security (Loading Dock, Gate)	Variable — weather-rated required	NEMA 4X-rated, heavy-duty commercial	Often quarterly/environmental inspection when in scope
Hazardous Environment (Industrial, Chemical)	Variable	Corrosion-resistant, explosion-proof where required	Review facility, OSHA, safety, and manufacturer requirements

Access control should be designed around peak traffic, not only average traffic. A lobby door that processes 400 employees in a 15-minute window during shift change requires hardware and reader throughput specifications that match the peak demand scenario, not the average daily count.

Lock Speed, Reader Speed & Turnstile Throughput

Throughput — the rate at which people can move through a controlled opening — is a critical design parameter that is systematically underweighted in access control specifications. When throughput is insufficient for actual peak traffic, the results are predictable: queues form, tailgating increases, employees prop doors open, and the security value of the system is negated by behavioral workarounds. Engineering for throughput requires analyzing the entire transaction chain from credential presentation to door clear.

The total throughput time for a single access transaction includes: reader read time (credential decode and panel query response), panel decision time (rule evaluation and relay trigger), lock release time (electromechanical actuation), door open time (manual swing or automatic operator), and door clear-and-relock time. Each element contributes to the end-to-end transaction time, and small delays compound into significant queuing effects at high-volume openings.

Component	Typical Performance Range	Higher-Performance / Design Consideration	Design Note
125 kHz Prox Card Reader	300–500ms read time	Generally not preferred for high-throughput applications	Legacy technology; limited to low-traffic
13.56 MHz Smart Card / HID iCLASS SE	100–200ms read time	Common choice for many commercial deployments	Supports OSDP; encrypted comms
Mobile Credential (BLE/NFC)	150–400ms depending on device and app state	Tap-to-go NFC: ~150ms	Phone wake state affects performance
Biometric (Fingerprint)	500ms – 2 seconds	Often poorly suited for primary high-throughput openings	Often poorly suited for primary high-throughput openings
Magnetic Lock Release	10–50ms electrical; mechanical sound ~100ms	Fast release; door swing time still affects throughput	Door closer speed affects throughput
Electric Strike Release	20–80ms	Can be fast; performance depends on latch tension and door condition	Latch tension must be maintained
Optical Turnstile (Speed Gate)	25–40 persons/minute per lane	35–40 persons/minute with mobile credentials	Evaluate lane count against peak traffic volume, credential type, staffing, and acceptable queue time
Full-Height Turnstile	15–25 persons/minute per lane	Common for secured perimeter applications	Lower throughput; higher security containment
Waist-High Turnstile (Tripod)	20–30 persons/minute per lane	Common in industrial and transit-style applications	Accessible route should be reviewed separately

Turnstiles, Speed Gates & Controlled Entrance Solutions

Turnstiles and speed gates can provide a higher-integrity form of pedestrian entry control when properly selected, monitored, and integrated. Unlike a card reader on a door — where tailgating and piggybacking are constant vulnerabilities — a properly specified turnstile can reduce unauthorized entry, tailgating, and piggybacking when paired with the right monitoring and operating procedures. For organizations managing high employee counts, visitor flows, or regulatory audit requirements, turnstile-based entry control delivers a fundamentally different security posture than door-based access alone.

Selecting the right turnstile type requires evaluating security requirements, throughput demand, architectural constraints, ADA compliance obligations, and aesthetic considerations. The range of available solutions spans from decorative optical speed gates in Class-A office lobbies to full-height anti-climb turnstiles at industrial perimeter fences. Each type offers a different combination of security level, throughput capacity, and physical footprint.

Turnstile Type	Security Level	Throughput	Best Application	ADA Path
Optical Speed Gate (Flap Barrier)	Medium — detection-based, not physical barrier	30–40 ppm	Corporate lobby, financial, healthcare main entrance	Accessible path should be reviewed; adjacent ADA lane may be required
Waist-High Tripod Turnstile	Medium — physical arm barrier	20–30 ppm	Industrial sites, transit, construction	Accessible path should be reviewed; adjacent ADA lane may be required
Waist-High Optical Turnstile	Medium-High — glass panel barrier	25–35 ppm	Class A office, corporate HQ, multi-tenant lobby	Accessible path should be reviewed; adjacent ADA lane may be required
Full-Height Turnstile (Rotor)	High — complete physical enclosure	15–25 ppm	Industrial perimeter, utilities, correctional, stadiums	Accessible path should be reviewed; adjacent ADA gate may be required
Mantrap / Security Airlock Vestibule	Very High — one person at a time, anti-tailgate	4–8 ppm	Data centers, server rooms, high-security entries	Separate ADA consideration
ADA Swing Gate (Adjacent Lane)	Low-Medium — must be monitored	Per staff availability	Accessible companion lane to any turnstile configuration	Often used as accessible companion path; review monitoring and egress needs

Turnstile projects should include an accessible path of travel and should be reviewed for ADA, egress, staffing, monitoring, and AHJ requirements. Adjacent swing gates or bypass lanes may require monitoring, video, staffing, or alarm workflows so they do not become uncontrolled entry points.

Credentials: Cards, Fobs, Mobile, PINs, Biometrics & Smart Cards

The credential is the identity assertion layer of the access control system — it is how the system knows who is requesting access. Credential technology has evolved dramatically over the past two decades, from proximity cards that broadcast an unencrypted ID number to sophisticated smart card platforms supporting mutual authentication, encrypted data exchange, digital certificates, and converged physical-logical access. Understanding the security architecture, interoperability implications, and operational tradeoffs of each credential type is essential for making a selection that will remain viable over the system's lifecycle.

