

PRELIMINARY SITE WALKTHROUGH

The 12 security gaps criminals look for.

And how to close them.

A walkthrough you can run on your own site, tonight, with nothing but a flashlight and an hour. It is the same preliminary look our people take on a first visit: the questions that come before anyone talks about equipment, headcount or price.

READ THIS PAGE FIRST

An honest description of what you are holding.

Most security guides are advertisements with page numbers. This one tells you where it stops.

SCOPE AND LIMITS

This guide walks you through a **preliminary vulnerability and risk assessment**, the basic first look. It is **in no way comprehensive or all-encompassing**. A real assessment is a dedicated engagement: threat modeling against the adversaries who actually target your sector, asset criticality, adversary capability and intent, testing rather than observation, and documentation that stands up to an insurer, a regulator or a court. None of that is in these pages, and no eighteen-page document can substitute for it.

What a preliminary walkthrough is good for is this: **it finds the obvious things first**. In our experience the obvious things are usually still there. Sites are rarely compromised by a sophisticated adversary defeating a well-run program. They are compromised through a door that was propped, a camera nobody was watching, a credential belonging to someone who left in March.

You do not need a consultant to find those. You need an hour, a systematic order to walk in, and a willingness to write down what you actually see rather than what you believe is in place. That is what the next sixteen pages give you.

If a walkthrough like this finds nothing, you have learned something worth knowing. If it finds four things, you have just done the most valuable hour of security work available to you this month.

HOW TO USE IT

- **Walk the outside first, and walk it after dark.** Daylight hides almost every lighting and sightline problem you have.
- **Then walk the inside, in the order a stranger would.** Approach, entry, lobby, elevators and stairs, corridors, back-of-house, dock.
- **Record what you observe, not what is policy.** The gap between the two is the finding.
- **Use the worksheet on pages 13–14.** Mark *Not tested* honestly. Untested is not the same as working, and the difference matters more than any other distinction in this document.

WHO WROTE THIS

Security Alliance was founded in Miami in 2001 by a former U.S. intelligence officer. Our leadership comes from intelligence, military and law-enforcement backgrounds, and the company holds Florida agency licenses for security and private investigation and operates a licensed Security Officer School. Everything in this guide reflects that background rather than any single client engagement. Nothing here describes, or is drawn from, a specific client's site.

BEFORE THE TWELVE

How a site gets chosen.

Almost nobody picks a target because it is valuable. They pick it because it is easy, and then discover whether it was valuable.

It is tempting to think about security as a contest between your defenses and someone's determination. For a small number of adversaries, the ones a full assessment exists to model, that is true. For the overwhelming majority of incidents at commercial, residential and institutional sites, it is not. The person who breaks into your building, walks off with a laptop, follows a resident through a garage door or talks their way past a lobby is not solving a hard problem. They are choosing an easy one from several available.

That choice is made on three questions, usually in under a minute, usually from outside:

- **How much effort will this take?** Not *can it be done*, but how long, how loud, how many hands.
- **Who is watching, and will they do anything?** A camera is not observation. A guard reading a phone is not observation. Someone who looks up and makes eye contact is.
- **How do I leave?** Every approach is chosen backwards from the exit. Sites with one obvious way in and several unmonitored ways out are chosen more often than the reverse.

A site does not have to be hard. It has to be harder than the one next to it, and it has to look like somewhere that would notice.

This is why the twelve gaps that follow are mostly not equipment failures. Equipment is the part organizations buy, and buying is the part that gets done. The gaps are in maintenance, in decisions, in the things that were correct on the day they were installed and have been quietly degrading since: a light that failed, a policy nobody enforces after 6 p.m., a door that gets propped every morning because the alternative is inconvenient.

Each of the following pages gives you one gap, what it looks like on a real site, why it matters more than it appears to, and what closing it actually requires. Some closures cost money. Most cost a decision.

GAP 01**A perimeter that advertises nobody is paying attention.****WHAT IT LOOKS LIKE**

Fence panels bent and never straightened. A gate that no longer latches, wedged with a brick. Graffiti that has been there long enough to fade. Litter accumulated in a corner. Signage sun-bleached to illegibility, or naming a security company that has not held the contract in years.

