Acquiring a company without a disciplined look at its technology and cyber risk is like buying a building without checking the foundation. The numbers can look clean, the market can be attractive, and still a single breach notification, license audit, or ransomware event can consume a year of integration work and erase hard-won margin. I have sat in war rooms where a deal almost died over a forgotten database server and a misconfigured cloud bucket. The fix cost less than ten thousand dollars. The delay cost a quarter.

Technology diligence is not about cataloging every cable. It is about understanding how the target creates value, how digital systems support that value, and where hidden liabilities sit. For sponsors running Business Acquisition Training programs and searchers Buying a Business, getting this part right grows confidence with lenders and gives you options at the negotiating table.

Why this work changes the deal math

Technology and cyber risk show up in places financial models miss. Revenue concentration looks worse when a single, unpatched on-premises server runs the customer portal. Working capital swings harder if software licenses are out of compliance and a vendor audit looms. Integration costs can double when no one can explain a brittle set of scripts that move orders between the website and the ERP. One lower mid-market buyer I advised trimmed purchase price by 6 percent after discovering that the target’s “cloud” CRM was actually a self-hosted fork with no upgrade path. That discount funded the migration and saved a year of post-close pain.

Cyber incidents now carry contractual and regulatory teeth. If the target processes card payments, SOC 2 or PCI posture affects merchant fees and, in some cases, the ability to accept cards at all. If the company sells into healthcare or government, a missing Business Associate Agreement or an incomplete vendor risk program can trigger breach notifications that tank customer trust. The question is not whether to assess tech risk. It is whether to do so before you are on the hook for it.

Begin with the business model, not the server room

The best technology diligence mirrors how the company makes money. Start with a simple mapping: list the top three revenue streams, then identify the systems and data that enable each one. If 70 percent of revenue comes from ecommerce, the uptime of the storefront, the payment flow, and the order-to-cash integrations matter more than the HRIS. If the company operates field services, mobile dispatch reliability and asset tracking may be the crown jewels.

Ask the seller’s operational leaders, not just IT, to walk you through a week in the life. Where do orders start, how do they travel, where do exceptions occur? Which tasks grind to a halt when one application is down? These conversations quickly reveal single points of failure. I once watched a controller nervously admit that month-end close required exporting a CSV from an ancient accounting package, hand-editing formulas, then emailing the file to a single analyst who “knew the macros.” That is not a spreadsheet problem, it is key-person risk wearing a spreadsheet’s clothes.

As you map, name the dependencies that would take more than two weeks to replace. That time horizon forces clarity. Swapping a printer takes hours, rebuilding a custom warehouse picking workflow with scanner logic and label templates can take months.

Systems and architecture: look for seams

Once you see how work flows, inspect the architecture supporting it. Many small and mid-sized companies live on hybrid stacks, part cloud, part on-premises, often stitched together with one-off scripts. The goal is not to criticize, it is to understand where those seams create fragility.

Four questions uncover most of the risk:

- What are the authoritative systems of record for customers, orders, inventory, and cash? If you hear “it depends,” probe how discrepancies are reconciled.
- How do systems talk to each other? Native connectors, managed iPaaS, nightly file drops, custom code? File transfers and custom code are not inherently bad, but they demand owners, logging, and documentation.
- Where do production workloads run? Public cloud, private datacenter, colocation, a server in the closet? If multiple environments exist, who manages identity and network boundaries?
- What is the backup and restore pattern? Snapshots alone are not a strategy. You want retention windows, offsite copies, and evidence of test restores.

I like to ask for one diagram per critical process, drawn by the people who own it. Whiteboard art says more than Visio files that have not been updated since the last ISO audit. When someone draws a box labeled “custom API,” ask who wrote it and whether the source lives in a repository with version control. Your aim is not to read code, it is to judge whether changes are disciplined or wizard-driven.

Security posture: evidence over assurances

Most sellers will claim they “take security seriously.” Take them at their word, then ask for artifacts. A small packet of recent evidence tells you volumes: a penetration test report less than a year old, a vulnerability scan output with remediation notes, MFA enforcement screenshots from the identity provider, a data classification policy that is more than a template. If the target operates under SOC 2, ISO 27001, PCI DSS, or HIPAA, request the latest reports or attestation letters and the scope statements. Scope creep and out-of-scope systems are where surprises hide.