Credential Type	Technology	Security Level	Best Use Cases	Key Limitations
125 kHz Proximity Card/Fob	EM4100, HID Prox	Low — unencrypted, cloneable	Legacy use only; stronger options are generally preferred for new deployments	Limited security; widely understood cloning risk
13.56 MHz Smart Card (MIFARE Classic)	ISO 14443A	Medium — some encryption, but known vulnerabilities	Upgrade from 125 kHz; still widely deployed	MIFARE Classic has known cracking exploits
13.56 MHz Smart Card (DESFire EV3)	ISO 14443A, AES-128	High — mutual auth, AES encrypted	Enterprise, healthcare, government, financial	Higher per-card cost; requires compatible readers
HID iCLASS SE / Seos	13.56 MHz, SIO-encrypted	Very High — SIO protocol, diversified keys	Government, enterprise, high-security environments	Proprietary ecosystem; reader compatibility required
Mobile Credential (BLE/NFC)	Bluetooth LE, NFC on smartphone	High — device-bound, certificate-backed	Modern corporate, multi-tenant, healthcare	Phone battery/wake state dependency
PIN Keypad	Wiegand or OSDP output	Low-Medium — shareable, observable	Secondary factor, low-security interior, IT rooms	PINs shared; shoulder surfing; no unique identity
Multi-Factor (Card + PIN)	Combined reader	High	Server rooms, pharmacies, regulated zones	Slower throughput; user friction
Fingerprint Biometric	Capacitive or optical sensor	Very High — user-unique	High-security rooms, time-attendance	Biometric privacy, consent, retention, and hygiene considerations may apply
Facial Recognition	Camera + AI processing	Very High — touchless	Touchless entry, VIP identification	Privacy, consent, retention, and jurisdiction-specific requirements may apply
Smart Card (PIV/CAC)	Contact/contactless PKI	Government-grade	Federal, defense, HSPD-12 environments	Requires full PKI infrastructure

⚠ Biometric credentials — including fingerprint, facial recognition, and iris scanning — may trigger biometric privacy, employee privacy, consent, retention, deletion, and notice requirements depending on jurisdiction and use case. Organizations should consult legal counsel and establish appropriate policies before deploying biometric access control.

HID, Smart Credentials & Converged Credentials

HID is one of the most widely used credential and reader ecosystems in North American commercial access control. Understanding HID's credential portfolio — and the concept of converged credentials — is important context for any organization making a medium-to-long-term access control investment. HID's Seos credential platform, delivered via smart cards or mobile devices using their Origo cloud provisioning infrastructure, represents one of the leading modern approaches to commercial credential technology: device-bound, cryptographically diversified, and capable of supporting both physical access and logical (IT) access from a single credential.

Converged credentials — also called converged physical and logical access — can allow the same smart card or mobile credential used for door access to also support logical access use cases such as workstation, VPN, or application authentication when the technology stack is designed for that purpose. This convergence can reduce the friction of separate physical and logical identity systems, help reduce orphaned-credential risk, and simplify reviews where organizations need to demonstrate that terminated users are removed from both physical and logical access systems. For healthcare, financial, government, and regulated environments where unified identity governance is required or desired, converged access can simplify administration and reduce the risk of orphaned credentials.

HID Proximity (Legacy)

125 kHz, unencrypted. Still widely deployed but cloneable. Migration to 13.56 MHz is recommended where stronger credential options are practical. BTI generally recommends against new 125 kHz proximity deployments.

HID iCLASS SE

13.56 MHz, SIO-encrypted. Significant security improvement over proximity. Widely supported across major platform hardware. Common recommendation for many enterprise retrofit projects where compatible with the platform and budget.

HID Seos

The current HID flagship. Supports smart card and mobile delivery. Device-bound cryptography, Origo cloud provisioning, and PACS integration. Often recommended for new enterprise deployments where compatible with the client's platform, security requirements, and budget.

HID Mobile Access

Delivers Seos credentials to iOS and Android via BLE and NFC. Supports tap, twist-and-go, and hands-free modes. Can reduce card issuance overhead in appropriate environments.

Converged Physical + Logical

One credential for door access and workstation/VPN login. A strong fit for healthcare, financial, government, and regulated environments where unified identity governance is required or desired.

Cloud Access Control vs. On-Premises Access Control

The architecture of the access control platform — cloud-hosted versus on-premises — is one of the most significant decisions in system design, with long-term implications for cost structure, IT staffing requirements, software update cadence, integration flexibility, and resilience during internet outages. The market has shifted substantially toward cloud-native platforms over the past five years, driven by lower upfront costs, subscription-based economics, automatic software updates, and the dramatic improvement in cloud platform feature parity with legacy enterprise systems. However, on-premises solutions retain important advantages in specific environments — particularly those with stringent data sovereignty requirements, low-bandwidth connectivity, or complex enterprise integrations.

Dimension	Cloud Access Control	On-Premises Access Control
Upfront Cost	Lower — hardware-light, subscription-based	Higher — server, software licenses, installation
Total Cost of Ownership (5 yr)	Subscription accumulates; lower IT labor	Higher upfront; lower ongoing if IT staff exists
Software Updates	Automatic, vendor-managed, continuous delivery	Manual, IT-managed, periodic release cycles
IT Staffing Requirement	Minimal — vendor manages infrastructure	Significant — requires server admin, patching, backup
Offline Resilience	Panels operate locally; management console offline	Full local operation; no internet dependency
Data Sovereignty	Data in vendor cloud; review DPA and regional storage	Data can remain on-site depending on architecture and configuration
Integration Flexibility	API-driven; vendor ecosystem partnerships	Broader enterprise integration; on-prem API access
Multi-Site Scalability	Strong fit for multi-site administration and distributed locations	Requires replication architecture; more complex
Video Integration	Strong in Avigilon Alta, Brivo, Alarm.com for Business; Axis and Avigilon integrations	Deep integration with Avigilon Unity / ACM, Software House, Kantech, Milestone (video platform)
Compliance & Audit Logging	Vendor-managed retention; verify contract terms	Organization controls all retention policies
Recommended For	SMB to mid-market, multi-site distributed, low IT overhead	Enterprise, government, healthcare, high-security

BTI designs and deploys cloud, on-premises, and hybrid access control architectures across our supported platform ecosystem — Kantech, Software House, Avigilon Alta, Avigilon Unity / ACM, Brivo, RS2 / ACRE, Alarm.com for Business, and YourSix. The right choice depends on your IT staffing model, compliance or documentation needs, connectivity profile, supported integrations, budget, and long-term service model.

