Anyway Ventures

PRIVATE EQUITY · VC · CORPORATE ACQUIRERS · 2026 EDITION

Technical due diligence *checklist*.

Twelve areas, 107 numbered data-room requests, an interview plan by role and a costing method that turns findings into price, SPA protection, conditions or a 100-day plan. Built for deal teams who need to know which two answers out of fifty change the number.

PDF GUIDE | EXCEL WORKBOOK

AUTHOR

Brannan Coady, Anyway Ventures

EDITION

Version 1.0 · October 2026

ONLINE, WITH DOWNLOADS

anywayventures.com/resources/technical-due-diligence-checklist

CONTACT

brannan@anywayventures.com

Free to use, adapt and share with attribution · Not legal, tax or investment advice

CONTENTS

In this guide

1. Executive summary
2. How to use this checklist
3. What changed in 2026
4. The checklist on one page
5. Architecture and scalability
6. Code quality and technical debt
7. Team, delivery and key-person risk
8. Security
9. Data protection and privacy
10. IP, open source and AI-generated code
11. Infrastructure, cloud and cost to run
12. Product and roadmap
13. Third parties, vendors and contracts
14. IT and internal systems
15. AI and data
16. Integration and the first 100 days
17. Data-room request list
18. Interview plan and questions by role
19. Severity and costing method
20. Red-flag, full and vendor scoping
21. Sector variants
22. Worked example
23. Red flags that should stop or reprice a deal
24. Common mistakes
25. Glossary
26. Sources and further reading
27. About this resource

About Anyway Ventures

WHO IT IS FOR

Deal teams, operating partners, VC investors, corporate development teams, deal lawyers, CTOs preparing for a sale

ALSO AVAILABLE

PDF guide, Excel workbook at anywayventures.com/resources/technical-due-diligence-checklist

KEY TAKEAWAYS

The short version

1. The Anyway Ventures technical due diligence checklist covers twelve areas, from architecture and code to AI claims and the first 100 days, with 107 numbered data-room requests and an Excel workbook.

2. Every technical due diligence finding needs a pound figure and a route, and annual costs count at the multiple: an ignored £80k yearly inference bill is £960k of enterprise value at 12 times EBITDA.

3. Key-person risk and IP ownership are the most common price-moving findings on lower mid-market deals, so make access transfer and confirmatory IP assignments conditions of completion, not 100-day actions.

4. Black Duck's 2026 audit of 947 commercial codebases found open source licence conflicts in 68%, up from 56% a year earlier, partly from AI tools reproducing code without its licence.

5. Front-load technical due diligence by sending the P1 data-room requests on day one, interviewing engineers in week one and giving the deal team a red-flag note with rough costs by the end of week one.

This is a complete technical due diligence checklist and data-room request list for private equity, venture and corporate acquirers buying or investing in software and tech-enabled businesses. It covers twelve areas, from architecture and code to AI claims and the first 100 days, and for each one sets out what to check, the evidence to request, what good looks like, the red flags and where each finding should land in the deal. It comes with 107 numbered requests ready to paste into a tracker, an interview plan by role, a costing method, sector variants and a worked example, plus an Excel workbook that totals findings by area, severity and route.

1. Executive summary

1. **Every finding needs a pound figure and a route, or it is an observation.** The routes are price (including debt-like items and run-rate EBITDA), a condition of completion, a specific warranty or indemnity in the SPA, structure (retention, escrow, deferred consideration, earn-out terms), the 100-day plan, or the file. A checklist that ends in a red, amber and green grid has not done the job.
2. **Annual costs are worth the multiple, not their face value.** An inference bill of £80k a year that the plan ignores is £960k of enterprise value at 12 times EBITDA. One-off remediation is worth roughly what it costs. Most deal teams treat the two the same, and the gap is usually where the money is.
3. **Ask for evidence, not documents.** A policy says what should happen. A deployment log, a cloud bill, a commit history and a restore test show what did. Where only the policy exists, that is a finding.
4. **Key-person risk and IP ownership are the most common price-moving findings on lower mid-market deals.** Both are cheap to find and cheap to fix before completion, and expensive after. Make access transfer and confirmatory IP assignments conditions of completion, not 100-day actions.
5. **Open source and AI-generated code have changed the IP picture.** Black Duck's 2026 audit of 947 commercial codebases found licence conflicts in 68%, up from 56% a year earlier, and linked part of the rise to AI tools reproducing code without its licence (Black Duck, 2026). A dependency scan is no longer optional.
6. **Test the AI story on real data.** Ask for usage, cost per call and the model behind each feature. If the CIM says "AI-powered" and nobody can show last month's usage, discount the revenue that depends on it.
7. **Front-load the work.** Send the P1 requests on day one, interview engineers in week one, and give the deal team a red-flag note with rough costs by the end of week one. Findings that move price take longest to negotiate.
8. **Scope to the question, not the fee budget.** A five-day red-flag review answers "should we keep going, and at what price?" A full review gives lawyers, lenders and insurers something to rely on. A vendor review lets a seller fix the cheap problems before a buyer prices them.

2. How to use this checklist

Who it is for. Deal partners and associates who need to commission, scope or challenge technical due diligence. Operating partners who inherit the findings. Corporate development teams running acquisitions without a specialist adviser. Deal lawyers turning findings into SPA drafting. CTOs and founders preparing for a sale, who can run it on themselves first. VC investors can use the red-flag subset for Series A and later rounds; the VC technical due diligence page sets out the lighter version.

When to use it. Pre-LOI, use the executive summary and the P1 requests to frame questions for management. In exclusivity, use all of it. Sellers should run it three to six months before a process, which is long enough to fix missing IP assignments, open pen test findings and single-person admin access before a buyer finds them.

How long it takes. A red-flag review of a single-product business with up to 15 engineers takes five to seven working days. A full review takes two to three weeks. Larger, multi-product or carve-out targets take four to six weeks. The clock starts when code and people are available, not when the engagement letter is signed. Fees and published price points are compared in how much technical due diligence costs in the UK.

Inputs you need. The investment case (the growth, product and margin assumptions the technology must support), read-only repository access, the data room, four to seven interviews, and the target's salary bands so you can cost findings in its own money.

How it connects to the workbook. The Excel companion has five working tabs. The request list holds all 107 items from the data-room request list below, with the same IDs, plus dates, owner, status and a days-open counter. The findings register takes each finding with its area, severity, cost range, cost type and route. The dashboard totals both, by area, severity and route, and capitalises annual costs at the entry multiple you enter. The reference tab holds the severity and route definitions from the costing method and a calculator for engineer-time estimates. The example tab is the Northgate worked example, filled in.

A three-week plan

WHEN	WHAT HAPPENS	OUTPUT
Day 1	Send P1 requests; agree interview list and confidentiality circle; request read-only code access	Request list sent
Days 2 to 5	First CTO session; engineer interviews; commit history and access review; dependency scan; cloud bill read	Working findings log
Day 5 to 7	Red-flag note to the deal team, each item with a rough cost and proposed route	Two to five page note
Week 2	P2 requests; security and data protection review; product and roadmap testing; AI claims tested on live data	Draft findings register
Week 3	Second CTO session to raise findings; factual accuracy check with management; costing finalised	Final report and 100-day plan

3. What changed in 2026

Four things move this checklist on from the versions most firms still circulate.