WHY IT MATTERS

None of this stops anyone, and none of it is meant to. Its function is signaling. A boundary in visible disrepair says the same thing to a person assessing your site as a stack of uncollected mail says about an empty house: *no one here is looking closely, and no one has for a while*. It is the cheapest possible intelligence about how you run everything else, and it is accurate more often than not.

HOW TO CLOSE IT

Walk the full boundary line, on foot, at the pace you would walk a dog, not from a vehicle. **Fix the small things within a week and keep fixing them.** Replace outdated signage; a sign naming the wrong provider tells a reader your paperwork is as stale as your fence.

GAP 02**Lighting that creates shadow instead of removing it.****WHAT IT LOOKS LIKE**

Bright pools under each fixture with darkness between them. A floodlight aimed outward that dazzles anyone looking in and silhouettes anyone standing under it. Failed lamps nobody has reported because nobody is on site at the hour they matter. A parking lot lit beautifully and a service path beside it lit not at all.

WHY IT MATTERS

Lighting does not deter by brightness. It deters by **removing places to be unobserved** and by making faces recognizable to people and to cameras. Uneven lighting can be worse than none: high contrast destroys the eye's ability to see into the dark areas, and destroys a camera's ability to do the same. Most sites have enough light and the wrong distribution of it.

HOW TO CLOSE IT

Do the walk after dark. This gap is invisible in daylight and it is the single most common finding on a first visit. Look for continuity rather than intensity: **can you recognize a face at every point along the approach, at every entrance, and at every vehicle route?** Log failed lamps as a maintenance ticket with a deadline, not an observation.

GAP 03**Landscaping and sightlines that hand over concealment at the door.****WHAT IT LOOKS LIKE**

Shrubs grown above waist height beside an entrance. A tree canopy that has dropped below head height across a walkway. Recessed doorways, alcoves and trash enclosures that cannot be seen from anywhere a person routinely stands. Boundary planting that has matured into a screen, excellent for privacy, and equally excellent for whoever is standing behind it.

WHY IT MATTERS

Concealment is worth more to someone than the absence of a lock. It buys the two commodities that matter most: **time at the door, and freedom from observation while using it.** Landscaping is the one security-relevant feature of a site that gets worse on its own, every season, with nobody deciding anything.

HOW TO CLOSE IT

Apply the ordinary rule of thumb: **planting below waist height, canopies above head height**, so a person cannot be hidden by either. Stand at each entrance and ask what can see you. Then put it in the grounds-maintenance contract with a specification, because otherwise it will be trimmed for appearance and grow straight back.

GAP 04**A front door that any confident stranger walks through.****WHAT IT LOOKS LIKE**

A visitor book nobody reads. A badge printed from a name the visitor gave, unverified against anything. A receptionist whose actual role is hospitality, with no authority to refuse anyone and no script for trying. A safety vest, a clipboard, a purposeful stride, and a sentence like *"I'm here for the fire panel inspection"*, delivered at 8:40 a.m. when the lobby is busiest.

WHY IT MATTERS

The great majority of unauthorized access at professional facilities is not forced. It is **granted**, by a person doing their job politely under social pressure they have not been trained or empowered to resist. The failure is almost never the individual's. It is that no one ever decided what they were permitted to do.

HOW TO CLOSE IT

Decide, in writing, three things: **who is expected today, who verifies an unexpected arrival, and what a refusal sounds like.** Pre-notification for contractors turns an argument into an administrative check. Give the front desk explicit authority to say *"I'll call and confirm, please take a seat"*, and back them when they use it.

GAP 05**Keys and credentials nobody has ever audited.****WHAT IT LOOKS LIKE**

No current list of who holds what. Keys cut on request over years by whoever asked. A master key whose distribution is remembered rather than recorded. Access cards belonging to people who left, still active because deactivation is nobody's named job. A contractor's card issued for a two-week job three years ago.

WHY IT MATTERS

This is the gap that quietly voids everything else. You can invest heavily in doors, locks and readers, and if **the number of people who can open them is unknown**, you do not have access control. You have access convenience. It is also the gap most likely to matter after an incident, when the first question asked by an investigator or an insurer is who had legitimate means of entry, and the honest answer is that nobody knows.

HOW TO CLOSE IT

Produce the list. Just once, properly: every key, every card, every code, every person. **Then attach deactivation to the departure process** so it happens without anyone remembering, and re-audit on a fixed date each year. If reconciliation is impossible, that is your answer, and it is a rekeying decision.