BTI-Supported Access Control Platforms & Ecosystems

BTI designs, installs, supports, and maintains access control systems around platforms and hardware ecosystems we can responsibly deploy, document, and service long term. Our supported ecosystem includes Kantech, Software House, Avigilon Alta, Avigilon Unity / ACM, Brivo, RS2 / ACRE, Alarm.com for Business, YourSix, HID credential technologies, Axis and Avigilon video integrations, 2N and Aiphone intercom workflows, and major commercial locking hardware manufacturers.

The goal is not to list every access control product in the market. The goal is to help buyers choose from platforms and ecosystems BTI can responsibly design, install, integrate, document, and support over time.

Primary Access Control Platforms

Platform	Best Fit	Strengths	BTI Design Notes
Kantech	Commercial, industrial, healthcare, office, multi-site	Mature platform, strong dealer ecosystem, proven scalability	BTI is a Global Certified Kantech vendor. Primary platform for commercial, healthcare, industrial, and multi-site access control.
Software House	Enterprise, healthcare, industrial, government-adjacent, complex multi-site	Enterprise-grade architecture, strong integration capability, mature workflows	Best for environments requiring advanced workflows, mature architecture, and long-term governance.
Avigilon Alta	Cloud access control, mobile-first, distributed offices, multi-site	Cloud management, mobile credentials, modern UX, strong video ecosystem fit	Strong cloud option for mobile-first access, distributed sites, and simplified remote administration.
Avigilon Unity / ACM	Avigilon video environments, enterprise physical security, healthcare, industrial, campus	Strong Avigilon video alignment, centralized security ops, enterprise-controlled workflows	Strong fit where Avigilon video and access control standardization are important.
Brivo	Commercial offices, multi-site, property managers, remote admin	Cloud management, mobile credentials, simple administration, multi-site support	Good fit for organizations prioritizing cloud management, remote administration, and mobile credentials.
RS2 / ACRE	Commercial, industrial, healthcare, education, enterprise-style	Platform flexibility, open architecture, scalable design	Supported for clients requiring flexible architecture, open options, and long-term serviceability.
Alarm.com for Business	Small to mid-sized commercial, multi-location, intrusion/access/video	Unified security platform, remote management, intrusion/video/access ecosystem	Good fit where access control, intrusion, video, and remote management should be unified under one platform.
YourSix	Commercial environments requiring unified cloud video surveillance, access control, and AI-driven security operations	Cloud-managed video + access control, AI analytics, remote monitoring, unified security operations platform	Supported as a unified cloud security platform where video surveillance, access control, and AI-driven monitoring should operate under a single management environment.

BTI recommends platforms based on fit, supportability, integration needs, lifecycle requirements, and the systems BTI can responsibly deploy and maintain. See the following page for BTI's supported credential, intercom, video, and door hardware ecosystems.

BTI-Supported Credentials, Intercoms, Video & Door Hardware Ecosystems

The following ecosystems support BTI access control deployments across credential design, video verification, door communication, and physical locking hardware.

Credentials, Intercoms, Video & Door Hardware

Ecosystem	Role in Access Control Design	BTI Design Notes
HID	Credential and reader technology: HID Signo readers, HID Seos smart cards, HID Mobile Access (BLE/NFC), iCLASS SE, and converged physical + logical credentials	Preferred credential and reader ecosystem for secure modern credential design, including HID Signo, HID Seos, HID Mobile Access, smart cards, and converged credentials.
Axis	Video verification, door stations, intercoms, and network security device integrations	Key ecosystem for video verification, door stations, intercoms, and access-control-adjacent network security integrations.
Avigilon Video	Video verification and security operations, especially where Avigilon access control or camera standardization is important	Strong video verification and security operations ecosystem, especially where Avigilon access control or camera standardization is important.
2N / Aiphone	Video intercoms, door stations, gate communication, visitor entry, and remote door-release workflows	Use when access control must integrate with lobby, gate, visitor, video intercom, or remote door-release workflows.
Commercial Door Hardware Ecosystem	Electric strikes, maglocks, electrified panic hardware, door closers, power supplies, hinges, transfer hardware, and locksets — the physical layer that makes access control reliable, code-compliant, and serviceable	ASSA ABLOY, Allegion, HES, Adams Rite, Securitron, Schlage, Von Duprin, LCN, Camden, RCI, SDC, Dormakaba, and BEST. The door hardware ecosystem is what makes the access control system physically reliable, code-aware, and serviceable.

Platform Selection Criteria

Door Count & Scalability

Does the platform support your current door count and five-year growth projection without architecture changes or cost cliffs?

Hardware Openness

Is the controller hardware open (Mercury-based) or proprietary? Open hardware can help preserve flexibility if your organization changes software platforms later.

Integration Ecosystem

Can the platform integrate with your HR system, video surveillance, visitor management, SIEM, and IT identity providers?

Compliance & Audit Support

Can the platform produce the reports, access logs, and role-based access reviews your organization may need for internal, audit, insurance, or compliance reviews?

Access Control Integrations

Modern access control systems do not operate in isolation. Their full strategic value is realized when they are integrated with adjacent systems — video surveillance, IT identity providers, HR platforms, visitor management, intrusion detection, building automation, and cybersecurity tools. Each integration extends the system's ability to enforce policy, investigate incidents, demonstrate compliance, and reduce operational friction. Designing for integration from the outset — rather than attempting to bolt integrations on post-installation — is essential for maximizing long-term return on investment.