Expect incomplete answers. In lower mid-market deals, I often find that backups exist, but restores have not been tested for a year, or MFA is active in the core apps but not enforced on remote desktop gateways. Judgment matters here. A gap that can be closed in thirty days with modest effort is a post-close action item. A pattern of gaps with no owners is a cultural problem. Price and reps and warranties can address the first, but the second requires a plan and sometimes a pass.

Ask plainly about incidents in the last three to five years. You want dates, systems affected, data at risk, response steps, and notification decisions. If the seller insists there were “no reportable incidents,” probe how they define reportable. Quiet containment of ransomware by restoring from backup is still an incident. If they paid, you need to know.

Data, privacy, and the legal thread

Data is an asset and a liability. Know what the target collects, where it stores it, how long it keeps it, and what promises it makes in privacy disclosures and contracts. A mismatch between practice and promise becomes your problem on day one.

For consumer data, map obligations under laws that actually apply given the customer base and footprint. California, Virginia, Colorado, Connecticut, and Utah have state privacy laws with different scopes and thresholds. For EU or UK users, GDPR or UK GDPR may bite even if the company is US-based. For B2B, watch for

confidentiality and breach notification clauses in master service agreements. Some contracts require notification within 24 hours of discovering an incident. Others mandate annual audits or specific certifications.

Backup retention and right-to-erasure requests collide more than owners expect. If a customer asks to delete their data, can the company honor the request across production systems and backups without corrupting restore integrity? There is a practical way to handle this, usually by sequestering deletion markers until backups age out, but you should know whether the target has a process or hand-waves the question.

License compliance is another legal thread often missed in Business Acquisition Training. Audit rights from major vendors can turn into six-figure surprises. Ask for a software asset inventory, proof of purchase, and any past correspondence about audits. I have seen a $20 million ARR software firm carry a quiet $400,000 risk due to virtual machine sprawl and misunderstood core licensing. It took three months to right-size.

People, process, and the bus factor

Tools do not run themselves. The reliability of a small company’s tech footprint often depends on two or three people who have been there forever. The bus factor, how many people need to disappear before a critical system becomes unmanageable, tells you how brittle things are.

During diligence, meet the head of IT or the outside MSP and at least one practitioner who actually clicks the buttons. Ask who approves access, who handles change control, and how they document work. If the answer is “we track tickets in email,” you are buying more than a to-do list problem. Probe for cross-training and coverage during vacations. One distribution company I saw relied on a single network admin who also owned warehouse RF scanners. He handled every password reset and switch change. He was conscientious, but he also had 200 hours of unused PTO and a standing fishing trip each June. The first post-close incident would have hit during peak season.

Vendor management is part of this people picture. If the company outsources help desk, infrastructure, or security operations, request the statements of work, SLAs, and termination clauses. If the MSP owns the keys to the kingdom, you need to know how you will transition or retain them. I like to see a list of named individuals with privileged access, whether internal or vendor, and a record of last access reviews. If no one can produce that list, put it on the integration plan.

Cloud is not a synonym for secure

Cloud adoption reduces capital expense and speeds experiments. It also makes it easy to deploy things you cannot see. Many teams spin up services with default settings or leave proof-of-concept resources running long after they serve a purpose. The risks are not exotic. The top three I see repeatedly are public storage buckets with sensitive logs, over-permissive IAM roles that let compromised users pivot, and unpatched virtual machines running in quiet corners of a VPC.

Ask for the target's cloud providers and a high-level inventory of accounts and subscriptions. Does each environment, production and non-production, have a dedicated account? Is identity centralized through a single provider? Are guardrails like SCPs, Azure policies, or organization-level controls in place? If you can, sample a few configurations. You do not need a full cloud security assessment during confirmatory diligence, but you can ask for screenshots of S3 bucket policies, firewall rules, and MFA enforcement for console logins. A few minutes of evidence gathering beats a thousand assurances.

Costs also tell a story. Review the last twelve months of cloud spend. Spikes without corresponding revenue events are worth explaining. Committed use discounts or reserved instances indicate a team that plans. Zombie resources, such as unattached volumes or idle databases, suggest a need for hygiene that you should price into your first hundred days.

On-premises is not a synonym for doomed

Plenty of durable, profitable companies still run their own servers. The risks here tend to stem from aging hardware, end-of-life software, and environmental controls that no one loves to buy until something fails. I once found a core line-of-business server sitting on the floor under a leaky AC unit, with a RAID array that had been in a degraded state for months. Everyone knew it was bad, but no one owned the downtime to fix it.