68%

of 947 audited commercial codebases had open source licence conflicts, up from 56%. Black Duck, 2026

43%

of UK businesses identified a cyber breach or attack in the last year, 65% of medium and 69% of large ones. DSIT, 2026

15%

of UK businesses had reviewed the cyber risks of their immediate suppliers. DSIT, 2026

18%

of UK breaches started with a third-party vendor or supply chain compromise, the most common cause. IBM, 2025

AI-written code. Black Duck's 2026 Open Source Security and Risk Analysis found that 17% of open source components entered codebases outside package managers, through copied snippets or AI generation, and that only 54% of organisations evaluate AI-generated code for IP and licensing risk. The same audit found high-risk vulnerabilities in 78% of codebases and components four or more years out of date in 92%. Google's 2025 DORA report put AI use among developers at 90%. The question is no longer whether a target uses AI to write code, but whether its review, testing and licence scanning kept pace.

UK data protection reform. Most of the Data (Use and Access) Act 2025 data protection changes came into force on 5 February 2026, and the duty to run a data protection complaints procedure (acknowledge within 30 days, investigate without undue delay) has applied since 19 June 2026, as Mishcon de Reya set out in 2026. Ask for the complaints log as well as the breach log.

EU product and AI rules. For targets selling into the EU, Cyber Resilience Act reporting duties for products with digital elements started on 11 September 2026, with the remaining obligations from 11 December 2027 (Skadden, 2026). Under the EU AI Act, the Digital Omnibus pushed high-risk obligations for Annex III systems to 2 December 2027 and for Annex I products to 2 August 2028 (Gibson Dunn, 2026). The EU Data Act's cloud switching rules have applied since 12 September 2025, and switching charges are largely prohibited from 12 January 2027 (Latham & Watkins, 2025), which matters for any SaaS target whose retention depends on high exit costs for EU customers.

Enforcement against software suppliers. In March 2025 the ICO fined Advanced Computer Software Group £3.07m, after a 2022 ransomware attack that came in through a customer account without multi-factor authentication (ICO, 2025). Software businesses that process data for customers carry their own exposure, and MFA coverage on customer-facing admin accounts is now a P1 request.

4. The checklist on one page

AREA	THE QUESTION THE INVESTMENT COMMITTEE NEEDS ANSWERED	MOST COMMON ROUTE
Architecture and scalability	Can the platform carry the growth and product changes in the plan?	Price (known capex), 100-day plan
Code quality and technical debt	How much of next year's engineering capacity is already spent?	Price (debt-like item)
Team, delivery and key-person risk	Does the product survive any one person leaving?	Structure, condition
Security	Is there an unreported incident or an open door?	Condition, specific indemnity
Data protection and privacy	Is personal data handled lawfully, and is the paperwork real?	SPA protection, 100-day plan
IP, open source and AI-generated code	Does the target own what it sells?	Condition, specific indemnity
Infrastructure, cloud and cost to run	Is cost to serve under control and is the business recoverable?	Run-rate EBITDA, 100-day plan
Product and roadmap	Does the revenue plan depend on things that do not exist yet?	Price (model adjustment)
Third parties, vendors and contracts	Could one supplier or customer contract stop or reprice the business?	Condition, SPA protection

AREA	THE QUESTION THE INVESTMENT COMMITTEE NEEDS ANSWERED	MOST COMMON ROUTE
IT and internal systems	Do the back-office systems and devices hold up, and what does separation cost?	100-day plan, TSA
AI and data	Is the AI real, used, affordable and governed?	Price (model adjustment), disclosure
Integration and the first 100 days	What has to happen between signing and day 100, and what will it cost?	100-day plan

Severity labels used throughout are critical, high, medium and low, defined in the severity and costing method. Each area's evidence column references the request IDs in the data-room request list.

5. Architecture and scalability

The question is whether the platform can carry the volume and the product changes in the investment case, and if not, what breaks first and what fixing it costs. Start with the plan, not the diagram: if the model assumes 2.5 times the customers and an enterprise tier, test for those two things.

Items to check

- ☐ The architecture diagram matches what engineers describe and what the cloud console shows
- ☐ The tenancy model, and the marginal cost and effort of onboarding one more customer
- ☐ The first bottleneck at two and five times current volume, as named by the team
- ☐ Customer-specific branches, forks or bespoke installs, and how many customers sit on them
- ☐ Availability against SLA for 12 months, and whether incidents have root-cause write-ups
- ☐ Integration surface: public APIs, partner integrations and how breaking changes are handled
- ☐ Whether the architecture supports what the plan needs next (enterprise SSO, data residency, multi-region, new product lines)

Evidence, good and red flags

EVIDENCE	WHAT GOOD LOOKS LIKE	RED FLAG
Team-drawn diagram and inventory (ARC-01, ARC-02)	Drawn recently by engineers; matches the console and interviews	Only the CIM version exists, or engineers contradict it
Tenancy model (ARC-03)	Shared infrastructure with logical isolation; onboarding is configuration	A new database, server or deployment per customer, done by hand
Incident log and availability (ARC-04)	SLA met; incidents written up with causes and fixes	Repeated incidents with the same cause; no write-ups
Bespoke code (ARC-05)	One codebase; customer differences in configuration	Forks per customer, each needing its own upgrades
Bottleneck view (ARC-07)	Named component, rough plan and cost, headroom matching the plan	"It scales" or "it's in the cloud"

Severity and deal route

FINDING	TYPICAL SEVERITY	LIKELY ROUTE
Platform cannot carry the plan's volume without re-architecture	Critical or high	Price as known capex; re-base the plan's timing
Single-tenant installs that make each customer a deployment	High or medium	Price or 100-day plan, depending on when growth bites

FINDING	TYPICAL SEVERITY	LIKELY ROUTE
Customer forks requiring separate maintenance	Medium	100-day plan; warranty on disclosed customisations
Missing incident write-ups, no capacity testing	Low	File, 100-day plan

6. Code quality and technical debt

The question is how much of next year's engineering capacity is already committed to keeping the lights on, and what has to be rebuilt before the plan can happen. Technical debt should be costed, not described. Treat test coverage and static analysis scores as signals: modest coverage of billing and permissions beats high coverage of trivial code.