Integration Type	Function	Example Systems / Integration Paths	Business Value
Video Surveillance (VMS)	Correlate access events with camera footage; auto-pull clip on door event	Avigilon video, Axis cameras and intercoms, Milestone video integration where applicable	Faster incident investigation; evidence support when retained
HR / Identity Provisioning	Auto-provision and de-provision credentials from HR system on hire/termination	Active Directory, Workday, BambooHR, SAP	Can reduce orphaned-credential risk and administrative burden
Visitor Management System (VMS)	Pre-register visitors; issue time-limited credentials; log visit records	Envoy, Traction Guest, Proxyclick	Reception efficiency; visitor records when retained
Intercom / Video Intercom	Remote door release from reception or mobile device; visitor audio/video verification	2N, Aiphone, Axis door stations	Remote entry workflow; video verification when configured
Intrusion Alarm / IDS	Arm/disarm alarm partitions via access event; correlate door events with alarm zones	Bosch, DSC, Napco, DMP	Unified security monitoring; may reduce false alarms
SIEM / Security Operations	Forward access event logs to SIEM for correlation with IT security events	Splunk, Microsoft Sentinel, IBM QRadar	Physical-logical event correlation when in scope
Building Automation (BAS/BMS)	Trigger HVAC, lighting, or elevator on first-person-in access event	BACnet, Modbus, KNX, Niagara Framework	Potential energy efficiency and operational automation
Parking / Vehicle Gate	Unified credential for pedestrian and vehicle entry; LPR integration	Kantech, Software House, Avigilon, gate operators, LPR, and vehicle credential integrations where applicable	Unified credential workflow; reporting continuity when configured
Elevator Control	Credential-based floor access; fire recall integration	ThyssenKrupp, Otis, Schindler, KONE via relay	Floor-level permissions and secured-area reporting
Time & Attendance	Use access events as time-punch records; integrate with payroll systems	Kronos/UKG, ADP, Paychex via API	May reduce duplicate systems where time and attendance integration is appropriate

Related BTI Resource
Access control often works best when it is planned together with video surveillance, intercoms, intrusion alarms, and network infrastructure. BTI helps organizations evaluate these systems as part of a broader commercial security environment.

Explore BTI Commercial Security Solutions

Converged Security: Physical, IT, Cybersecurity, VoIP & Compliance

The traditional boundary between physical security and IT security has become increasingly blurred. Access control systems are network-connected devices running embedded operating systems, communicating via IP protocols, managed through web interfaces, and integrated with cloud services. This means many access control deployments should be treated as both physical security and cybersecurity projects. Organizations that treat it as only one or the other may miss risks that should be considered during design, implementation, and support planning.

BTI Communications Group's converged security approach can align access control, video surveillance, alarms, intercoms, VoIP, IT network infrastructure, and cybersecurity hardening as part of a coordinated project scope. This is not a marketing position — it reflects the technical reality that an access control controller on your network is a network device that should be considered for security hygiene appropriate to networked endpoints: firmware updates, certificate management, VLAN segmentation, encrypted communications, and monitored logging.

Physical Security

Access control, video surveillance, intrusion detection, turnstiles, and perimeter protection designed as an integrated physical security envelope.

IT Infrastructure

PoE switching, VLAN segmentation, fiber backbone, UPS, and structured cabling designed to support security system reliability and network performance simultaneously.

Cybersecurity Hardening

Controller firmware planning, encrypted OSDP communications where supported, TLS certificate considerations, network segmentation, and SIEM integration when in scope.

VoIP & Intercoms

IP intercom, video intercom, and VoIP integration with access control for remote door release, visitor verification, and emergency communications across the facility.

Compliance-Supporting Documentation

Access logs, audit reports, role-based access reviews, and compliance-supporting evidence can be configured, exported, and maintained when required by the client's scope, service agreement, and applicable compliance program.

BTI recommends platforms and hardware ecosystems we can responsibly design, install, document, and support within the agreed project scope. Our supported access control ecosystem includes Kantech, Software House, Avigilon Alta, Avigilon Unity / ACM, Brivo, RS2 / ACRE, Alarm.com for Business, YourSix, HID, Axis, 2N, Aiphone, and major commercial door hardware manufacturers.

Related BTI Resource

For organizations that need access control to connect with IT infrastructure, cybersecurity, VoIP, compliance-supporting documentation, and managed support, BTI can help evaluate the broader business technology environment when those needs are part of the project scope.

Explore BTI Managed IT and Cybersecurity Services

Access Control Compliance, Privacy & Regulatory Design Considerations

Regulated industries may have access control design considerations that go beyond general physical security best practices. Healthcare, financial services, government contractors, logistics, food production, technology companies, and other regulated organizations may need access control systems to support physical safeguards, visitor controls, access reviews, log retention, privacy requirements, and cyber insurance documentation. These requirements vary by organization, location, system design, and legal/regulatory context.

Regulation / Framework	Industry	Access Control Design Considerations	Potential Evidence / Configuration Considerations
HIPAA Security Rule	Healthcare	Physical safeguards, facility access controls, workstation-area safeguards, visitor controls	Restricted-area access logs, visitor records, access policies, access reviews, and records that may support audits, investigations, legal reviews, or insurance requests when retained and managed appropriately
42 CFR Part 2	Substance use disorder treatment / behavioral health	Restricted access to areas where Part 2 records, systems, or workstations may be accessed	Role-based access groups, visitor records, workstation-area controls, badge deactivation records, and access approvals where required by the organization's Part 2 program
PCI DSS v4.0	Financial, Retail	Physical access to cardholder data environments, visitor controls, timely credential deactivation	CDE-area door logs, visitor records, access reviews, badge deactivation records, and retained reports where applicable
SOC 2 / AICPA Trust Services	SaaS, data centers, MSPs, technology, service organizations	Facility access controls, visitor records, restricted-area access, incident support, access reviews	Server room logs, visitor logs, termination evidence, access review records, and incident documentation when in audit scope
CMMC / NIST 800-171	Defense Contractors	Physical access controls on CUI environments, visitor escort, access logging	Strong access controls, visitor escort processes, restricted-area logs, and documented reviews where required by the CMMC/NIST scope
SOX (Sarbanes-Oxley)	Public Companies	IT general controls, physical access to financial systems, segregation of duties	Access logs on server rooms, separation between IT and finance physical access
Cyber Insurance	All industries seeking or renewing cyber liability coverage	Insurers may ask about MFA, logging, physical safeguards, visitor controls, and protection of IT/server areas	Server room access logs, visitor records, badge deactivation records, access review reports, and incident records when requested by insurer or broker

Additional Privacy, Life-Safety & Industry Design Considerations

The following frameworks and requirements may apply depending on industry, geography, credential type, and system design. Organizations should review applicable requirements with qualified legal, compliance, code, and AHJ advisors before deploying biometrics, visitor management systems, or regulated access control workflows.