GAP 06**Doors defeated by hardware, not by force.****WHAT IT LOOKS LIKE**

A fire door propped with an extinguisher every morning because the alternative is walking all the way around. Strike plates fixed with short screws into the frame's facing rather than the stud behind it. Hinges with exposed pins on the outward face. Glass beside a lever handle. A latch that can be slipped because the door has dropped and no longer seats. An exit device that releases to a hand through a mail slot.

WHY IT MATTERS

Doors are rarely broken through. They are **opened**, using the way the hardware was fitted or the way people have adapted around it. And a propped door is not a discipline problem to be solved with a memo. It is evidence that the building's design is fighting the way the work actually happens. The memo will lose.

HOW TO CLOSE IT

Walk every external and every controlled internal door and try it, physically. Look at fixings, hinge pins, glass beside handles, and seating. **Where a door is habitually propped, ask why before you ask who**, and fix the reason: a badge reader on the convenient route usually ends the behavior permanently where a notice will not.

GAP 07

Cameras that record, watched by nobody, with retrieval nobody has tested.

WHAT IT LOOKS LIKE

Wide shots that cover a lot of ground and identify no one. Cameras pointed into the sun at the hour that matters. A recorder that has been overwriting at seven days when everyone believes it holds thirty. Failed channels showing black for months. And the discovery, on the day something happens, that nobody present knows how to export footage, or in what format, or who holds the password.

WHY IT MATTERS

Cameras are bought as deterrence and used as evidence, and they are frequently good at neither. A camera deters only a person who believes someone is watching. As evidence it is worthless unless it **identifies** rather than merely records, retains long enough for the incident to be noticed, and can be got out of the system by someone available at 3 a.m. on a Sunday.

HOW TO CLOSE IT

Test it, do not survey it. **Pick a date last week and export five minutes of footage from three cameras.** That single exercise will tell you your true retention, your true image quality, your true channel health and whether anyone on site can actually do it. Then fix identification coverage at the choke points (entrances, registers, docks) before adding any breadth.

GAP 08

The loading dock is the building's real front door.

WHAT IT LOOKS LIKE

A front entrance with a reader, a camera and a person, and a service door standing open all morning for deliveries. A freight elevator reaching every floor without a credential. A dock area unobserved from anywhere. A yard gate that opens on a button for anything that looks like a truck.

WHY IT MATTERS

Security investment concentrates where visitors and executives arrive, because that is where the building is judged. Meanwhile the route with the least attention, the most traffic, the widest opening and the most legitimate-looking strangers is at the back. Anyone assessing your site professionally will look there second. **Anyone assessing it opportunistically will find it first.**

HOW TO CLOSE IT

Walk your own building starting from the service entrance and see how far you get before anyone speaks to you. **Apply the same standard you apply at the front: identification, observation, and a decision about who may proceed unescorted.** If the dock must stand open during a delivery window, that window needs a person, not a policy.

GAP 09**Contractors and deliveries holding standing, unescorted access.****WHAT IT LOOKS LIKE**

Cleaning, maintenance, landscaping and vending staff moving through the building at hours when nobody is present to observe them. Access granted once and never reviewed. Personnel who have changed several times at the contractor while the credential stayed the same. No requirement that the contractor tells you when their staff change, and no idea whether their vetting standard resembles yours.

WHY IT MATTERS

These are the people with the most access, at the least observed hours, subject to the least scrutiny, and they are usually not your employees, so your vetting, your discipline and your controls do not reach them. **You have outsourced part of your perimeter to a company whose hiring standard you have never read.**

HOW TO CLOSE IT

List every third party with access, what access they hold and when they use it. **Ask each for their vetting standard in writing and a duty to notify you of personnel changes.** Where escort is impractical, compensate with credential expiration, restricted zones and a named point of contact who is accountable when something goes wrong.

GAP 10**Post orders that describe posture but never decisions.****WHAT IT LOOKS LIKE**

Instructions that specify uniform, patrol times and where to stand, and say nothing about what to do when a person refuses to leave, when a resident is locked out and angry, when a fire alarm sounds during a delivery, when someone is photographing the building, or when a member of your staff instructs the officer to do something the orders forbid.

