KENNEDY ADVISORY

INVESTOR CHECKLIST

Technology Due Diligence Checklist

What investors and acquirers should examine in a target's technology, security and AI posture — and where the cost surprises usually hide.

Michael Kennedy · Former Group CIO, Robert Walters · Singapore / Global · July 2026

THE POINT OF TECH DD

Technology due diligence is priced-risk discovery — not an IT audit.

The question is never "is the technology good?" It is: **what will it cost to make this platform do what the deal thesis needs it to do?** A dated but stable estate may be fine for a cash-flow play and fatal for a growth thesis. Every finding in a tech DD should convert into one of three things: a price adjustment, an SPA protection, or a line in the 100-day plan.

This checklist covers the eight areas that decide most deals — including the AI exposure section that most DD processes still miss — plus the questions worth asking management directly.

AREA 01

Strategy and spend

- [ ] IT spend as a percentage of revenue, benchmarked against sector — and the trend over three years, not the snapshot.
- [ ] Run vs change split. A business spending 95% on keeping the lights on has no capacity to deliver the thesis.
- [ ] Capitalisation policy: is “efficiency” actually deferred investment dressed up as discipline?
- [ ] Does the technology roadmap exist, and does it support or contradict the investment thesis?

> **Where the cost hides:** Three years of under-investment presents as an attractive cost ratio. The catch-up bill lands in your hold period.

AREA 02

Architecture and technical debt

- [ ] Age and support status of core platforms. Demand the end-of-life register; if there isn’t one, that is a finding in itself.
- [ ] Single points of failure — systems, data centres, and the undocumented middleware everything secretly depends on.
- [ ] Scalability against the thesis: can the platform handle 3x volume, a new market, a new product line? Ask for evidence, not assurance.
- [ ] Release cadence and change failure rate — the most honest proxy for engineering health.

> **Where the cost hides:** The core system “rewrite that’s nearly done”. It never is. Price it as if it hasn’t started.

AREA 03

Cybersecurity

- [ ] Certifications actually in force — and their **scope**. An ISO 27001 certificate covering one office is marketing, not assurance.
- [ ] Incident history including near misses, and whether the cyber insurance policy has ever been claimed against.
- [ ] The basics that predict everything else: MFA coverage, patching cadence, privileged access management, tested backups.
- [ ] Outstanding audit or penetration test findings, their age, and their owners.

> **Where the cost hides:** A breach discovered post-completion that predates the deal. Warranties help; a proper look before signing helps more.

AREA 04

Data and intellectual property

- ☐ Does the target actually own its code and data? Contractor agreements, offshore development and legacy licensing are where ownership quietly leaks.
- ☐ Open-source licence exposure — copyleft components in proprietary products can compromise the IP the deal is buying.
- ☐ Data quality versus the promised analytics value. “We have ten years of customer data” usually means ten years of inconsistent, duplicated records.
- ☐ Cross-border data flows and residency obligations — decisive in APAC deals, where regimes differ sharply by market.

> **Where the cost hides:** The analytics upside in the model assumes data the target cannot legally use, or cannot practically clean, in the hold period.

AREA 05

Team and key-person risk

- ☐ The depth chart: who could not be replaced within 90 days, and what do they uniquely know?
- ☐ Contractor dependency — headcount charts flatter permanent staffing while the platform is actually run by day-rate contractors who owe you nothing.
- ☐ Retention risk on announcement. Deal news makes technologists take recruiter calls; who needs locking in, and what will it cost?
- ☐ The technology leadership itself: is the incumbent CIO/CTO part of the thesis, or part of the risk?

> **Where the cost hides:** Retention packages for five engineers is noise in the deal model — losing the three people who understand the core platform is not.

AREA 06

Vendors and contracts

- ☐ **Change-of-control clauses** — the classic post-signing surprise. Key suppliers may be entitled to re-price or terminate on completion.
- ☐ Concentration risk: any vendor whose failure or price rise would be material, and the realistic cost of switching.
- ☐ Source-code escrow on business-critical software from small vendors — and whether it has ever been verified.
- ☐ Auto-renewals and termination notice periods falling inside the first 12 months of ownership.

> **Where the cost hides:** A single change-of-control re-price on a core platform can exceed the entire projected IT synergy line.

AREA 07

AI exposure — the section most DD misses

- [ ] AI claims versus reality. If the deck says “AI-powered”, establish whether that means a proprietary capability or an API call to someone else’s model.
- [ ] Model provenance and dependencies: whose models, on what terms, and what happens commercially if the provider re-prices or withdraws?
- [ ] Training data rights — was the model trained on data the target had the right to use? This is tomorrow’s litigation risk, priced today.
- [ ] Ungoverned internal AI use: what staff are pasting into public tools today is a live data-leakage exposure you inherit at completion.
- [ ] Regulatory exposure of AI-assisted decisions in the target’s markets — especially credit, hiring, insurance and healthcare use cases.

> **Where the cost hides:** Valuation credit given for “AI capability” that is a thin wrapper on a third-party model with no moat, no data rights and no switching cost for customers.

AREA 08

Integration and separation

- [ ] For carve-outs: TSA scope, duration and true exit cost. TSAs always run longer and cost more than the deal model says.
- [ ] Day-one plan for identity, email and access — the thing customers and staff actually notice.
- [ ] Synergy assumptions tested by someone who has delivered them. “Consolidate the ERPs” is a sentence in a deck and a two-year programme in reality.
- [ ] Who pays for remediation of everything found above — and is it in the price, the SPA, or the 100-day plan?

IN THE ROOM

Five questions to ask management directly

Answers matter less than fluency. Hesitation on these is data.

- [ ] “What would you fix first with £1M and no oversight?” — reveals the real debt register.
- [ ] “What broke last year that we won’t find in the data room?”
- [ ] “Which single person’s resignation would hurt most, and why?”
- [ ] “Which vendor relationship keeps you awake?”
- [ ] “Where does the roadmap disagree with what the owners want to hear?”

> **Turning findings into value:** every material finding should land in one of three places — the price, the SPA (warranties, indemnities, escrow), or the 100-day plan with a named owner and budget. A finding that lands nowhere was not worth finding.

ABOUT THE AUTHOR

Michael Kennedy is the founder of Kennedy Advisory and former Group CIO of Robert Walters, where he led a 150+ person technology organisation across 14 countries, delivered £3M+ in annualised savings,

achieved ISO/IEC 27001 across all jurisdictions and took AI safely into production. He is CISSP certified and based in Singapore with a global remit.

Working through this for real?

Independent judgement on technology, cyber risk and AI — as an interim or fractional CIO, or at the board table. Engagements start with a conversation, not a proposal.

michael@kennedyadvisory.co · kennedyadvisory.co · Singapore / Global