Regulation / Framework	Industry	Access Control Design Considerations	Potential Evidence / Configuration Considerations
Illinois BIPA	Employers in Illinois using biometrics	Written consent, retention schedule, disclosure, deletion rights	Notice, consent, retention, disclosure, deletion, and litigation-risk considerations; written consent program and documented retention/destruction policy before deploying biometrics
California CCPA/CPRA	Businesses subject to CCPA in California	Biometric data as sensitive personal information, opt-out and deletion rights	Biometric data governance program, privacy notice, deletion capability
Employment / HR Privacy	Employers using badges, biometrics, mobile credentials, or access analytics	Access logs may become employee activity records; biometric workflows may require notices, policies, retention limits, and consent	Employee notices, biometric consent records, access log retention policy, HR approval workflow, and deletion records where applicable
NFPA 101 Life Safety Code	All occupied commercial buildings	Egress, delayed egress rules, fire alarm interface for mag locks	Code-compliant egress, fire alarm interface review, AHJ coordination, and life-safety documentation where applicable
DEA 21 CFR Part 1301	Healthcare, Pharma	Controlled storage and access for certain regulated substances	Individual credential assignment, access records, and controlled-area controls where required by applicable DEA and organizational requirements
FDA FSMA / Food Defense	Food manufacturing, processing, distribution	Controlled access to vulnerable areas, production zones, chemical storage, ingredient storage	Restricted-area access records, visitor/vendor logs, food defense area controls, and access group reviews where applicable
Logistics / TSA / Chain-of-Custody	Logistics, air cargo, freight, distribution	Controlled access to secure cargo areas, screening areas, yards, docks	Secure-area access logs, visitor/vendor logs, employee authorization records, and chain-of-custody support documentation where applicable

In regulated environments, access control is not only a security system. It can also be an evidence system. Access logs, user provisioning records, access review reports, and hardware maintenance logs are records that may support audits, investigations, legal reviews, or insurance requests when retained and managed appropriately.

Educational Disclaimer

This guide is for educational purposes only and is not legal, regulatory, compliance, insurance, code, or audit advice. Organizations should consult qualified legal, compliance, insurance, audit, code, and AHJ advisors before deploying biometrics, facial recognition, employee access analytics, visitor management systems, regulated access control workflows, or formal compliance evidence programs.

Access Control Evidence: What the System Can Produce When in Scope

A well-designed and properly maintained access control system can produce useful evidence for audits, insurance reviews, internal investigations, and security reviews when the system is configured, retained, and documented for that purpose. Evidence outputs depend on the platform, retention settings, integrations, service agreement, and the client's compliance program.

Compliance Evidence Type	What the Access Control System Produces	Commonly Relevant Frameworks / Reviews
Access Event Log	Time-stamped record of every door transaction when logging is enabled and retained: user, door, direction, credential presented, grant/deny result	HIPAA, PCI DSS, SOX, CMMC, DEA
User Provisioning Record	When each credential was issued, to whom, by which administrator, with which access rights when provisioning records are maintained	SOX, PCI DSS, HIPAA, CMMC
Access Review Report	Periodic report of users and access rights when reviews are configured; may support internal, audit, insurance, or compliance reviews depending on scope	PCI DSS, SOX, CMMC, HIPAA Security Rule
Terminated User Revocation Record	Timestamp or record of when credentials were disabled when revocation records are retained; may be correlated with HR termination date where applicable	PCI DSS, HIPAA, SOX, internal access governance
Visitor Log	Visitor name, host, purpose, entry time, exit time, badge number issued and returned when visitor records are maintained	PCI DSS, HIPAA, CMMC, DEA
Failed Access Attempts Report	Aggregated denied entry events by user, door, or time window when failed-attempt reporting is configured; flags anomalous patterns	HIPAA, CMMC, SOC 2
Forced/Propped Door Alarm Log	Record of all door forced or held open events with timestamp and door identity when alarm logging is enabled	HIPAA, PCI DSS, CMMC
Hardware Maintenance Record	Scheduled inspection dates, findings, repairs, firmware updates — may support review of physical safeguard maintenance when maintenance records are retained	HIPAA Security Rule, PCI DSS Req. 9
Video Correlation Record	Access events linked to video clips confirming physical presence match when video integrations are in scope; supports incident investigation	PCI DSS, HIPAA, investigations, legal reviews, or insurance requests where applicable

Licensed Access Control Installation, National Deployments & Select International Support

Access control, low-voltage, alarm, electrical, locksmith, and door hardware work may require different licenses, permits, or approvals depending on the state, city, country, project scope, and authority having jurisdiction. BTI directly serves California, Illinois, and Arizona and can provide license and insurance documentation during the proposal process. For national deployments, BTI coordinates with properly licensed local contractors, subcontractors, and project partners where required. For select international projects, BTI can support planning, standardization, manufacturer coordination, and deployment oversight when local regulations, product availability, and qualified in-country resources allow.

California

Access control, alarm, and related low-voltage work in California may fall under BSIS, CSLB, local permit, AHJ, or other requirements depending on project scope. BTI can provide applicable California license and insurance documentation during the proposal process.

Illinois

Access control, alarm, locksmith, and related electronic security work in Illinois may fall under IDFPR and other state or local requirements depending on project scope. BTI can provide applicable Illinois license and insurance documentation during the proposal process.

Arizona

Access control, alarm, low-voltage, and related security work in Arizona may involve Arizona ROC, DPS, local permitting, AHJ, or other requirements depending on project scope. BTI can provide applicable Arizona license and insurance documentation during the proposal process.

National Multi-Site Deployments

BTI supports national access control, video, intercom, and physical security deployments by coordinating standardized design, manufacturer selection, documentation expectations, project management, and qualified local installation resources. Licensing, permits, labor, inspections, and authority-having-jurisdiction requirements are handled according to the rules of each project location.