WHY IT MATTERS

Under pressure, people do not perform to a job description. They perform to whatever they have rehearsed, and if nothing has been rehearsed they improvise, usually toward the least confrontational option. **Every serious incident is decided in the first two minutes by whoever is standing there.** Orders that do not cover decisions have left those two minutes to chance.

HOW TO CLOSE IT

Take your five most plausible incidents and write what the officer does, who they call, in what order, and what they must not do. **Then ask an officer on post to tell you the answer without looking.** If they cannot, the document is decoration, and that is a finding about your provider, not about the officer.

GAP 11**Shift change: the gap that runs on a published schedule.****WHAT IT LOOKS LIKE**

Two officers standing together at a post, handing over, both facing each other and neither facing the door. A twenty-minute window at the same time every day where coverage is nominal. Handovers that pass on nothing: no note of the vehicle that circled twice yesterday, the door found unsecured, the person who asked unusual questions about the alarm.

WHY IT MATTERS

Every predictable pattern in your operation is available to anyone willing to watch the building for three days, and shift change is the most visible and most consequential of them. It is also where continuity dies: **a series of small observations that would form a pattern instead ends at the end of each shift**, and nobody ever sees the shape of it.

HOW TO CLOSE IT

Vary handover timing where you can, and require it to happen **at post, facing outward, with the incoming officer taking position before the outgoing one leaves**. Require a written pass-down of anything unusual, however minor, and require a supervisor to read across days. The pattern is only visible from above.

GAP 12**An escalation path that has never been tested end to end.****WHAT IT LOOKS LIKE**

A call list on a laminated sheet with two numbers that have changed. A monitoring contract nobody has exercised since installation. An assumption that the alarm reaches someone who will attend. Nobody able to answer, without checking, what happens between the moment a detector triggers at 2 a.m. and the moment a human being arrives, or how long that takes.

WHY IT MATTERS

Detection without response is a recording of your loss. Every element can be individually correct (sensors working, monitoring paid for, guard force posted, numbers on file) and the chain can still break at a single handoff nobody owns. **You do not find out where until the night it matters**, and by then the question is no longer academic.

HOW TO CLOSE IT

Test the whole chain, once, deliberately, after hours, with the monitoring company notified in advance. **Time it**. Write down what actually happened at each step versus what was supposed to. Then repeat annually. This is the least performed and most revealing exercise in physical security, and it costs an evening.

WHAT THEY HAVE IN COMMON

None of these is an equipment problem.

Read the twelve again and notice what is missing: almost nothing on that list is solved by buying something.

A bent fence, an unlit path, an overgrown shrub, an unverified visitor, an unaudited key list, a propped door, an untested recorder, an open dock, an unreviewed contractor, a thin post order, a predictable handover, an unexercised alarm chain. Some of those have a purchase attached somewhere. Most are **decisions that were never made, or were made once and never revisited.**

This matters because it changes the question. Organizations tend to ask *what security do we have?*, a question answered by an inventory, and one that flatters almost every site. The more useful question, and the one a preliminary walkthrough is designed to answer, is:

Not *what do we have*, but *when was it last tested, and by whom, and what happened?*

An inventory says you have thirty-two cameras. A test says you have thirty-two cameras, twenty-nine of which are recording, seven days of retention rather than the thirty you are paying for, and one person on the payroll who knows how to export a clip, and she left in April.

Security decays quietly and on its own. Nothing announces the failure of the lamp on the service path, the departure of the person who understood the recorder, or the drift of the delivery window from thirty minutes to three hours. There is no alarm for the slow loss of a security posture, which is why the walkthrough has to be a recurring habit rather than a project.

THE ONE THING TO TAKE FROM THIS PAGE

If you do nothing else in this guide, do the two tests: **export five minutes of last week's footage from three cameras**, and **trigger the alarm chain after hours and time it end to end**. Between them they will tell you more about the true state of your security than any inventory, any inspection report, and most proposals you will be shown.

WHERE PROFESSIONAL FACILITIES ARE EASIEST

Access control fails in five predictable ways.

Every one of them is a failure of the system around the technology, not of the technology. Modern readers, cards and locks work. What fails is what people were permitted to do with them.

FAILURE 01

The badge as talisman.

A visible badge stops questions. Nobody checks that the photograph matches, that the badge is current, that it belongs to this building, or that it is anything other than a rectangle of plastic on a lanyard. In most facilities a plausible-looking badge, worn confidently, is a better key than any actual credential, because it defeats the only control that still involves a human being.