Items to check

- ☐ Components on unsupported or end-of-life versions (languages, frameworks, databases, operating systems)
- ☐ The team's own debt list, and whether it is willing to write one down
- ☐ Share of engineering time on maintenance, support and bugs against new features
- ☐ Tests on the code that matters most: billing, permissions, the core data model, integrations
- ☐ Deployment pipeline: automated build, test and deploy, and how often it runs
- ☐ Code review practice, including for AI-assisted code
- ☐ Capitalised development costs, and whether capitalised work is still in use

Evidence, good and red flags

EVIDENCE	WHAT GOOD LOOKS LIKE	RED FLAG
Repository access (COD-01)	Full history; readable code; consistent structure	Access refused, or a curated copy without history
End-of-life list (COD-02)	Short, known and scheduled	Core product on a framework out of support with no plan
Debt list (COD-03)	Written, prioritised, roughly estimated	"We don't have much debt" alongside a feared, untouched module
Maintenance split (COD-06)	Well under half of engineering time on maintenance	Most capacity on support and fixes, so the roadmap is fiction
Deployment logs (COD-05)	Several deploys a week, automated, low failure rate	Monthly manual releases run by one person
Capitalised development (COD-07)	Policy applied consistently; assets in use	Capitalised spend on abandoned work, flattering EBITDA

Severity and deal route

FINDING	TYPICAL SEVERITY	LIKELY ROUTE
Rewrite or major upgrade needed before the plan's product changes	High	Price as a debt-like item; 100-day plan
Maintenance consumes most engineering capacity	High or medium	Price via slower roadmap in the model
Capitalised development on work no longer in use	Medium	Quality of earnings adjustment; flag to financial DD
Weak tests on billing or permissions	Medium	100-day plan
No staging environment, manual releases	Medium or low	100-day plan

7. Team, delivery and key-person risk

The question is whether the product survives any one person leaving, and whether the team can deliver the roadmap at the speed the plan assumes. Research on 133 popular GitHub projects found 65% had a truck factor of two or less (Avelino and others, ICPC 2016), and MIT research on around 4,000 US startup acquisitions found 33% of acquired workers left within a year (MIT Sloan, Kim). A deal gives people the money and the moment to leave. The full method is in key person risk in due diligence.

Items to check

- ☐ Commit history by area (billing, permissions, core data model, integrations, infrastructure) over 12 to 24 months
- ☐ Who owns and administers the cloud root account, code hosting, domain and DNS, app stores, payments, identity and secrets
- ☐ Contractors and agencies who hold knowledge, with notice terms
- ☐ Who resolves serious incidents, and whether the on-call rota has at least three people
- ☐ Onboarding documentation that someone other than its author has used
- ☐ Attrition over two years and the reasons
- ☐ Retention, notice periods, restrictive covenants and post-deal incentives for key people
- ☐ Delivery metrics: deployment frequency, lead time, change fail rate and recovery time, as defined by DORA

Evidence, good and red flags

EVIDENCE	WHAT GOOD LOOKS LIKE	RED FLAG
Commit history (COD-01)	At least two active contributors on every critical area	One author behind most changes to billing or the core data model
Admin list (TEA-03)	Company-owned accounts, two or more admins, MFA	Personal email or card on the domain or cloud root account

EVIDENCE	WHAT GOOD LOOKS LIKE	RED FLAG
Contractor list (TEA-02)	Contractors on defined work with assignments and handover	Long-serving contractor wrote the core, short notice, no assignment
Incident and on-call data (TEA-07)	Serious incidents resolved by different engineers	Same name on every incident, including weekends
Contracts and incentives (TEA-04, TEA-05)	Notice and covenants match the 100-day plan; rollover or retention in place	Large cash-out at completion, three months' notice, no reason to stay
Leavers (TEA-06)	Low churn; explainable departures	Several senior engineers left for the same reason

Severity and deal route

FINDING	TYPICAL SEVERITY	LIKELY ROUTE
Founder or CTO is the only person who can run the core platform, with no retention	High	Structure: rollover, retention escrow on handover milestones
Critical accounts held personally or by one person	High (cheap to fix)	Condition: transfer before completion
Core code written by an unretained contractor or agency	High	Condition (assignment); retention or handover contract
Delivery slower than the plan assumes	Medium	Price via the model's roadmap timing
Thin documentation, small on-call rota	Medium or low	100-day plan

8. Security

The question is whether there is an unreported incident or an open door, and what closing the open findings costs. SOC 2 and ISO 27001 are signals of process during an audit window, not proof of security. The pen test findings, and what happened to them, show what the team does when nobody is checking.

Items to check

- ☐ Pen tests: scope, date, tester, open findings and their age
- ☐ Incident history, including near misses and any ransomware or extortion contact
- ☐ MFA on staff accounts, admin consoles, production access and customer admin accounts
- ☐ Vulnerability scanning on code, dependencies and infrastructure, with ageing of high and critical items
- ☐ Secrets management, and whether secrets have ever been committed to repositories
- ☐ Certifications held and whether their scope covers the product being bought
- ☐ What the target has told customers in security questionnaires, against what is true
- ☐ Cyber insurance declarations, against what diligence finds

Evidence, good and red flags

EVIDENCE	WHAT GOOD LOOKS LIKE	RED FLAG
Pen tests and remediation (SEC-01)	Annual, reputable tester, findings closed on a documented timeline	Critical or high findings open for months; scope excludes the main app
Incident log (SEC-02)	Incidents recorded, responded to and learned from	"We've never had one"; or one that should have gone to the ICO and did not
MFA coverage (SEC-03)	Enforced everywhere, including customer admins and break-glass accounts	Optional MFA on customer accounts; shared admin logins
Certifications (SEC-04)	Scope covers the product; exceptions are minor	Certificate covers a head office, not the platform
Customer questionnaires (SEC-07)	Answers match the evidence	Answers that overstate controls, which is a contract and disclosure risk
Insurance declarations (SEC-08)	Consistent with findings	Declarations that diligence contradicts, putting cover at risk

Severity and deal route

FINDING	TYPICAL SEVERITY	LIKELY ROUTE
Evidence of an unreported or undisclosed incident	Critical	Specific indemnity; possibly a condition or renegotiation
Open critical or high pen test findings; MFA gaps on admin access	High	Condition: fix and retest before completion
Questionnaire answers or insurance declarations that overstate controls	High or medium	SPA protection; disclosure
Certification scope narrower than the product	Medium	100-day plan
Policies exist but are not followed	Low	File

9. Data protection and privacy

The question is whether personal data is handled lawfully under UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025, and whether the paperwork describes reality. Most targets have a privacy notice. Fewer know where their personal data actually sits.