Select International Deployments

For select international projects, BTI can assist with access control planning, manufacturer coordination, remote technical support, deployment standards, and project oversight. International work depends on product availability, local regulations, site conditions, qualified in-country installation resources, and client-specific requirements.

BTI Communications Group directly serves California, Illinois, and Arizona and can provide applicable license and insurance documentation during the proposal process. For national and select international deployments, BTI coordinates with properly licensed local contractors and project partners where required. License, insurance, and subcontractor documentation can be reviewed as part of project scoping and proposal development.

The Access Control Site Survey: What BTI Reviews Before Quoting

An access control quote produced without a comprehensive site survey is usually an estimate built on assumptions and may increase the risk of change orders, surprises, and cost overruns. BTI typically conducts a site survey or structured discovery process before producing a detailed access control proposal, depending on project type and scope. The survey produces the door-by-door hardware specifications, infrastructure requirements, network design parameters, power supply sizing, life safety integration requirements, and labor estimates that form the foundation of an accurate, executable project scope.

The site survey is also the point at which existing conditions are documented — including legacy wiring that cannot be reused, door frames that require modification, fire-rated openings that require specific hardware, and network infrastructure that needs to be upgraded to support the new system. Identifying these conditions before project kickoff prevents the budget surprises that erode trust between installation partner and client.

Survey Category	What BTI Assesses	Why It Matters
Door Inventory & Classification	Count, type, material, frame, current hardware, fire rating, life safety status of every opening	Drives hardware specification and compliance review
Traffic Volume Analysis	Peak and average daily throughput per opening; shift change volumes; visitor volumes	Determines hardware grade, reader type, turnstile sizing
Network Infrastructure	Existing switch capacity, PoE budget, VLAN configuration, cable plant condition, panel locations	Determines network upgrade requirements and cabling scope
Power Infrastructure	Panel locations, available circuits, UPS status, conduit routing feasibility	Sizes power supplies; identifies backup power gaps
Fire Alarm Integration Points	FACP manufacturer, panel location, relay availability, zone mapping for mag lock shunt wiring	Supports review of fail-safe, fire alarm, and AHJ requirements
Existing Access Control System	Platform, age, firmware version, credential technology, panel hardware, integration state	Determines migration path vs. full replacement
Video Surveillance Infrastructure	Existing VMS platform, camera coverage gaps, integration capability with access control platform	Enables video-access event correlation design
Compliance Requirements	Applicable regulations, existing audit findings, documentation requirements, credential governance needs	Shapes system design, reporting configuration, and documentation deliverables
IT Security Requirements	Network segmentation policies, certificate requirements, SIEM integration needs, encryption standards	Supports cybersecurity hardening recommendations when in scope
Intercom & VoIP Integration	Existing intercom system, reception workflow, remote door release requirements, visitor management workflow	Determines intercom and VoIP integration scope

Related BTI Resource
If your organization is planning a broader security upgrade, BTI's Business Security Systems page provides an overview of access control, video surveillance, alarms, intercoms, and related physical security services.
Explore BTI Business Security Systems

Installation Quality, Documentation & Closeout Standards

The quality of an access control installation is measured not only by whether the system functions on day one, but also by whether the agreed documentation, labeling, and handoff materials support ongoing management, future expansion, compliance-supporting records, and serviceability. BTI's installation standards are driven by this principle. BTI defines closeout documentation requirements during project scoping. For projects where documentation is included, BTI provides the agreed closeout materials needed to support serviceability, future expansion, internal administration, and compliance-supporting records.

Documentation-driven delivery is a core differentiator for BTI. In regulated, insurance, legal, or operational contexts, access control installation documentation may support evidence, review, serviceability, and future expansion when included in scope and properly retained. In a future expansion project, it can reduce the need for expensive re-surveying and reverse-engineering.

Potential Closeout Deliverable When in Scope	Description	Format
As-Built Wiring Diagrams	Complete panel wiring documentation as actually installed, including all door hardware, reader, REX, and DPS connections	PDF + AutoCAD/Visio
Panel and Equipment Location Drawing	Floor plan showing location of all access control panels, power supplies, and network equipment	PDF floor plan markup
Door Hardware Schedule	Door-by-door record of installed hardware: lock type, reader model, REX type, credential type, access group assignment	Excel / PDF
Network Documentation	IP address assignments, VLAN configurations, switch port assignments for all access control devices	Excel / PDF
Access Control Platform Configuration Backup	Full system configuration export; credential database backup; system settings documentation	Encrypted digital file + print summary
User Administration Guide	Step-by-step procedures for adding/removing users, managing access groups, running reports	PDF / printed binder
Compliance Documentation Package	Access log retention configuration, audit report templates, and user review procedure documentation — when compliance documentation is included in the project scope or service agreement	PDF compliance folder
Warranty and Service Contacts	Manufacturer warranty terms for all installed hardware; BTI service contact information and SLA summary	PDF
Training Sign-Off Record	Signed acknowledgment from system administrator confirming platform administration training completed	Signed PDF form

Service, Maintenance & Lifecycle Management

An access control system is not a set-and-forget installation. Like all technology infrastructure, it may require ongoing firmware and software updates, periodic hardware inspection and testing, credential database hygiene, and proactive lifecycle planning to maintain security effectiveness and compliance posture over time — depending on platform, risk level, environment, and service agreement. Organizations that treat access control as a one-time capital expenditure with no recurring service planning often face avoidable risks such as worn hardware, outdated firmware, and stale credentials.

BTI can provide managed service agreements for access control lifecycle management when ongoing support is included in the client's service plan. Depending on scope, these agreements may include hardware inspections, firmware coordination, access review support, documentation updates, and technology refresh planning.