THE CORRECTION

A badge is a prompt to check, not a permission. Where credentials matter, the reader, not the eye, must be what grants access, and readers must be positioned so there is no way past them that is easier than through them.

FAILURE 02

Tailgating tolerated, because challenging is socially expensive.

One badge, four people through the door. Holding the door for a stranger carrying a box is basic courtesy, and asking someone to badge in separately feels like an accusation. So a control that cost real money is defeated dozens of times daily by ordinary politeness, and by the fact that nobody has ever told staff they are allowed to be impolite.

THE CORRECTION

This is a permission problem before it is a design problem. **Tell people explicitly that challenging is expected, give them a courteous script**, such as *"Sorry, we're asked to have everyone badge in"*, and make sure the first person who uses it is supported, not overruled. Where the risk justifies the cost, remove the social element with a turnstile or an airlock.

FAILURE 03**Credentials that outlive the person.**

Deactivation belongs to whoever remembers. HR completes an exit process that does not reach the access system. A contractor's card is issued for a short engagement with no expiration date set. Nobody reconciles the active credential list against the payroll, ever, so the list only grows, and every departure adds a permanent, invisible key to your building.

THE CORRECTION

Attach deactivation to the departure process itself, with a named owner, so it happens whether or not anyone remembers. Set expiration dates on every temporary credential at the moment of issue: a card that expires by default cannot be forgotten. Reconcile annually against payroll and the contractor list.

FAILURE 04**Access granted by convenience rather than need.**

Someone needed a door once, so they were added to the group that opens every door. Access levels multiply until "everyone can go everywhere" is the operating reality, described in the documentation as a tiered scheme. Nobody wants to be the person who refuses a colleague, and nobody is asked to review what was granted last year.

THE CORRECTION

Grant to the role, not the person, and **review the roles annually**. The useful test is not *should this person be trusted*. Almost everyone should. It is *what does this role need in order to work*, which is a question about jobs rather than about people, and is therefore answerable without insulting anyone.

FAILURE 05**The standing override.**

The master key. The code taped inside a drawer. The shared account used by the whole night team. The door left on free-access from 7 a.m. for the cleaners and returned to secure by whoever notices. Every access control system has these, they are almost never documented, and they represent the actual security posture, not the one in the specification.

THE CORRECTION

Find them and write them down; you cannot govern what is undocumented. **Then justify each one out loud**. Some are legitimate operational necessities and should be scheduled, logged and time-bounded. The rest exist because they were once convenient, and will keep existing until somebody asks.

THE COMMON THREAD

Four of these five failures are about **who is permitted to say no**, and whether that person will be supported afterwards. That is a management question, not a security-industry one, and no vendor can answer it for you.

[PRINT THIS PAGE](#)

Walk your site. Mark what you see.

Outside first, after dark. Mark *Not tested* honestly. It is not a lesser answer than *Present*, it is a different finding, and usually a more urgent one.

CHECK	PRESENT	PARTIAL	ABSENT	NOT TESTED
APPROACH AND PERIMETER				
01 Boundary intact, maintained, free of long-standing damage or graffiti; signage current and naming the correct provider	☐	☐	☐	☐
02 After dark: continuous light along every approach, entrance and vehicle route: a face recognizable at each point, no dazzle, no deep shadow between fixtures	☐	☐	☐	☐
03 Planting below waist height and canopies above head height near entrances; no alcove, recess or trash enclosure that cannot be seen into	☐	☐	☐	☐
ENTRY AND CONTROL				
04 An unexpected visitor is verified against something before being admitted; the front desk has written authority to refuse and knows it	☐	☐	☐	☐
05 A current list exists of every key, card and code and who holds it; deactivation is attached to the departure process by name	☐	☐	☐	☐
06 Every external and controlled door physically tried: seats and latches properly, sound fixings, no exposed hinge pins, none habitually propped	☐	☐	☐	☐
SURVEILLANCE AND BACK OF HOUSE				
07 Tested: five minutes of last week's footage exported from three cameras, by someone on site, without outside help	☐	☐	☐	☐
08 Service entrance and dock held to the same standard as the main entrance; walked from the dock inward without being challenged?	☐	☐	☐	☐
09 Every third party with access listed, with their vetting standard in writing and a duty to notify you of personnel changes	☐	☐	☐	☐
PEOPLE, TIMING AND RESPONSE				
10 Post orders cover decisions for the five most plausible incidents, and an officer on post can state them without looking	☐	☐	☐	☐
11 Handover happens at post, facing outward, with a written pass-down that a supervisor reads across days	☐	☐	☐	☐
12 Tested: full alarm-to-attendance chain exercised after hours within the last twelve months, and timed	☐	☐	☐	☐

ACCESS CONTROL

The five failures, on your site.