Items to check

- ☐ A record of processing activities that matches the data map
- ☐ Personal data outside the main database: logs, backups, analytics, support tools, the warehouse, laptops and spreadsheets
- ☐ Breach log and any ICO reports, and whether the 72-hour reporting rule was met

- [ ] Data processing agreements with every sub-processor, and the sub-processor list given to customers
- [ ] International transfer mechanisms and transfer risk assessments
- [ ] DPIAs for high-risk processing, including AI features and profiling
- [ ] Subject access requests and complaints: volumes, response times and the new complaints procedure
- [ ] Retention: a schedule, and evidence deletion actually runs

Evidence, good and red flags

EVIDENCE	WHAT GOOD LOOKS LIKE	RED FLAG
RoPA and data map (DAT-01, DAT-02)	Current, owned and consistent with the architecture	Personal data in places neither document mentions
Breach log and ICO contact (DAT-03)	Breaches logged, assessed and reported where required	A reportable breach that was not reported
Sub-processors (DAT-04)	DPAs signed; customer list kept current	Processors in use that customers were never told about
Transfers (DAT-05)	IDTA or UK Addendum in place; assessments on file	Data in non-adequate countries with no mechanism
DPIAs (DAT-06)	Done before launch for AI and profiling features	AI feature using customer personal data with no DPIA
Complaints and SARs (DAT-07)	Procedure in place since June 2026; responses on time	No complaints route; SAR backlog

Severity and deal route

FINDING	TYPICAL SEVERITY	LIKELY ROUTE
Unreported reportable breach	Critical or high	Specific indemnity; disclosure strategy
Personal data processed without lawful basis or customer knowledge	High or medium	Specific indemnity; 100-day remediation
Missing DPAs, stale RoPA, no transfer mechanism	Medium	Warranty; 100-day plan
No complaints procedure or retention schedule	Low	100-day plan

10. IP, open source and AI-generated code

The question is whether the target owns what it sells and whether any licence obligation threatens the commercial model. Under section 11 of the Copyright, Designs and Patents Act 1988 an employer owns copyright in code an employee writes in the course of employment. Contractors, agencies and founders writing before incorporation are not covered unless they assigned in writing.

Items to check

- ☐ A written assignment or employment term for every person and firm that has written code, including the agency that built version one
- ☐ Founder code written before incorporation, and any code brought from a previous employer
- ☐ A dependency scan or SBOM for each shipped product, with licences identified
- ☐ Copyleft components (GPL, AGPL, LGPL) and how they are used against the distribution model
- ☐ Code entering outside package managers: copied snippets, vendored libraries, AI-generated blocks
- ☐ AI coding tools: which, under what licence, with what review rules and whether the vendor offers IP indemnity
- ☐ Customer escrow agreements and their release triggers
- ☐ Trade marks and domains in the company's name

Evidence, good and red flags

EVIDENCE	WHAT GOOD LOOKS LIKE	RED FLAG
Assignments (IPO-01)	Signed by everyone who wrote code, founders included	Early contractor or agency with a licence, not an assignment
SBOM or scan (IPO-02)	Mostly permissive licences; copyleft absent or isolated	AGPL in a hosted product; GPL in distributed or on-premise software
Distribution model (IPO-04)	Licence analysis matches how each product ships	On-premise or mobile builds never scanned
AI coding tools (IPO-06)	Business licences, review gates, licence scanning in the pipeline	Personal accounts, no review change, no scanning
IP claims (IPO-03)	None, or resolved	Open licence compliance letters
Escrow (IPO-07)	Triggers limited to insolvency and failure to support	Change of control as a release trigger

Severity and deal route

FINDING	TYPICAL SEVERITY	LIKELY ROUTE
Core code not owned (missing assignment from founder, agency or contractor)	High or critical	Condition: confirmatory assignment before completion; specific indemnity
Copyleft licence obligation that conflicts with the commercial model	High or medium	Specific indemnity; replacement cost in the 100-day plan
No dependency scanning; unmanaged AI-generated code	Medium	100-day plan
Trade marks or domains held personally	Medium (cheap)	Condition

11. Infrastructure, cloud and cost to run

The question is whether cost to serve is under control, whether the business can recover from losing its main environment, and whether the hosting line in the model is right. Hosting cost growing faster than revenue with nobody able to explain it is a run-rate EBITDA question, not just a 100-day saving.

Items to check

- ☐ Twelve months of cloud bills by account and service, against revenue growth
- ☐ Cost allocation by customer or product, and gross margin by product
- ☐ Committed spend, reserved capacity and their terms
- ☐ How much of production is defined in code, and whether it could be rebuilt from scratch
- ☐ Backup coverage and the last full restore test, with the time it took
- ☐ Disaster recovery targets (RPO and RTO) and the last test against them
- ☐ Monitoring, alerting and who gets woken up
- ☐ Engineering tooling costs and renewals

Evidence, good and red flags

EVIDENCE	WHAT GOOD LOOKS LIKE	RED FLAG
Cloud bills (INF-01)	Growth slower than revenue; main lines explained	Cost up faster than revenue; nobody can explain the top three lines
Cost allocation (INF-08)	Margin known by product or customer tier	Large customers served at a loss without anyone knowing
Restore test (INF-02)	Full restore tested in the last six months, timed	Backups taken but never restored
DR plan (INF-05)	Targets set and tested	Single region, no tested failover, targets unknown
Infrastructure as code (INF-04)	Most of production defined in code	Hand-built servers nobody dares to touch
Commitments (INF-06)	Matched to steady-state usage	Multi-year commits above current usage

Severity and deal route

FINDING	TYPICAL SEVERITY	LIKELY ROUTE
Cost to serve rising faster than revenue, unexplained	High or medium	Run-rate EBITDA adjustment; 100-day plan
Backups never restored; no DR capability	Medium (high if regulated)	Pre-completion undertaking to test; 100-day plan
Over-commitment on cloud contracts	Medium	Debt-like item for unused commitment

FINDING	TYPICAL SEVERITY	LIKELY ROUTE
Hand-built infrastructure	Medium or low	100-day plan

12. Product and roadmap

The question is whether the revenue plan depends on features that do not exist yet, and how far to trust the team's estimates. The best evidence is last year's roadmap set against what shipped.

Items to check

- ☐ Roadmaps from 12 and 24 months ago, against delivery
- ☐ Revenue in the plan that depends on unbuilt features or products
- ☐ Features promised to named customers, in contracts or sales, with dates
- ☐ Cohort retention by product and feature-level usage
- ☐ Support volumes and categories, as a read on product quality
- ☐ How usage is metered and billed, and whether billing matches contracts
- ☐ Accessibility conformance where the target sells to the public sector

Evidence, good and red flags

EVIDENCE	WHAT GOOD LOOKS LIKE	RED FLAG
Past roadmaps (PRD-02)	Most commitments delivered roughly on time	A third delivered; the rest quietly dropped
Plan dependencies (PRD-05)	New-product revenue modest or already in build	Year-one revenue from a product with no team assigned
Customer commitments (PRD-04)	Few, dated and resourced	Contractual feature promises with penalties, unresourced
Cohorts and usage (PRD-03, PRD-06)	Retention holds by cohort; a few features do most of the work	Headline ARR hides decaying older cohorts
Support data (PRD-07)	Stable or falling tickets per customer	Rising tickets on core workflows

Severity and deal route

FINDING	TYPICAL SEVERITY	LIKELY ROUTE
Plan revenue depends on unbuilt features delivered by a team with a weak record	High or medium	Price: discount or delay that revenue in the model
Unresourced contractual feature commitments	Medium	SPA disclosure; 100-day plan
Billing and contract mismatch	Medium	Financial DD; warranty

FINDING	TYPICAL SEVERITY	LIKELY ROUTE
Accessibility gaps for public sector customers	Low or medium	100-day plan

13. Third parties, vendors and contracts

The question is whether one supplier or one customer contract could stop, reprice or reshape the business. Technology diligence reads these contracts for what lawyers can miss: a 30-day termination clause on the API that runs the core feature, or an SLA the platform cannot meet.