Potential Maintenance Activity	Typical Frequency When in Scope	Scope	Operational / Compliance Considerations
Door Hardware Inspection	Quarterly (high-traffic); Semi-annual (medium); Annual (low)	Lock function test, latch tension, door closer adjustment, REX test, DPS test	HIPAA Security Rule; PCI DSS Req. 9
Panel Firmware Updates	Per vendor release; minimum annual	Review release notes, test in staging, deploy with rollback plan	CMMC, SOC 2, cybersecurity hardening
Platform Software Updates	Per vendor release schedule	Version upgrade, database backup, configuration verification	Regulated environments where applicable
Credential Database Audit	Quarterly	Identify and disable orphaned credentials; compare with HR active roster	PCI DSS, SOX, HIPAA, CMMC
Access Rights Review	Quarterly or semi-annual	Manager-level attestation of user access group membership by zone	PCI DSS, SOX, CMMC, HIPAA
Battery & UPS Test	Semi-annual	Load test backup power; replace batteries per manufacturer schedule	Business continuity; life safety
Fire Alarm Integration Test	Annual with fire alarm inspection	Verify mag lock release on alarm signal; test REX-fire alarm coordination	NFPA 72, NFPA 101, AHJ or inspection requirements where applicable
Compliance Documentation Update	Annual	Update access control procedures, user administration guide, audit report templates	Regulated environments where applicable
Technology Refresh Assessment	Every 3–5 years	Evaluate hardware age, platform end-of-life timeline, credential technology currency	Supports proactive capital planning and may reduce emergency replacement risk

Common Access Control Mistakes to Avoid

Across commercial access control deployments, BTI has observed recurring planning, design, and operational issues that can contribute to post-installation problems, compliance findings, and budget overruns. These issues are often not the result of bad intentions — they usually arise when access control is designed without enough attention to door hardware, life safety, IT infrastructure, and operational security. Understanding these pitfalls before your project begins is one of the most valuable contributions this guide can make.

→ Specifying Hardware Without a Site Survey

Generic hardware specifications applied without a door-by-door survey can produce mismatched hardware, inspection issues, and expensive change orders. A door-by-door survey is strongly recommended before final hardware specification.

→ Installing 125 kHz Proximity Credentials

Legacy proximity cards are cloneable with readily available, inexpensive devices. New deployments using 125 kHz proximity technology may create avoidable credential-security risk compared with modern smart credential options. Consider 13.56 MHz smart credentials or stronger options where compatible with the platform, risk profile, and budget.

→ Ignoring Throughput at High-Volume Openings

Under-specifying reader speed, lock release time, and door hardware grade for high-traffic openings can create queues that increase tailgating risk. Design around peak traffic, not only average traffic.

→ Skipping Fire Alarm Integration

Maglocks often require fire alarm, REX, egress, and AHJ review. Skipping this coordination can create inspection, safety, or remediation issues that are difficult and expensive to address after installation.

→ No Credential Offboarding Process

Without a defined offboarding workflow, terminated employee credentials accumulate in the system. This is a common access control governance issue and is preventable with a defined offboarding process.

→ Deploying Biometrics Without Legal Review

Biometric privacy laws vary by jurisdiction and can carry significant legal and financial risk. Consider biometrics only after appropriate legal, privacy, HR, and policy review, with consent, retention, and deletion processes defined where applicable.

→ No Documentation at Closeout

A system with limited as-built documentation can be harder to service, expand, or review. Define required closeout documentation as part of the project scope before installation begins.

Access Control Buyer Checklist: Questions to Ask Before You Buy

Use this checklist to identify the decisions, risks, and requirements that may affect your access control project. Not every item applies to every organization, but these questions help buyers avoid under-scoped systems, weak hardware choices, compliance gaps, and service problems.

System Design & Hardware

- Has a door-by-door site survey been completed?
- Have fire-rated openings been identified and reviewed?
- Has each opening been reviewed for fail-safe, fail-secure, egress, and AHJ considerations?
- Has traffic volume been analyzed for high-use openings?
- Has hardware grade been matched to duty cycle and traffic requirements?
- Have REX, door position monitoring, and alarm needs been reviewed for each controlled opening?
- Has fire alarm integration been reviewed for maglocks where required by hardware, code, occupancy, and AHJ interpretation?
- Has an accessible path of travel been reviewed for all turnstile and gate configurations?
- Has backup power been planned for critical panels and openings?

Credentials & Identity

- Are stronger credential options being considered instead of legacy 125 kHz proximity?
- Has credential technology been selected, with 13.56 MHz smart credentials or stronger options considered where compatible with platform, risk profile, and budget?
- Has multi-factor authentication been evaluated for high-security zones?
- Has legal, privacy, and HR review been completed if biometrics are being considered?
- Has a mobile credential strategy been evaluated?
- Has a credential provisioning and offboarding workflow been designed?

Platform & Integration

- Has the cloud vs. on-premises architecture decision been made?
- Has platform scalability been validated against the organization's growth plan?
- Has video surveillance integration been designed?
- Has IT security or SIEM integration been evaluated?
- Has visitor management integration been considered if required?
- Have elevator and parking integrations been planned if applicable?

Compliance & Documentation

- Have applicable regulatory frameworks, compliance programs, or insurance requirements been identified?
- Has an access log retention approach been defined?
- Has a periodic access rights review process been considered?
- Have compliance documentation needs been identified with the organization's legal, compliance, audit, or insurance advisors?
- Has closeout documentation been defined as part of the project scope?
- Has the installer's license been verified in applicable states or jurisdictions?

Maintenance & Lifecycle

- Has the organization decided who will maintain the system after installation?
- Has a firmware and software update process been considered?
- Has periodic fire alarm integration testing been planned?
- Has a technology refresh timeline been included in planning?

Related BTI Resource

Before requesting a formal proposal, many organizations benefit from completing a basic physical security self-assessment. This can help identify obvious gaps around doors, cameras, visitor access, alarms, and after-hours security before the site survey.

Use BTI's Commercial Security Self-Assessment Checklist

Access Control Planning Worksheet

Complete this planning worksheet before engaging BTI or any access control installer for a site assessment or proposal. The more completely you can answer these questions, the more accurate and useful the initial consultation will be. This worksheet can also serve as a starting point for your internal requirements documentation and RFP process.