On-prem diligence is tactile. Ask for the equipment list, warranty status, and OS versions. Look for software beyond vendor support dates. Windows Server releases pass into end of extended support on a cadence, and the difference between "still gets patches" and "out of support" matters. Request photographs of the server room if you cannot visit. A rack with cable management and labeling is not just aesthetics. It signals operational discipline that tends to correlate with better outcomes when things break.

Backups are life support. Confirm where they land, how often they run, and whether one full restore from bare metal has succeeded in the last year. Do not settle for "we back up to the NAS." Back up to what, then to where else? If the building burns, what do you lose?

Product and software risk when tech is the product

If you are Buying a Business that sells software, the diligence bar moves. Code quality, architecture, release cadence, and dependency management all tie directly to enterprise value. You will not fix a brittle monolith in a quarter, but you can price the work.

I like to focus on four signals. First, branch and release discipline in the repository. Are there meaningful code reviews, or is everything green-lighted by the same two people? Second, automated tests and build pipelines. Even lightweight CI tells you the team can change the system safely. Third, third-party component hygiene. Ask for software composition analysis reports or at least a list of top dependencies with versions. Aging frameworks and high-severity CVEs with no remediation plan should trigger questions. Fourth, roadmaps that match customer commitments. When a target promises feature X to a top account by Q2, is that a sales slide or a staffed initiative?

License and IP hygiene deserve their own mention. Confirm contributor agreements, assignment of inventions for employees and contractors, and the use of copyleft licenses that could contaminate proprietary code if misused. This is Business Acquisition Training not scaremongering. It is math. One open-source misstep can turn into a forced disclosure risk that a strategic buyer will punish later.

Ransomware and business continuity: test the story

Ransomware changed the shape of operational risk. It is not enough for a company to say “we have backups.” Attackers target backups first, then encrypt active systems, then call customers if you do not pay. A credible backup strategy includes offline or immutable copies, segmented admin credentials, and a recovery plan that has been walked through end-to-end. Ask how long it would take to rebuild the most critical system from scratch, not just restore data. Times that feel optimistic probably are.

Business continuity plans often live as binders on shelves. Better to ask how the company handled the last real outage. How did they communicate with customers, what manual processes kicked in, what changed afterward? A manufacturer I worked with suffered a weekend ransomware event. They shipped Monday because the plant manager kept paper travelers and the ERP admin had a golden image of the app server. Their recovery was messy, but muscle memory saved them. You want to know where muscle memory exists and where it does not.

Quantify what you can, rank what you cannot

You will not turn every risk into a dollar figure during diligence, but you can organize them so decision-makers know what matters. Group findings by business impact and effort to remediate. High impact and low effort items become immediate asks in the purchase agreement or day-one actions. High impact and high effort items may justify price adjustments, escrows, or specific indemnities. Low impact items become integration backlog. Avoid burying executives in a 60-line spreadsheet of CVEs. Tell a story: what could stop the cash register from ringing, what could force a breach notification, what could delay integration plans.

The ranges can be concrete. A move from single-factor VPN access to MFA across the fleet might cost ten to thirty thousand dollars depending on user count and tool choice. Replacing an end-of-life firewall could be five to fifteen thousand plus labor. Replatforming an ecommerce site off a self-hosted CMS to a managed platform can run into six figures and several months. No need to be precise in diligence, but be honest about order of magnitude.

Build the right team for the size of the deal

Not every acquisition needs a Big Four-style cyber assessment. Scale your approach. For a sub-$5 million EBITDA target with straightforward IT, a focused external review, a few interviews, and selective artifact sampling can surface the main risks in two to three weeks. For a software product company or a regulated data processor, add specialist threads such as secure SDLC review, privacy counsel, and cloud posture assessment. In Business Acquisition Training, teach associates to recognize signals that warrant escalation. A shared admin password written on a whiteboard is not a cute anecdote. It is an escalation.

Where possible, separate seller-facing requests from back-channel checks. Public breach databases, ASN records, SSL certificate histories, and even job postings can give you a sense of the environment without spooking operators. Keep the tone collaborative. You are not trying to embarrass the team that built the business. You are trying to ensure that you can steward it well.

