ELEVATE
SOLUTIONS

CHECKLIST · BUSINESS & INDUSTRY

IT Due Diligence for M&A

Pre-acquisition assessment

What to assess before acquiring a company — infrastructure risk, security posture, compliance gaps, and the red flags that affect deal value. Sixty items, numbered for your data-room request list.

01 — INFRASTRUCTURE ASSESSMENT

What you are actually buying

IT findings move price and terms. Every end-of-life server, unlicensed seat, and undocumented network is a number — either a purchase-price adjustment, an escrow holdback, or a post-close budget line. The checklist below turns the target's IT estate into those numbers.

Timing matters. Bring IT diligence in before LOI exclusivity ends, not after. Once exclusivity lapses or the closing calendar compresses, findings stop changing the price and start becoming your problem. The requests in sections 01–03 belong in your first data-room list, alongside the financial and legal asks.

> **YOU BUY THEIR INCIDENTS**
>
> An acquisition inherits the target's security history: dormant attacker access, undisclosed breaches, and unmet notification duties all transfer with the stock or assets. Third-party involvement doubled to 30% of breaches Verizon DBIR 2025 — and on closing day, the target's vendors, integrations, and credentials become your third parties. Treat the security record as a liability schedule, not an IT detail.

Section 01 establishes what exists, who owns it, and what it will cost to keep running. Request artifacts, not assurances — an inventory export beats a verbal "we have about 200 machines."

- [ ] **Request the complete hardware asset inventory with purchase dates and warranty status** 1
  No inventory means no basis for the capex model. Gaps here make every downstream estimate a guess — and refresh costs land on the buyer.
- [ ] **Profile server and workstation age against a stated replacement cycle** 2
  A fleet past its refresh cycle is deferred capex the seller banked as profit. Quantify it and move it into the price.
- [ ] **Identify every end-of-life operating system and platform still in production** 3
  Unsupported systems cannot be patched. They carry breach exposure, can void cyber insurance attestations, and often gate the security uplift in section 04.
- [ ] **Obtain the line-of-business application list with versions, vendors, and support status** 4
  An app from a defunct vendor, or one only the founder knows, is a migration project with a price tag. Revenue-critical apps get the closest look.
- [ ] **Request current network topology diagrams and configuration documentation** 5
  Absence of documentation signals tribal knowledge. You cannot scope integration cost — or day-1 operations — for a network nobody can draw.
- [ ] **Inventory firewalls, switches, and wireless gear with firmware versions and support contracts** 6
  Edge devices past vendor support are a common breach entry point and a near-certain day-1 replacement cost.
- [ ] **Compare software license entitlements against deployed counts** 7
  True-up exposure transfers to the buyer. A pending or likely vendor audit on unlicensed seats is a quantifiable liability — put it in the model.

- [ ] **Verify who legally owns and administers the Microsoft 365 or Google Workspace tenant** 8
  Tenants registered to a founder's personal account, or controlled by an outside party with no contract, can hold the entire transaction hostage. Make clean transfer a closing condition.
- [ ] **Confirm ownership of domain names, DNS hosting, and TLS certificates** 9
  A domain registered to a personal email is a single point of failure for the brand you are paying for. Require transfer to corporate control before close.
- [ ] **Inventory all cloud subscriptions — AWS, Azure, GCP, and platform services — with billing ownership** 10
  Cloud spend hidden on personal credit cards or in marketing budgets distorts the IT cost baseline and breaks at the moment the card is cancelled.
- [ ] **Verify source-code custody for any custom software: repositories, access, and escrow** 11
  If the code sits in a contractor's personal account, you are buying software you do not control. Confirm repo ownership and IP assignment in writing.
- [ ] **Request the technical-debt register, or interview engineering leads on what they would fix first** 12
  Sellers rarely volunteer this list. The honest version is a preview of your first two years of unplanned spend.
- [ ] **Map key-person dependencies: who alone holds admin access, vendor relationships, or system knowledge** 13
  One administrator with every password is a retention problem, a TSA term, and a ransom-grade single point of failure. Price the retention package now.
- [ ] **Review build standards, runbooks, and how credentials are stored** 14
  A shared password spreadsheet is a finding in itself. Mature documentation lowers integration cost; its absence raises the key-person risk in item 13.
- [ ] **Run shadow-IT discovery: reconcile SaaS charges in expense reports against the approved application list** 15
  Unapproved tools hold company data outside any control you are evaluating. Each one is an unbudgeted contract and a possible data-exposure path.
- [ ] **Collect telecom and internet circuit contracts: terms, renewal dates, assignment and termination clauses** 16
  Circuits with years remaining and steep termination fees constrain your consolidation plan. Assignment clauses determine whether contracts even survive the deal.
- [ ] **Review hardware leases and maintenance agreements for change-of-control provisions** 17
  Change-of-control clauses can trigger repricing or termination at close. Find them before the counterparty does.
- [ ] **Assess capacity headroom — storage, compute, bandwidth — against the growth case in the deal model** 18
  If the investment thesis assumes growth the infrastructure cannot absorb, the expansion capex belongs in the model, not in a post-close surprise.