Items to check

- ☐ Every third-party service the product depends on, with termination, change of control and price change terms
- ☐ Top customer contracts: SLAs, service credits, liability caps, uncapped indemnities, escrow and change of control
- ☐ Service credits actually paid against SLA performance
- ☐ Outsourcing and agency contracts, including exit and handover
- ☐ Platform dependencies: app stores, cloud marketplaces, a single payment or messaging provider
- ☐ The target's own supplier security reviews

Evidence, good and red flags

EVIDENCE	WHAT GOOD LOOKS LIKE	RED FLAG
Supplier list (VEN-01)	Alternatives known for critical suppliers	Core feature on an API with short-notice termination or uncapped price rises
Customer contracts (VEN-02)	Caps on liability; no change-of-control termination	Uncapped data protection indemnity; termination on change of control from a top customer
SLA history (VEN-05)	Met, with few credits	Credits paid routinely, or SLAs the architecture cannot support
Outsourcing (VEN-03)	Exit assistance and handover terms	Agency holds code, keys or knowledge with no exit terms

Severity and deal route

FINDING	TYPICAL SEVERITY	LIKELY ROUTE
Major customer can terminate on change of control	High	Condition: consent before completion; price if refused
Critical supplier with short-notice termination or uncapped pricing	High or medium	100-day plan to dual-source; warranty
Uncapped indemnities in customer contracts	Medium	Specific indemnity; renegotiate at renewal
Agency with no exit terms	Medium	Condition or 100-day plan

14. IT and internal systems

The question is whether the systems the business runs on (finance, CRM, HR, billing, identity, devices) hold up, and what separating or integrating them will cost. For a tech-enabled services business this area often matters more than the code.

Items to check

- ☐ Internal systems inventory with owners, licences and renewal dates
- ☐ Identity and access: SSO, joiners and leavers, shared admin accounts
- ☐ Device management and disk encryption on laptops
- ☐ Spreadsheets and manual steps that produce month-end, billing or board numbers
- ☐ Shared services provided by a parent or seller group, and transitional services needs
- ☐ Licence compliance for major internal software

Evidence, good and red flags

EVIDENCE	WHAT GOOD LOOKS LIKE	RED FLAG
Shared services (ITS-01)	Listed and costed, with a TSA outline	Carve-out where the parent's systems run billing and nobody has priced separation
Identity and devices (ITS-03)	SSO, MDM and encryption on every device	Shared global admin; unmanaged laptops with customer data
Manual processes (ITS-04)	Few, documented	Board numbers built by one person in a spreadsheet
Licences (ITS-07)	Counts match usage	Under-licensing that an audit would catch

Severity and deal route

FINDING	TYPICAL SEVERITY	LIKELY ROUTE
Unpriced separation from a parent's systems	High	Price; TSA terms in the SPA
Shared admin accounts, unmanaged devices	Medium or low	100-day plan
Key reporting dependent on one spreadsheet and one person	Medium	100-day plan
Software under-licensing	Medium or low	Warranty; true-up cost

15. AI and data

The question has three parts. Is the AI described in the CIM real and used? What does it cost per use, and is that cost in the margins? Is it governed well enough to survive a customer audit and the EU AI Act? The fuller method is in AI due diligence for private equity and AI washing in due diligence, and the full question bank is our AI due diligence questions.

Items to check

- ☐ Every AI feature, the model or vendor behind it and when it launched
- ☐ Usage per feature last month and the trend
- ☐ Inference and AI vendor cost per month and per unit, at current and planned adoption
- ☐ A live demonstration on real data, not a recording
- ☐ Evaluation sets, accuracy measures and what happens when the model is wrong
- ☐ Training data provenance and rights, including customer data
- ☐ AI vendor terms: data use, training rights, retention, rate limits and indemnities
- ☐ Governance: policy, risk register, EU AI Act classification, DPIAs
- ☐ Who built the prompts, evaluation sets and model integrations (a newer form of key-person risk)
- ☐ Exposure: whether AI agents threaten the target's own pricing or customers' need for it

Evidence, good and red flags

EVIDENCE	WHAT GOOD LOOKS LIKE	RED FLAG
Inventory and usage (AID-01, AID-02)	Features named, used and growing	"AI-powered" in the CIM; no usage data
Unit cost (AID-03)	Known cost per call; in the margin model	Plan assumes wide adoption with no inference cost
Evaluation (AID-05)	Test sets and measured accuracy; fallbacks	Nobody can say how often it is wrong
Training data (AID-04)	Rights documented; customer data use permitted by contract	Customer data used to train models without contractual right
Vendor terms (AID-06)	Enterprise terms; no training on target's data	Consumer terms; data retained and used by the vendor
Governance (AID-07)	Classified against the AI Act where relevant; DPIAs done	Possible high-risk use with no assessment

Severity and deal route

FINDING	TYPICAL SEVERITY	LIKELY ROUTE
AI claims in the CIM not supported by a working, used feature	High or medium	Price: discount the AI-dependent revenue; disclosure warranty

FINDING	TYPICAL SEVERITY	LIKELY ROUTE
Inference cost missing from the plan's margins	Medium	Price: run-rate margin adjustment at the multiple
Customer data used for training without rights	High	Specific indemnity; stop and remediate
AI Act high-risk use without a compliance plan	Medium	100-day plan with budget

16. Integration and the first 100 days

The question is what has to happen between signing and day 100, who owns it and what it costs. The 100-day plan should contain only what the findings justify, each item with an owner, a budget and a date. If the fund has a wider value creation plan, link the two, as set out in AI due diligence and the value creation plan.

Items to check

- ☐ Accounts, domains and licences in founders' or the seller's names that must transfer
- ☐ Interim covenants between signing and completion: no major re-platform, hires or vendor changes without consent
- ☐ In-flight projects with budgets and status
- ☐ Technology budget for this year and next
- ☐ Decisions due in the next six months: renewals, hires, vendor changes
- ☐ National Security and Investment Act exposure: the mandatory regime covers 17 sectors, including artificial intelligence and data infrastructure, and the government confirmed changes in March 2026 (Herbert Smith Freehills Kramer, 2026)
- ☐ For corporate acquirers: which systems are merged, kept or retired, and the cost of each

A 100-day plan template

WINDOW	TYPICAL ACTIONS	OWNER
Before completion	Admin access transferred; confirmatory IP assignments; critical security fixes retested; customer consents	Seller, with buyer sign-off
Days 1 to 30	MFA everywhere; second admin on every critical account; backup restore tested; hiring started for key-person cover	CTO
Days 31 to 60	Documentation sprint tested by a new joiner; dependency scanning in the pipeline; cloud cost review; DPAs and RoPA fixed	CTO, CFO, privacy lead
Days 61 to 100	Debt remediation started with a budget; on-call rota of three or more; AI cost and governance in board reporting	CTO, operating partner

Severity and deal route

FINDING	TYPICAL SEVERITY	LIKELY ROUTE
NSI Act notification needed but not planned	Critical (void transaction risk)	Condition: clearance before completion
Assets held outside the company	High (cheap)	Condition
Large in-flight migration with uncertain budget	Medium	Price or interim covenant
Integration cost not in the buyer's model	Medium	Price for a corporate buyer; 100-day plan

17. Data-room request list

All 107 requests, numbered by area so they can be pasted straight into a request tracker or the Excel workbook, which uses the same IDs. **P1** items could move the price and go out on day one (40 items). **P2** items are needed for a full report. **P3** items are useful context and can be skipped on a red-flag review. Where an item does not exist, record "not available": the absence is usually a finding.

