Technology Due Diligence Checklist for PE Acquisitions:

What to consider in a target's technology today, and how AdvancedBITS helps you improve it

By AdvancedBITS | Business IT Solutions • About 6 minutes to read

> **Quick answer: what is technology due diligence for a PE acquisition?**
>
> **Technology due diligence** for a private equity acquisition is a structured review of a target's systems, security, data, AI use, vendors, and recovery capability. It confirms the technology can carry the value creation plan, puts a cost on what needs fixing, and sets up Day 1. It works best when it runs alongside financial and legal diligence, not after it.

This brief overview covers why it matters, ten areas to consider in the target as it stands today, and how AdvancedBITS helps you improve each one. A full working checklist (14 workstreams, 119 items, with evidence to request and red flags) is available separately.

General information about technology risks, not legal, tax, investment, or insurance advice. Counsel decides what the deal documents should say. Red flags are prompts for further inquiry, not automatic dealbreakers.

Why does technology diligence matter now?

Short answer: cyber and technology problems now show up in price, exit value, and litigation, and a deal team can inherit a problem that predates the deal. Each statistic appears once, here.

Finding	Source	Why it matters
Kroll surveyed 325 PE executives. 94% of firms absorbed financial losses from cyber risk, with an average impact of $2.1 million per incident and a 13% chance of losses above $5 million.	Kroll press release, Feb. 11, 2026; report page. Primary. Survey.	Cyber loss is a normal cost of PE ownership.
81% of firms with more than $25 billion in assets say cyber diligence is standard in their deals, versus 29% of smaller firms.	Kroll press release. Primary. Survey.	Smaller sponsors report less formal diligence.
On March 18, 2026, a federal court let negligence and other claims against Bain Capital proceed in part in the PowerSchool breach litigation. Plaintiffs allege Bain conditioned its offer on cost reductions, including layoffs of domestic cybersecurity staff, and later directed offshoring of security and IT functions. These are allegations in an ongoing case.	Court order. Primary. Allegation detail: Womble Bond Dickinson alert, via Data Breach Times. Secondary.	A sponsor's own plan can become part of the case.
Marriott acquired Starwood in 2016. The UK regulator found Starwood's systems were compromised in 2014 and that Marriott did not detect it until September 2018. Marriott was fined £18.4 million. In 2024 the FTC and 49 states plus D.C. settled, with $52 million to the states, and the FTC complaint cited the diligence timeline.	ICO penalty notice; Marriott statement; Alston & Bird summary. Primary and secondary.	An old compromise becomes the acquirer's problem.
In codebases audited for M&A transactions, Black Duck reports open source license conflicts in 94% of transactions and unpatched vulnerabilities in 97%.	Black Duck M&A page. Vendor-reported, not independently verified.	Code audits find issues in nearly every deal. Price them.

What should you consider in the target's technology today?

Short answer: ten areas, each with a question to ask, a red flag to watch for, and the help AdvancedBITS provides. The last column is how we will help you improve the area, before signing or after closing.

Area	What to consider	Common red flag	How AdvancedBITS helps
1. Deal fit and value plan	Does the technology support the growth case? Which plan actions touch security, IT staffing, or vendors?	Growth targets the systems cannot support; cost cuts that reach security with no risk review	Technology and compliance readiness assessment tied to your value creation plan
2. People, spend, key-person risk	Who runs IT, who holds administrator access, and what is the real spend and deferred capex?	A sole administrator; credentials outside a vault; deferred refresh	IT operations review and roadmap; co-managed IT alongside the target's team, or full management
3. Applications and software	Are core systems supported and able to scale? For software targets, who owns the code and what is inside it?	Systems past vendor support; code nobody understands; unreviewed AI-generated code	Application and technical-debt inventory with cost estimates; specialist code review brought in for software targets
4. Infrastructure, cloud, network	Is hardware supported, cloud governed, and the network segmented?	End-of-life servers; flat network; unmanaged cloud accounts	Infrastructure and cloud assessment; 24-month refresh and capex view
5. Cybersecurity and identity	Is MFA on every key account? Are flaws patched, endpoints and email protected, and activity monitored? Is there any sign of an existing compromise?	No MFA on email or administrators; unpatched known flaws; unexplained remote-access tools	Security risk assessment and program review; Microsoft 365 and identity review; MFA, endpoint and email security, monitoring
6. Data, privacy, compliance	What data does the target hold, and what has it promised customers?	No data map; uncapped liability for data incidents in customer contracts	Compliance readiness assessment; data and access review (counsel decides which laws apply)
7. AI use and readiness	Which AI tools are in use, approved or not? Is there a policy, and do customer or NDA terms restrict AI?	Public chatbots on personal accounts; AI features switched on by default	AI readiness assessment, shadow AI discovery, and acceptable-use policy support
8. Vendors and contracts	What do change-of-control, license, and exit terms allow? Who has access to the target's systems?	Consent rights triggered by the deal; standing vendor access with shared credentials	Vendor and third-party risk review
9. Backup, recovery, continuity	Are backups tested, including Microsoft 365 data? Can the business meet its recovery goals?	Restores never tested; backups deletable with the same administrator account	Backup and recovery validation; continuity and incident response planning; cyber insurance readiness review
10. Integration, cost-to-fix, exit	What must work on Day 1? What do the findings cost? What will the next buyer ask for?	Findings with no cost estimate; no Day-1 owner; evidence gathered in a rush at exit	Day-1 and 100-day plan; NIST CSF and CIS Controls alignment; SOC readiness; board-ready documentation