- [ ] **Inspect server-room or data-center conditions: power, cooling, physical access control — or the hosting contracts that replace them** 19
  A server rack in an unlocked closet under a sprinkler head is both a continuity risk and a signal about everything else you have not seen yet.
- [ ] **Document the remote-access architecture: VPN appliances, remote-management tools, and who can reach what from where** 20
  Aging VPN concentrators and unmanaged remote tools are recurring breach vectors and usually the first thing your security standard will force out.
- [ ] **Inventory specialty and peripheral systems: phone system, printers, lab or operational equipment, analog lines** 21
  An end-of-life PBX or an instrument that only runs on Windows 7 will not appear on the server list — and can stall operations on day one.
- [ ] **Obtain the IT org chart, staffing levels, and all outsourced IT or MSP contracts with their terms** 22
  You need to know who actually runs this environment and under what notice period. These contracts also feed the overlap analysis in item 57.

02 — SECURITY POSTURE REVIEW

The liabilities that do not appear on the balance sheet

Security findings are the diligence items most likely to change deal terms late. An undisclosed incident or an environment with no working backups is not a fix-it ticket — it is a representation issue, an escrow conversation, or a reason to walk. Demand evidence, not policy documents.

- [ ] **Request an MFA coverage report: every user, every admin, every remote-access path** 23
  Partial MFA is one of the cheapest red flags to verify and one of the strongest predictors of an incident you will inherit. Gaps go straight into the uplift estimate.
- [ ] **Verify EDR deployment percentage, which product, and who watches the alerts** 24
  An endpoint agent nobody monitors is shelfware. Coverage below the full fleet means the uncovered machines are where the problem will be.
- [ ] **Pull patch-compliance reports for the last 90 days — actual reports, not the patching policy** 25
  The gap between written policy and report data is the most honest measurement of operational maturity you will get in this entire exercise.
- [ ] **Obtain recent vulnerability scan results, internal and external** 26
  If no scans exist, commission one as a diligence condition. Critical findings on internet-facing systems are price-adjustment material.
- [ ] **Review backup configuration and evidence of the most recent successful restore test** 27
  Backups that have never been restored are a hypothesis. For a target holding client or patient data, an unrestorable backup set approaches deal-breaker territory.
- [ ] **Verify an immutable or offline backup copy exists, separated from production credentials** 28
  Ransomware operators delete reachable backups first. If every copy shares the domain admin credentials, the recovery story is fiction.
- [ ] **Request the full incident history for five years, including near-misses and how each was disclosed** 29
  An incident handled quietly without required notifications is a liability with your name on it after close. Cross-check against item 47.
- [ ] **Ask directly about prior ransomware events: any payment made, who handled recovery, what changed afterward** 30
  A paid ransom signals both a past control failure and a target known to attackers as willing to pay. Re-compromise of prior victims is common enough to price.
- [ ] **Collect prior security assessments and penetration tests with remediation status for each finding** 31
  A pentest with unremediated criticals from two years ago is documented, dated negligence — useful to you in negotiation, dangerous to you after close.
- [ ] **Review the open-findings register and any formal risk-acceptance log** 32
  Risks the seller "accepted" become risks you own. Each accepted item needs a cost to remediate or a reason to keep accepting it.