Architecture and scalability

ID	REQUEST	PRIORITY
ARC-01	Current architecture diagram drawn by the engineering team, dated (not the CIM version)	P1
ARC-02	Inventory of products, services, repositories and mobile apps, with languages, frameworks and versions	P1
ARC-03	Tenancy model: how customer data is separated (shared schema, schema or database per tenant, single-tenant installs)	P1
ARC-04	12 months of availability against SLA, and the incident log with root-cause write-ups	P1
ARC-05	Customer-specific branches, forks or bespoke deployments, and the customers on them	P1
ARC-06	Load or performance test results, and peak utilisation of the main database and services	P2
ARC-07	The team's written view of the first bottleneck at two and five times current volume, with a rough cost	P2
ARC-08	Integration inventory: public APIs, webhooks and partner integrations, with volumes and versioning policy	P2
ARC-09	Data model documentation and the main database schema	P3
ARC-10	Design documents or decision records for the last two major architectural changes	P3

Code quality and technical debt

ID	REQUEST	PRIORITY
COD-01	Read-only access to all source repositories with full history	P1
COD-02	List of languages, frameworks, databases and operating systems on unsupported or end-of-life versions	P1
COD-03	The team's own technical debt list or backlog, with any estimates	P1
COD-04	Test strategy and recent automated test results, with coverage for billing, permissions and the core data model	P2

ID	REQUEST	PRIORITY
COD-05	CI/CD pipeline configuration and six months of deployment logs	P2
COD-06	Split of engineering time between new features, maintenance and support, for 12 months	P2
COD-07	Capitalised development costs for three years and the capitalisation policy	P2
COD-08	Static analysis or code quality reports, if the team runs them	P3
COD-09	Code review policy and branch protection settings	P3

Team, delivery and key-person risk

ID	REQUEST	PRIORITY
TEA-01	Org chart for engineering, product, data and IT, with role, tenure, location and employment type	P1
TEA-02	Contractor, freelancer and agency list, with spend, scope, contract dates and notice terms	P1
TEA-03	Owner and admin list for cloud, code hosting, domain registrar and DNS, app stores, payments, identity provider and secrets vault	P1
TEA-04	Employment contracts for key technical staff: notice, restrictive covenants and IP clauses	P1
TEA-05	Current and proposed retention, bonus, option and incentive arrangements for key technical staff	P1
TEA-06	Leavers in the last 24 months, with role, tenure and reason	P2
TEA-07	On-call rota, and who resolved each serious incident in the last 12 months	P2
TEA-08	Delivery metrics if measured: deployment frequency, lead time, change fail rate, recovery time	P2
TEA-09	Salary bands and loaded cost per engineer by level (for costing findings)	P2
TEA-10	Onboarding documentation and runbooks, with authors and last-edited dates	P3

Security

ID	REQUEST	PRIORITY
SEC-01	Last two penetration test reports in full, with remediation evidence for each finding	P1
SEC-02	Security incident log for 36 months, including near misses, ransomware and extortion contacts	P1
SEC-03	MFA and SSO coverage: staff, admin consoles, production access and customer admin accounts	P1
SEC-04	SOC 2 Type II report, ISO 27001 certificate and statement of applicability, Cyber Essentials status	P2

ID	REQUEST	PRIORITY
SEC-05	Vulnerability scanning set-up and the open high and critical findings, with age	P2
SEC-06	Secrets management approach, and any history of secrets committed to repositories	P2
SEC-07	Customer security questionnaires completed in 12 months, and any customer audit findings	P2
SEC-08	Cyber insurance policy, claims history and the declarations made at the last renewal	P2
SEC-09	Security policies in use (access, joiners and leavers, incident response), with last review dates	P3
SEC-10	Named security owner, reporting line and security budget	P3

Data protection and privacy

ID	REQUEST	PRIORITY
DAT-01	Record of processing activities (RoPA)	P1
DAT-02	Data map: where personal data sits, including backups, logs, analytics, support tools and the warehouse	P1
DAT-03	Personal data breach log and all ICO reports or correspondence	P1
DAT-04	Sub-processor list with signed data processing agreements, and the customer-facing sub-processor list	P2
DAT-05	International transfer mechanisms (IDTA, UK Addendum, adequacy) and transfer risk assessments	P2
DAT-06	DPIAs for high-risk processing, including AI features	P2
DAT-07	Subject access request log with response times, and the data protection complaints log	P3
DAT-08	Privacy notices, cookie consent set-up and marketing consent records (PECR)	P3
DAT-09	Retention schedule and evidence that deletion runs	P3
DAT-10	DPO or privacy lead, and the last internal privacy review	P3

IP, open source and AI-generated code

ID	REQUEST	PRIORITY
IPO-01	IP assignment or employment terms for everyone who has written code, including founders before incorporation and agencies	P1
IPO-02	Software bill of materials or dependency scan for each shipped product, with licences	P1
IPO-03	Any IP claims, takedown notices or licence compliance correspondence	P1
IPO-04	Distribution model per product (SaaS, on-premise, mobile, embedded), for licence analysis	P2
IPO-05	Commercial code licensed in (SDKs, libraries, white-labelled components), with terms	P2

ID	REQUEST	PRIORITY
IPO-06	AI coding tools in use, licences held, usage policy, review rules and vendor IP indemnity terms	P2
IPO-07	Source code escrow agreements granted to customers, with release triggers	P2
IPO-08	Registered IP: trade marks, domains and patents, with owner of record	P2
IPO-09	Open source policy and any approved licence exceptions	P3

Infrastructure, cloud and cost to run

ID	REQUEST	PRIORITY
INF-01	12 months of cloud bills by account and service	P1
INF-02	Backup policy, and the last restore test with date and time taken	P1
INF-03	Hosting diagram: accounts, regions and environments	P2
INF-04	Infrastructure-as-code repositories, and the share of production defined in code	P2
INF-05	Disaster recovery plan, RPO and RTO targets, and the last DR test	P2
INF-06	Reserved instances, savings plans and committed spend, with terms	P2
INF-07	Engineering tooling subscriptions, with cost and renewal dates	P2
INF-08	Cost allocation by customer or product, and the gross margin build-up	P2
INF-09	Monitoring, alerting and on-call tooling	P3
INF-10	Any data centre, colocation or on-premise hardware, with lease and refresh dates	P3