CHECK	PRESENT	PARTIAL	ABSENT	NOT TESTED
A1 Access is granted by a reader or a lock, not by the sight of a badge; there is no route past a control point easier than through it	☐	☐	☐	☐
A2 Staff have been told explicitly that challenging is expected, have a courteous script, and have been supported when they used it	☐	☐	☐	☐
A3 Temporary credentials carry an expiration date set at issue; the active credential list was reconciled against payroll within the last year	☐	☐	☐	☐
A4 Access is granted to roles rather than individuals, and the roles were reviewed within the last year	☐	☐	☐	☐
A5 Every standing override (master keys, shared accounts, scheduled free-access) is documented, time-bounded and justified	☐	☐	☐	☐

FINDINGS

The three things you will fix first.

Anything marked Absent or Not tested is a candidate. Prefer the ones that cost a decision rather than a budget. They are the ones that will still be fixed in six months.

#	FINDING	OWNER	BY WHEN
1			
2			
3			

SET THE DATE NOW

A walkthrough performed once is an anecdote. Put the next one on the calendar before you put this guide down: quarterly for a site with public access or high turnover, annually at minimum for anything else. The value is entirely in the repetition, because what you are measuring is drift.

BEFORE YOU SIGN ANYTHING

Questions to put to every provider. Including us.

These are not trick questions. They are the ordinary questions a buyer would ask if the industry made it easy to compare providers, which, largely, it does not. A good provider will answer all of them without discomfort.

1 Are you licensed in every jurisdiction where you will place an officer, and what are the numbers?

Ask for the numbers, not the assurance, and check them yourself against the state register. Page 18 explains how. A provider who cannot produce them quickly is telling you something about their administration even if the licenses exist.

2 Will this contract be performed by your own employees, or subcontracted?

There is nothing wrong with subcontracting, but you should know before you sign, not after an incident. If any part is subcontracted, ask who, where, and whose vetting and supervision standard applies: yours, theirs, or nobody's.

3 What are your insurance limits, and will you name us as an additional insured?

General liability and workers' compensation at minimum. Ask for the certificate before signature, not on request afterwards, and read the limits rather than the fact of coverage.

4 What is your officer turnover on comparable contracts, and what do you do about it?

Turnover is the single best predictor of the service you will actually receive, because an officer who does not know your site cannot protect it. Providers rarely volunteer this. Ask anyway, and note whether the answer is a number or a paragraph.

5 Exactly what does your vetting cover?

"Background checked" means whatever the provider decides. Ask which checks: criminal history and over what period and geography, employment verification, references actually contacted, driving record where relevant, drug screening, and whether any of it is repeated during employment.

6 Who writes the post orders, and when do I see them?

Post orders should be site-specific and written with you before the first shift, not adapted from another client afterwards. Ask to see a sample from a comparable site, redacted. If it is generic, yours will be too.

THE QUESTIONS THAT PREDICT THE SERVICE

A contract is signed by executives and performed by an officer.

Nearly every disappointment in contract security traces back to a gap between the people who sold the work and the people who do it. These questions close that gap before it opens.

1 Who will actually manage this contract, and will I meet them before I sign?

The people at the presentation are frequently not the people you will deal with. Ask for the named manager, their tenure with the company, and how many other accounts they carry. Then ask what happens to your account when they leave.

2 What training do your officers receive beyond the statutory minimum, and who delivers it?

The licensing minimum is a floor, not a standard. Ask whether training is delivered in-house or bought in, what site-specific training an officer gets before their first shift here, and what refresher training happens after.

3 How do you supervise, and how would I know if you stopped?

Ask about supervisory visit frequency, whether visits are at varied hours including nights and weekends, and what record you receive. Verified patrol data and visit logs are ordinary now; a provider who cannot show you evidence of supervision is asking you to take it on trust.