- [ ] **Confirm centralized log collection exists and how far back retention goes** 33
  Without logs you cannot answer the only question that matters at close: is anyone already inside? Thin retention also caps any forensic investigation you may need later.
- [ ] **Audit admin accounts: how many, shared or individual, separated from daily-driver accounts, any stale entries** 34
  Excess and shared admin accounts multiply breach impact and make attribution impossible. Stale admin accounts are standing invitations.
- [ ] **Test offboarding: pick five departed employees and verify their access is actually gone** 35
  Live accounts for ex-employees are a frequent root cause in post-acquisition incidents — and a fast, cheap spot-check of process discipline.
- [ ] **Run a dark-web and credential-exposure check against the target's domains** 36
  Exposed credentials for current staff mean the perimeter may already be moot. Findings here change the urgency of items 23 and 33.
- [ ] **Check email authentication and filtering: SPF, DKIM, DMARC policy, and what sits in front of the mailboxes** 37
  Weak email controls at the target expose the buyer too — post-announcement, attackers impersonate the acquired company to reach your finance team.
- [ ] **Request security awareness training records and phishing-simulation results** 38
  Deal announcements trigger targeted phishing at both companies. A workforce that has never been tested is part of the integration risk, not just an HR note.
- [ ] **Inventory third-party and vendor access: remote support accounts, integrations, API keys, data feeds** 39
  Every standing vendor connection is an inherited trust decision you did not make. Each one needs an owner, a justification, and a revocation path by day 1.
- [ ] **Compare the target's cyber insurance application against observed reality** 40
  Controls attested on the application but absent in the environment can void the coverage you are counting on — and signal how the seller answers hard questions elsewhere in the data room.

03 — COMPLIANCE GAP ANALYSIS

Obligations that transfer at close

Regulatory exposure survives the closing dinner. Successor liability for privacy violations, missing vendor agreements, and unreported breaches attaches to the buyer — and regulators do not accept "that happened before we owned them." Map the obligations first, then test whether the target actually meets them.

- [ ] **Map every regulatory regime that applies: HIPAA, GLBA, state privacy laws (CCPA/CPRA and peers), PCI DSS, and sector rules** 41
  You cannot assess gaps against an undefined standard. The target's own list is a starting point — verify it against what their data and clients actually trigger.
- [ ] **If health data is in scope, request the most recent HIPAA security risk analysis and the names of the designated privacy and security officers** 42
  A missing or stale risk analysis is among the most commonly cited failures in OCR enforcement — and it becomes your finding the day the deal closes.
- [ ] **Obtain a data inventory: what regulated data exists, where it lives, and how it flows** 43
  Purchase price often assumes the data is an asset. Unmapped regulated data is also a liability — you cannot protect, retain, or lawfully delete what nobody can locate.
- [ ] **Inventory Business Associate Agreements for every vendor that touches PHI** 44
  Each missing BAA is a standing HIPAA violation that transfers with the business. Count the gaps; counsel can price them.
- [ ] **Collect DPAs and the security commitments embedded in client contracts** 45
  Clients may hold the target to audit rights, breach-notice windows, or control standards stricter than any statute. You inherit those promises verbatim.
- [ ] **Review the data retention and destruction policy — and evidence it is actually followed** 46
  Decades of unmanaged data inflate breach impact and discovery costs in future litigation. A policy without destruction logs is a wish, not a control.
- [ ] **Request the complete breach-notification history: regulator filings, state AG notices, OCR submissions, client notifications** 47
  Reconcile this against the incident history in item 29. An incident with no matching notification analysis is the single most dangerous artifact in the data room.
- [ ] **Verify certifications claimed versus evidenced: read the actual SOC 2 report, ISO certificate scope, and expiry dates** 48
  A SOC 2 logo on the website is not a SOC 2 report. Check the report type, period, scope, and exceptions — clients who relied on the claim become your problem if it was hollow.

- [ ] **Compare the public privacy policy and consent practices against actual data handling** 49
  Saying one thing and doing another is the fact pattern behind most privacy enforcement actions. The delta between policy and practice is inherited exposure.
- [ ] **Review insurance posture: cyber and tech E&O limits, retroactive dates, pending claims, and tail coverage for pre-close acts** 50
  If the target's policies terminate at close, pre-close incidents discovered later may land on the buyer uninsured. Tail coverage is a negotiable deal term — but only before signing.
- [ ] **Pull security and privacy training records with policy acknowledgments** 51
  Training records are routine evidence requests in regulatory inquiries and breach litigation. Missing records weaken every defense the combined company will ever mount.
- [ ] **Identify open regulatory matters: audits, inquiries, consent orders, corrective action plans, litigation holds** 52
  An active consent order binds the buyer's operations, not just the seller's history. Anything open here belongs in front of deal counsel immediately.