Product and roadmap

ID	REQUEST	PRIORITY
PRD-01	Product roadmap for the next 18 months, with resourcing	P1
PRD-02	Roadmaps from 12 and 24 months ago, and what shipped against them	P1
PRD-03	Cohort retention, logo and revenue, by product	P1
PRD-04	Features promised to customers in contracts or sales, with dates	P1
PRD-05	Revenue plan items that depend on features not yet built	P1
PRD-06	Feature-level usage data	P2
PRD-07	Support ticket volumes, categories and resolution times for 12 months	P2
PRD-08	Pricing and packaging, and how usage is metered and billed	P2

ID	REQUEST	PRIORITY
PRD-09	Accessibility conformance (WCAG) where selling to the public sector	P3

Third parties, vendors and contracts

ID	REQUEST	PRIORITY
VEN-01	Third-party services the product depends on, with spend, term, termination and change-of-control clauses	P1
VEN-02	Top 20 customer contracts: SLAs, service credits, liability caps, uncapped indemnities, escrow and change of control	P1
VEN-03	Outsourcing and agency agreements, statements of work and exit provisions	P1
VEN-04	Standard customer terms and any material deviations	P2
VEN-05	SLA performance and service credits paid over 24 months	P2
VEN-06	The target's own supplier security reviews	P3
VEN-07	Reseller, marketplace and platform terms (app stores, cloud marketplaces)	P3
VEN-08	Public sector frameworks and contracts with security or data clauses	P3

IT and internal systems

ID	REQUEST	PRIORITY
ITS-01	Shared services provided by a parent or seller group, and expected TSA needs	P1
ITS-02	Internal systems inventory (finance, CRM, HR, billing, support, warehouse), with owner and licence	P2
ITS-03	Identity and device management: SSO, MDM, disk encryption, joiners and leavers process	P2
ITS-04	Spreadsheets and manual steps that run month-end, billing or board reporting	P2
ITS-05	Microsoft 365 or Google Workspace admin set-up and licensing	P3
ITS-06	IT support model and any outsourced IT contract	P3
ITS-07	Licence position for major internal software (Microsoft, Oracle, Adobe and similar)	P3

AI and data

ID	REQUEST	PRIORITY
AID-01	Inventory of every AI feature in the product and in operations, with the model or vendor behind each	P1

ID	REQUEST	PRIORITY
AID-02	Usage data per AI feature: customers, calls and trend	P1
AID-03	Inference and AI vendor cost, per month and per unit of use	P1
AID-04	Training data provenance and rights, including any customer data used for training	P1
AID-05	Evaluation sets, accuracy measures and failure handling for each AI feature	P2
AID-06	AI vendor contracts: data use, training rights, retention, indemnities and rate limits	P2
AID-07	AI governance: policy, risk register, EU AI Act classification and DPIAs	P2
AID-08	Customer contract terms on AI and customer data	P2
AID-09	Data platform: warehouse, pipelines, data quality measures and ownership	P3

Integration and the first 100 days

ID	REQUEST	PRIORITY
INT-01	Accounts, domains and licences held in founders' or seller group names that must transfer	P1
INT-02	In-flight major projects (migrations, re-platforms), with budget, status and owner	P1
INT-03	Self-assessment against the NSI Act mandatory notification sectors	P1
INT-04	Technology budget for this year and next, opex and capex	P2
INT-05	Technology decisions due in the next six months (renewals, hires, vendor changes)	P2
INT-06	Systems the buyer expects to merge, keep or retire, mapped to the target's estate (buyer to complete)	P2

18. Interview plan and questions by role

Documents tell you what the target wants you to know. Interviews tell you what the documents leave out. The best interview question in technical due diligence is a request to be shown something, on a shared screen, while you watch. The rationale for each core question, and what good and worrying answers sound like, is in technical due diligence questions.

Who to interview, and in what order

SESSION	LENGTH	PURPOSE
CTO, first session	90 minutes	The CTO's own account of the system, strengths and problems
Most senior engineer other than the CTO	45 to 60 minutes	How the system works in practice; who knows what
Engineer hired in the last year	45 minutes	What was confusing; what the documentation missed

SESSION	LENGTH	PURPOSE
Whoever handles production incidents	45 minutes	Reliability, recovery and the 2am reality
Product lead	45 minutes	Roadmap credibility, usage and customer commitments
Security or privacy lead, if one exists	45 minutes	Incidents, open findings, data handling
Data or AI lead, if AI is in the investment case	45 minutes	What the AI does, costs and gets wrong
CFO or finance lead	30 minutes	Cost to run, capitalisation, contracts, tooling spend
Customer support or success lead	30 minutes	What customers complain about and why they leave
Agency or main contractor, if they write meaningful code	45 minutes	Knowledge held outside the company; exit terms
CTO, second session	60 minutes	Reconcile the first account with the evidence; raise findings

Not every target has all of these roles. For a team of 5 to 30 engineers, four to seven interviews are usually enough: the CTO twice, two or three engineers, the incident handler and the product lead. Interview engineers without the CTO or founders present, and say at the start that the aim is to understand the system, not to assess individuals. Leave the CEO and CFO out of technical sessions. Ask several people the same core questions (how does a change reach production, what would you fix first, who would you call at 2am) and compare. Agree the confidentiality circle with the seller in writing, and record in the report's scope section anyone you could not speak to.

CTO, first session

1. If customer volume doubled next year, what breaks first, and what would fixing it cost?
2. Walk me through what happens when a customer does the one thing they do most.
3. What would you rebuild with six months and no feature requests?
4. Show me the last change that went to production, from ticket to deploy.
5. Which part of the codebase is everyone afraid to touch?
6. Who has admin access to the cloud account, code hosting, domain registrar and app stores?
7. Who wrote the first version of the product, and were they employees?
8. Which outside service, if it disappeared or doubled its price, would hurt most?
9. Why did the cloud bill change last year?
10. Show me the AI feature running on real data, and tell me how many customers used it last month.
11. What do you want to be doing in two years? (Ask it plainly. The answer prices the retention package.)

Senior engineer and recent joiner

1. How does a change get from your laptop to production? Show me.
2. If something broke at 2am on a Sunday, who would you call?
3. What did you need to know in your first fortnight that was not written down?
4. Which part of the system do you avoid, and why?

5. How do you use AI coding tools, and does AI-written code get reviewed differently?
6. What would you fix first if you were given a month?
7. What is the slowest part of shipping a feature here?

Incident handler or platform engineer

1. Tell me about the last serious incident: how it was found, who fixed it, what changed.
2. When did you last restore from backup, and how long did it take?
3. What alerts wake you up, and how many of them are noise?
4. Could you rebuild production from what is in the repositories?
5. What is still open from the last pen test?