For cybersecurity, many teams use the NIST Cybersecurity Framework 2.0 (Govern, Identify, Protect, Detect, Respond, Recover) as the yardstick.

How does AdvancedBITS help at each stage of the deal?

Short answer: we help you see the target clearly before signing, fix the most important gaps in the first 100 days, and build the evidence that supports the exit. The stages below are an illustrative AdvancedBITS framework.

Stage	What we do
Before signing	Assess the target against the ten areas above, rank findings by severity, estimate what each costs to fix, and flag what belongs in the deal terms. Counsel decides the final protections.
Day 1 to Day 100	Lock down access with MFA and identity controls, add endpoint, email, and monitoring protection, validate backups, review vendor access, and set a security gate before the target connects to your platform.
Hold period and exit	Standardize security across the portfolio, report a short set of technology metrics to the board, and keep the documentation current so the next buyer's diligence goes smoothly.

For independence, you can contract the assessment separately from any remediation work. We do not give legal advice.

Frequently asked questions

What is technology due diligence in a private equity acquisition?

Technology due diligence in a private equity acquisition is a structured review of a target's applications, infrastructure, cybersecurity, data, AI use, vendors, and recovery capability. It confirms the technology can support the value creation plan, estimates the cost of fixing problems, and plans Day 1. It runs alongside financial and legal diligence and ends in findings the investment committee can act on.

What should a PE technology due diligence checklist cover?

A checklist should cover deal fit, IT people and spend, applications and software, infrastructure and cloud, cybersecurity and identity, data and privacy, AI use, vendors and contracts, backup and recovery, and integration and exit readiness. For each item, list the evidence to request and the red flag to watch for, then turn findings into costs and deal terms.

Should a private equity firm run a compromise assessment before closing?

A compromise assessment is an independent search of a target's systems for signs of an existing or past intrusion. It matters because a compromise can predate a deal and go unnoticed, as the Marriott and Starwood case shows. Scope it in writing with the seller, have counsel confirm permissions, and treat unexplained administrator accounts or remote-access tools as findings to investigate.

Does a SOC 2 report mean a target is secure?

No. A SOC 2 report is an independent CPA firm's report on controls within a defined scope, either at a point in time (Type I) or over a period (Type II). The AICPA says SOC services should be thoroughly evaluated. Check the period, scope, exceptions, and auditor, and confirm it covers the systems that matter to your thesis.

AdvancedBITS | Business IT Solutions
Secure. Compliant. Outcome-Focused.
sales@advancedbits.com | www.advancedbits.com | 561-300-3015

Sources

Read survey and vendor figures as directional. The Bain/PowerSchool facts are allegations in an ongoing case, and the Black Duck figures are vendor research. The ten areas, stages, and service mapping are illustrative AdvancedBITS frameworks.

- Kroll press release; Kroll report page
- Bain/PowerSchool court order (Mar. 18, 2026); Womble Bond Dickinson alert, via Data Breach Times
- ICO Marriott penalty notice; Marriott statement; Alston & Bird on the FTC and state settlements
- Black Duck M&A page; NIST Cybersecurity Framework; AICPA SOC suite