Integrate cyber diligence with the purchase agreement

Findings without levers change nothing. If you discover material risks, work with counsel to reflect them in the agreement. Reps and warranties can address past compliance and undisclosed incidents. Specific covenants can require the seller to complete certain remediations pre-close, such as enabling MFA for remote access or delivering a clean bill of health from a license audit. Escrows or holdbacks can protect against near-term known-unknowns like pending vendor audits or in-flight migrations. Be practical. For a mature team, a joint remediation plan tied to integration milestones may build more trust than trying to cram pre-close fixes into a narrow window.

A lightweight, high-yield diligence sequence

When time is tight and access is limited, a crisp sequence gets you 80 percent of the insight. Here is a compact flow that has worked across dozens of deals:

- Map revenue to systems by interviewing operations and sales leaders. Identify crown jewels and the two or three processes that cannot fail.
- Request core artifacts: network and application inventories, backup policies, most recent pen test or vulnerability scan, access control overview with MFA enforcement, and any security certifications or audits with scopes.
- Hold a working session with IT or the MSP to walk through identity, remote access, backups, and incident history. Ask for evidence, not just narratives.
- Sample the cloud or on-prem environment with targeted checks. Think storage access policies, IAM role summaries, firewall rules, and backup restore logs.
- Convert findings into a short risk memo with business impact, remediation effort ranges, and proposed levers for the agreement or the day-one plan.

That five-step path fits inside typical confirmatory windows and leaves room for depth where red flags emerge.

The hidden costs of technical debt, and when to pay them

Technical debt is not a moral failing. It is a series of trade-offs made under constraints. The problem is compounding interest. A brittle integration that requires a weekly manual fix steals time and creates error risk. An outdated framework may still run, but it pushes you off the upgrade path and limits hiring. The fix is not “rewrite everything,” it is to decide, with eyes open, where to spend. In one carve-out, we lived with an old warehouse management system for a year, paying a small tax in manual reconciliation, so that we could first centralize identity and endpoint management. That sequence reduced attack surface and sped later migrations.

When deciding what to fix first, triangulate on three questions. Does this risk threaten cash flow if it fails? Does it increase the likelihood or impact of a security incident? Does it block planned growth or integration? If the answer is yes to any, move it up. If no to all, park it behind customer-facing improvements that unlock revenue.

Culture, not just controls

Security and reliability flow from culture more than from tools. You can sense culture in small things. Are laptops encrypted by default, or do people find workarounds to avoid reboots? Do admins push back on exceptions, or does every VIP get a pass? Are post-incident reviews blameless and documented, or does everyone try to forget? A company that fixes the root cause of a small defect usually treats bigger risks with respect. One that celebrates heroics but never reduces toil will keep producing fires for your team to fight.

As a buyer, you will import this culture. If it is healthy, protect it. If it is brittle, plan for change management alongside technical fixes. That might mean early wins like rolling out a password manager, publishing a simple security handbook, or scheduling lunch-and-learns where engineers explain how a breach unfolds. You are not just buying systems. You are hiring habits.

Red flags that should slow you down

Plenty of gaps are normal. A few patterns should make you pause. No one can produce a list of systems. There is no inventory of users with admin access. Backups exist but have never been test-restored. A recent pen test

identified high-severity issues with no remediation plan. The company processes payment cards, but no one knows what PCI scope means. The product team cannot run a build without a specific developer present. The MSP resists giving visibility into configurations or deflects with jargon. None of these automatically kill a deal. Together, they suggest a risk you must price and plan for.

Turning diligence into advantage

The immediate goal is to avoid surprises. The longer-term gain is differentiation. Buyers who can credibly assess, prioritize, and fix technology and cyber risk win more often, pay appropriately, and integrate faster. Lenders and insurers notice. So do sellers. Operators who built resilient systems want stewards who will respect them. Teams that struggled want partners who will help without blame.

If you run a Business Acquisition Training track, treat technology and cyber risk as core deal work, not an IT side quest. Teach associates to translate technical findings into business language, to ask for evidence with respect, and to weigh trade-offs without drama. If you are Buying a Business, invest early in your playbook. Even a short one, reused and refined across deals, will save you multiples of the time it took to write.

You do not need to become a CISO or a CTO to make good calls. You do need to ask clear questions, insist on artifacts, and keep your eye on how systems serve revenue, customers, and trust. The rest is craft, built one careful deal at a time.