4 When something goes wrong at 3 a.m., who picks up, and who decides?

Ask for the escalation chain in writing, with names and the authority each person holds. Then ask how quickly you would be told about a significant incident, and what counts as significant. Get that definition in the contract.

5 What will I receive in writing, how often, and what is in it?

Incident reports, patrol records, visit logs, a monthly summary. Ask to see a real example. Reporting that only reaches you when you chase it will not survive the first quiet quarter.

6 Can I speak to a client you have lost?

Every provider offers references who are happy. The instructive conversation is with a client who left, and a provider's willingness to have you make that call is itself the answer. Very few will say yes. Note who does.

THE PART NOBODY ASKS ABOUT

Most of the risk is in the transition and the second year.

Buyers scrutinise the proposal and then stop asking questions on the day the contract starts, which is roughly the day the questions begin to matter.

1 What happens in the first thirty days, day by day?

A transition is where continuity is lost: post orders rewritten, officers who knew the site replaced, systems handed over. Ask for the plan in writing. Be wary of a provider who promises a specific phase-in period before they have seen your site. They are guessing, and you will pay for the guess.

2 Will you offer positions to the incumbent officers?

The officers already on your site hold knowledge no handover document contains. Whether a provider intends to retain them, and on what terms, tells you how the transition will actually feel, and whether week three will resemble week one.

3 What is your price in year two and year three, and what drives it?

Ask what happens at renewal, what triggers an increase, and how wage-rate changes flow through. A first-year price that cannot be sustained is a problem deferred, and it is usually paid for in officer quality.

4 How do I get out, and what happens to my data?

Notice period, exit obligations, and who owns the incident records, patrol data and footage. Ask before you need it. The terms are always more favourable while they are still trying to win you.

5 What would you tell me not to buy?

The most useful question on this page. A provider who will talk you out of something, whether more headcount, more cameras or an upgrade you do not need, is advising you. One who agrees with every requirement you propose is selling to you. Both are legitimate businesses; only one is on your side of the table.

SOMETIMES THE ANSWER IS NOT TO CHANGE PROVIDER

If your current arrangement has a fixable problem (thin post orders, absent supervision, a manager you never hear from), a transition may cost you more continuity than it buys. Put these questions to your existing provider first. Their answers, and how readily they give them, will tell you whether you have a problem with the company or a problem with the contract.

INCLUDING US

How to check any provider without asking them.

Licenses, registrations and federal records are public. Any claim a security company makes about its credentials can be verified in a few minutes, by you, without their help, and every provider you are considering should be checked the same way.

- **State licensing.** In Florida, private security and private investigation agency licenses are searchable through the Florida Department of Agriculture and Consumer Services. Most states publish an equivalent register. In Texas it is the Department of Public Safety. Search the license number the provider gave you and confirm the status and the name on it match.
- **Federal registration.** If a provider claims federal contracting capability, their registration is public at SAM.gov. Search their Unique Entity ID or CAGE code and confirm the registration is active and unexpired.
- **Insurance.** Ask for the certificate and read the limits, the named insured and the expiration date, not just the fact that a certificate exists.
- **Corporate standing.** Company registration and officers are public through the secretary of state where the company is registered.

So that you can practice on somebody, here are ours. Run the checks above against these numbers before you take anything else in this guide on trust.

LEGAL ENTITY	Security Alliance LLC · Florida · founded 2001
FLORIDA LICENSES	B 2100072 Security Agency · A 3200282 Private Investigation Agency · DS2700029 Security Officer School
TEXAS LICENSES	B07284601 · F07300001
FEDERAL	Unique Entity ID VBZBJQQNKT96 · CAGE 3SBX5

Security Alliance LLC

8323 NW 12th Street, Suite 218, Miami, Florida 33126

1 (888) 610-7769 · info@securityalliancegroup.com · securityalliancegroup.com

Contract security officers · executive protection · protective intelligence · investigations · officer training

This guide describes a **preliminary** vulnerability and risk walkthrough. It is not comprehensive or all-encompassing, and it is not a substitute for a dedicated assessment engagement, legal advice, or compliance with any standard or regulation applicable to your site. Nothing in it describes any specific client, site or engagement. Security Alliance accepts no liability for decisions taken on the basis of a self-directed walkthrough. If you would like the full assessment, that is a conversation, and the first one costs nothing.