Access Control System Comparison Checklist

Castle Security (Perth, WA)

Use this checklist to compare physical access control systems (PACS) across controllers, readers, software, integrations, security posture, and lifecycle cost. Tick each item during vendor demos and procurement reviews.

Organisation	
Sites / Locations	
Doors (Now / 24 Months)	
Deployment Model (Cloud / On-Prem / Hybrid)	
Primary Stakeholders (IT / Facilities / Security / Ops)	
Date	

How To Use This Checklist

- ☐ Define sites, doors, and growth plan (12–36 months).
- ☐ Involve IT, Facilities, Security, Operations, and HR (if onboarding/offboarding is in scope).
- ☐ Separate must-haves vs nice-to-haves before vendor demos.
- ☐ Validate outage behaviour (power/WAN/LAN/server) on a pilot door.

1) System Type And Deployment Model

- ☐ Cloud (SaaS), On-Prem, or Hybrid model clearly defined.
- ☐ Remote access management via browser/app with role-based administration.
- ☐ Data residency, retention, and export options documented.
- ☐ Shared responsibility (vendor vs customer) understood and agreed.

2) Core Components And Responsibilities

- ☐ Door controllers, readers, credentials, locks, sensors, and software clearly scoped.
- ☐ Door hardware (strikes/maglocks/egress) specified per door type.
- ☐ Commissioning and handover deliverables confirmed (as-builts, admin training, logs).

3) Reliability And Outage Behaviour

- ☐ Controllers cache credentials/schedules for offline operation.
- ☐ Local event buffering with later sync to central logs.
- ☐ Predictable door behaviour during power loss (fail-safe/fail-secure) and compliant egress.
- ☐ UPS/battery backup plan for critical doors and comms.

4) Authentication Methods And Credential Strategy

- ☐ Credential types supported: cards, PIN, mobile credentials, biometrics.
- ☐ Secure credential baseline chosen (e.g., DESFire/SEOS/mobile) for sensitive areas.
- ☐ Multi-factor authentication available for high-security zones (card + PIN, etc.).
- ☐ Visitor/contractor workflows supported (time-limited access, easy revocation).

5) Reader Standards And Protocols

- ☐ OSDP supported and OSDP Secure Channel mandated where feasible.
- ☐ Legacy Wiegand support only where necessary with a migration plan.
- ☐ Reader ecosystem validated (availability, firmware lifecycle, compatibility).

6) Permission Model And Governance

- ☐ Role-Based Access Control (RBAC) supported and preferred over per-person rules.
- ☐ Access groups structured by job function, site, zone, and shift.
- ☐ Approval workflow and change logging for admin actions.
- ☐ Regular credential audits scheduled (leavers, contractors, lost badges).

7) Admin UX And Day-To-Day Operations

- ☐ Single dashboard for alarms, access events, and reports.
- ☐ Fast user search, bulk updates, and template-based rollout across sites.
- ☐ Emergency actions: global lockdown, targeted lockdown, muster reports.
- ☐ Usability validated with real scenarios (shift change, visitor entry, after-hours alarms).

8) Integrations And Open API

- ☐ Video integration (VMS/CCTV) links access events to video bookmarks.
- ☐ Alarm/intrusion, intercom, lifts, gates, and BMS integrations confirmed.
- ☐ HR/IAM integration options (AD/Entra ID/SCIM/APIs) reviewed.
- ☐ Open API availability and limits documented (rate limits, auth, events).

9) Security Posture And Hardening

- ☐ End-to-end encryption covered (card→reader→controller→server/cloud).
- ☐ Certificate/TLS requirements and compatibility with TLS inspection clarified.
- ☐ Patch cadence, firmware update process, and vulnerability response defined.
- ☐ Audit trails include admin changes and configuration changes.

10) Cost Per Door And Total Cost Of Ownership

- ☐ Per-door hardware, labour, licensing, and commissioning costs itemised.
- ☐ Recurring fees (SaaS) vs server maintenance (on-prem) compared over 3–5 years.
- ☐ Support terms: warranty, response times, after-hours support, spares strategy.
- ☐ Expansion costs: adding doors/users/sites and enabling features.

11) Enterprise Vs SMB Fit

- ☐ Multi-site governance needs matched to platform (templates, inheritance, multi-tenancy).
- ☐ SMB simplicity vs enterprise complexity trade-offs agreed by stakeholders.
- ☐ Roadmap aligns with growth (doors, sites, integrations, reporting).

12) Lifecycle Planning

- ☐ Expected lifespan and upgrade path documented (readers, credentials, controllers, software).
- ☐ Migration strategy defined for legacy systems (staged rollout, dual-credential period).
- ☐ Ongoing maintenance plan agreed (patching, backups, cert renewals, audits).

Next Step

If you want a vendor-neutral shortlist and a practical design for your doors, sites, and integrations, Castle Security can run a structured design consult and produce a comparison scorecard you can use internally.