Planning Question	Your Response
How many doors/openings require access control?	
How many buildings or sites are included?	
What states are the facilities located in?	
What is the peak hourly employee count at the primary entry?	
Do you have fire-rated doors requiring hardware? Which ones?	
What credential technology are you currently using?	
Is an existing access control system in place? What platform?	
What video surveillance platform is currently in use?	
What HR/HRIS system is in use for employee management?	
Are turnstiles or speed gates required at any entry points?	
Are biometric credentials being considered?	
What regulatory frameworks apply to your organization?	
Is intercom or video intercom integration required?	
Do you prefer cloud-hosted or on-premises platform architecture?	
What is your target installation timeline?	
What is your approximate budget range for this project?	
Who is the primary internal decision-maker and technical contact?	
Are managed service / ongoing maintenance services required?	

Why Choose BTI Communications Group for Commercial Access Control

BTI Communications Group brings a fundamentally different approach to commercial access control than a single-trade security installer. Our team integrates expertise across physical security, IT infrastructure, cybersecurity, VoIP, intercoms, and compliance-supporting documentation — which means access control can be planned with network, IT, life-safety, documentation, and support considerations in mind when those items are part of the project scope. This integrated competency is an important differentiator for organizations that need access control to perform as a strategic business technology investment rather than a commodity door-locking project.

BTI uses a platform-fit design approach. We recommend systems based on the client's doors, users, compliance or documentation needs, IT environment, integration requirements, support model, and the platforms BTI can responsibly deploy and maintain. However, we only recommend platforms and hardware ecosystems we can responsibly install, document, maintain, and support long term. BTI supports a focused, proven access control ecosystem that includes Kantech, Software House, Avigilon Alta, Avigilon Unity / ACM, Brivo, RS2 / ACRE, Alarm.com for Business, YourSix, HID credential technologies, Axis and Avigilon video integrations, 2N and Aiphone intercom workflows, and major commercial door hardware manufacturers. We do not try to be everything to everyone. We recommend and support systems we can design correctly, install cleanly, document fully, and maintain over the long term.

BTI directly serves California, Illinois, and Arizona and can provide applicable license and insurance documentation during the proposal process.

BTI also supports national multi-site deployments through properly licensed local contractors, subcontractors, and project partners where required.

For select international projects, BTI can assist with planning, standardization, manufacturer coordination, remote support, and deployment oversight when the project scope, local regulations, product availability, and qualified in-country resources allow.

California

BTI directly serves California and can provide applicable license and insurance documentation during the proposal process. California access control, alarm, low-voltage, electrical, locksmith, and door hardware requirements may vary by project scope, permit requirements, and AHJ review.

Illinois

BTI directly serves Illinois and can provide applicable license and insurance documentation during the proposal process. Illinois access control, alarm, locksmith, and electronic security requirements may vary by project scope, location, and state or local requirements.

Arizona

BTI directly serves Arizona and can provide applicable license and insurance documentation during the proposal process. Arizona access control, alarm, low-voltage, and related security work may involve ROC, DPS, local permitting, AHJ review, or other requirements depending on project scope.

National + Select International Reach

BTI helps multi-site organizations standardize access control, video, intercom, credentials, documentation expectations, and project delivery across multiple regions while coordinating with properly licensed local resources where required. Select international support is available when scope, regulations, product availability, and qualified in-country resources allow.

Built on 40 Years of Technology Convergence

BTI's access control work is part of a larger business story that began in 1985, when founder Eric W. Brackett started Brackett Telecommunications to help businesses take more control of their communications systems. BTI Communications Group was incorporated in 1992 and evolved from telecom, structured cabling, and digital phone systems into VoIP, IT infrastructure, cybersecurity, physical security, access control, video surveillance, and managed technology services.

That history matters because access control is no longer just a door project. It depends on networks, cloud platforms, identity, video, intercoms, cybersecurity, documentation, and long-term support. BTI has evolved through each wave of that connected security landscape, giving clients a practical partner for projects that cross physical security, IT, communications, and operations.

1985

Brackett Telecommunications founded. Helping businesses take control of their communications systems.

1992

BTI Communications Group incorporated. Expanding into structured cabling, digital phone systems, and business technology.

2000s–2010s

Evolution into VoIP, IT infrastructure, cybersecurity, and physical security. Access control, video surveillance, and intercoms added to the portfolio.

Today

Full-service managed technology provider. Access control, video, alarms, intercoms, IT, VoIP, cybersecurity, and compliance-supporting documentation — as a coordinated business technology environment.

Read the BTI Story →

Start Your Access Control Project with BTI

Planning a new access control system, replacing an older platform, or standardizing doors across multiple sites? BTI can help your team evaluate door conditions, hardware options, credential strategy, integrations, documentation needs, and likely project scope before you commit to a platform or installation plan.

BTI Communications Group helps organizations plan, install, upgrade, and support commercial access control systems as part of a broader security and business technology environment. Direct service is available in California, Illinois, and Arizona, with national deployment coordination and select international support when scope, regulations, product availability, and qualified local resources allow.

> BTI can design, install, document, support, and manage access control as part of a complete security and business technology environment when those services are included in the project scope or managed service agreement.

Regional + National Reach

Direct service in California, Illinois, and Arizona, with national deployment coordination through properly licensed local resources where required. Select international support is available when scope and local resources allow.

6+ Security Disciplines

Access control, video, alarms, intercoms, IT infrastructure, VoIP, cybersecurity, and compliance-supporting documentation when in scope.

Focused Supported Ecosystem

BTI recommends platforms we can responsibly design, install, document, and support, including Kantech, Software House, Avigilon Alta, Avigilon Unity / ACM, Brivo, RS2 / ACRE, Alarm.com for Business, YourSix, HID, Axis, 2N, Aiphone, and major commercial door hardware manufacturers.

Helpful next step

Not ready for a full access control assessment? Start with BTI's Commercial Security Self-Assessment Checklist to identify obvious gaps around doors, cameras, visitor access, alarms, and after-hours security.

Start with the Security Self-Assessment Checklist

Ready to plan your project?

Contact BTI Communications Group to discuss an access control assessment, system upgrade, multi-site standardization project, or managed support plan. Our team can review your facility, requirements, current infrastructure, and any compliance or documentation needs you identify — then provide a practical proposal aligned to the agreed scope.

Request an Access Control Assessment

Explore BTI Business Security Systems · Read the BTI Story