04 — INTEGRATION RISK & COST

The price of making it one company

Integration cost is part of the purchase price — it just gets paid after close. Estimate it before signing, while the number can still shape the deal. These eight items produce the figure.

- [ ] **Scope the tenant-merge effort: mailbox counts, SharePoint and Teams data volumes, tenant-to-tenant migration path** 53

  Tenant consolidation is routinely the longest and most disruptive integration workstream. Sizing it now sets the TSA duration and the synergy timeline.

- [ ] **Plan identity consolidation: AD/Entra structure, domain trusts, duplicate accounts, conflicting conditional-access policies** 54

  Identity is the dependency under every other integration task. Conflicting security policies between the two estates surface here first — and stall everything behind them.

- [ ] **Price the security uplift: an itemized estimate to bring the target to the buyer's control standard** 55

  Every gap from sections 02–03 — MFA, EDR, backups, logging, training — becomes a line item. Presented before close, this number is negotiating leverage; after close, it is just your budget.

- [ ] **Total the contract friction: change-of-control triggers, assignment consents, and early-termination fees across telecom, software, and MSP agreements** 56

  These fees are deterministic — they are written in the contracts collected in items 16, 17, and 22. Sum them and decide who pays.

- [ ] **Resolve IT staffing and MSP overlap: who stays, who transitions, what notice periods and retention costs apply** 57

  Letting the only person who understands the environment leave in month one is a self-inflicted outage. Retention agreements for key IT staff are cheap relative to the alternative.

- [ ] **Build the day-1 access plan: payroll, email, ERP, and client-facing systems working at close, with admin credentials delivered in escrow** 58

  Day 1 is when employees and clients judge the deal. A credential handover protocol agreed in the purchase documents prevents the seller's IT departure from becoming your first incident.

- [ ] **Define TSA needs: which services the seller must keep operating, at what service level, for how long, at what cost** 59

  An undersized TSA forces a rushed migration; an open-ended one lets the seller bill you indefinitely. The scoping in items 53–54 sets the realistic duration.

- [ ] **Produce the red-flags-to-price summary: every open finding classified as deal-breaker, price adjustment, or post-close fix — with an owner and a dollar figure** 60

  This one page is the deliverable the deal team actually reads. The severity table below is the template.

Red-flag severity table

Classify every finding from items 1–59 into one of three buckets. The bucket determines who acts, when, and what it does to the price.

SEVERITY	TYPICAL FINDINGS	HOW IT HITS THE DEAL
Deal-breaker	Evidence of an active, undisclosed intrusion; a known breach with notification duties never met; core tenant, domains, or IP not legally owned by the company; an active consent order the buyer cannot operate under; no recoverable backups for the systems the revenue depends on.	Pause or walk. If proceeding, demand pre-close remediation, specific indemnities, and a forensic clean-bill as a closing condition.
Price adjustment	End-of-life fleet and platforms at scale; MFA or EDR substantially absent; large license true-up exposure; unremediated critical pentest findings; missing BAAs across the vendor base; steep contract termination fees; security uplift cost material to deal economics.	Quantify and negotiate: purchase-price reduction, escrow holdback, or seller-funded remediation with verification before release.
Post-close fix	Documentation gaps; stale training records; DMARC not yet at enforcement; short log retention; shadow-IT cleanup; policy refreshes; minor configuration findings with no evidence of exploitation.	Fold into the 100-day integration plan with an owner, a budget line, and a completion date reported to the deal sponsor.

One discipline makes the table work: nothing stays unclassified. A finding without a bucket, an owner, and a number is a finding the deal team will ignore — until it reprices the company after you own it.

ELEVATE SOLUTIONS

Elevate Solutions provides managed IT and cybersecurity for businesses that answer to regulators, clients, and courts.

Elevate Solutions

6230 Wilshire Blvd Suite 2120, Los Angeles CA 90048

(424) 400-6625 · support@elevatesolutions.io · elevatesolutions.io