Product lead

1. Take me through last year's roadmap and what shipped.
2. Which features in the plan have no team on them yet?
3. What have sales promised customers that is not built?
4. Which features do customers use most, and which did you build that nobody uses?
5. Why do customers leave?

Security and privacy lead

1. Tell me about your last security incident and your last personal data breach.
2. Where does personal data live, including the places it should not?
3. Which sub-processors were added in the last year, and were customers told?
4. Is MFA enforced for customer admin accounts?
5. How do you handle a data protection complaint now that the complaints duty applies?

Data or AI lead

1. Which model or vendor sits behind each AI feature, and what does a call cost?
2. How do you know when the model is wrong, and what happens then?
3. What data trained or tunes it, and do customer contracts allow that use?
4. If the model vendor changed its price or terms, what would you do?
5. Who else could maintain the prompts, evaluation sets and integrations if you left?

CFO, support lead and agency

1. CFO: what is hosting and tooling as a share of revenue, and what is capitalised as development?
2. CFO: which technology contracts renew or step up in price in the next 12 months?
3. Support lead: what are the top three ticket categories, and are they rising?

4. Support lead: which customers have threatened to leave over product problems?
5. Agency: what code, accounts or keys do you hold, and what happens if the contract ends?

What to listen for

Who gets named as the person to ask: if it is always the same person, you have found the key-person risk. Where answers go vague: people are precise about what they are proud of and general about what worries them. Rehearsal: identical polished answers from three people about security suggest a briefing, so ask the follow-up nobody prepared for. And the newest engineer's account of deployment, which is usually the accurate one.

19. Severity and costing method

Severity

SEVERITY	DEFINITION	DEFAULT TREATMENT
Critical	Could stop the deal, or cause material loss or regulatory exposure: an unreported breach, core code not owned, a platform that cannot carry the plan, an unplanned NSI Act notification	Walk away, renegotiate, or condition plus specific indemnity
High	Should change the price or terms: a costed re-platform, key-person dependency with no retention, missing assignments, a major customer's change-of-control right	Price, condition, specific indemnity or structure
Medium	Real cost or risk that belongs in the first 100 days with an owner and budget	100-day plan, sometimes a warranty
Low	Hygiene	File

Severity describes consequence, not how easy the fix is. A personal email on the domain registrar is high severity and a £500 fix, which is why it should be a condition of completion.

Costing rules

1. **Cost in the target's money.** Use its salary bands and loaded costs (TEA-09). Where they are not available, state the assumption. This guide uses £85k a year loaded for a mid-level engineer and £110k for a senior hire, which are illustrative assumptions, not market data.
2. **Use engineer-months.** Cost equals engineers times months times monthly loaded cost. At £85k a year, one engineer-month is about £7.1k. Three engineers for six to nine months is £128k to £191k.
3. **Give a range and its basis.** A single number implies precision nobody has. Write the basis next to the number, so the deal team can argue with the assumption rather than the conclusion.
4. **Add contingency for rewrites and migrations.** Twenty to fifty per cent is normal for work the team has not done before; state which you used.
5. **Count opportunity cost separately.** Engineers rebuilding a framework are not building the plan's new module. Show the delay in months and let the model team price the revenue effect, rather than adding it to the remediation cost and counting it twice.

6. **Separate one-off from annual.** One-off remediation is roughly worth its cost. An annual cost the plan misses (inference, hosting, licences, an extra hire) is worth its annual value times the entry multiple, because it reduces run-rate EBITDA. At 12 times, £60k a year is £720k of enterprise value.
7. **Weight contingent items for indemnity sizing, not for price.** A possible regulatory fine or licence claim should not be added to the price as if certain. Estimate the plausible range, and use it to size a specific indemnity, escrow or cap.
8. **Say when something cannot be costed yet, and what it would take.** "Cost unknown until the agency confirms whether it will assign; legal estimate £5k to £15k if it does" is a finding. "May have IP risk" is not.

From severity and cost to route

IF THE FINDING IS	ROUTE IT TO
Known, one-off, needed for the plan to happen	Price, as a debt-like item or known capex
A recurring cost missing from the plan	Price, through run-rate EBITDA at the multiple
Cheap to fix and binary (access, assignment, consent, critical fix)	Condition of completion
A known issue with uncertain cost (a licence claim, a possible breach)	Specific indemnity, possibly with escrow; known issues are usually excluded from W&I cover
A dependency on a person	Structure: rollover, retention, escrow released on handover milestones
A real cost with an obvious fix and an owner	100-day plan with budget
Hygiene	File

The scope section of the report matters for insurance as well as for the findings. Paul Hastings' 2026 buyer's guide to W&I notes that the scope of protection depends heavily on the quality of diligence and that cyber cover depends on a review of the target's IT and security. State exactly which repositories, commits, environments and people were reviewed. How each finding then appears in the deliverable is set out in what a technical due diligence report should contain.

20. Red-flag, full and vendor scoping

TYPE	WHEN TO USE IT	TYPICAL TIME AND FEE	WHAT IT COVERS
Red-flag review	Pre-LOI or early exclusivity; uncertain deals; VC rounds	Five to seven working days; £8k to £12k at our rates	P1 requests only; CTO and two engineer interviews; commit and access review; dependency scan; rough cost and route per finding
Full buy-side review	Exclusivity on a deal heading to completion; lenders or W&I insurer involved	Two to three weeks; £15k to £30k at our rates	All twelve areas; P1 and P2 requests; full interview plan; costed register; scope and reliance; 100-day plan
Vendor review	Three to six months before a sale process	Usually longer, with a fix phase	All areas, written for several unknown buyers; reliance letter for the winner; remediation before launch

TYPE	WHEN TO USE IT	TYPICAL TIME AND FEE	WHAT IT COVERS
Top-up review	Buyer relying on a vendor report	Two to five days	Tests the vendor report's key findings and anything that changed since

Published fees from other UK and US providers are compared in technical due diligence cost UK. Two scoping rules matter more than the fee. First, insist on read-only code access: documents-only diligence is cheaper and reliably misses the findings that matter. Second, scope by the investment committee's questions. "Can the platform carry the growth?" is a different job from "is the AI real?" or "can we separate this from the parent in six months?"

A vendor review is worth doing when there is time to act on it. Fixing missing assignments, transferring admin access and closing pen test findings costs a seller little; a buyer finding them prices them at its own estimate. When to commission one is covered in vendor technical due diligence, and what a seller should fix, and when, is in our exit readiness checklist.

For carve-outs, add a separation workstream: shared code, shared infrastructure, shared licences and shared people, each with a transitional services cost and an exit date. For VC rounds, cut to the red-flag scope and weight team, IP and architecture-for-scale; most of the rest has not had time to matter.

21. Sector variants

The twelve areas apply everywhere, but the weight shifts. Use these as additions, not replacements. Our sector guides cover the deal questions for each industry in more depth.

SaaS

Weight up architecture (tenancy), cost to run and product (the software and SaaS guide goes further). Add:

- ☐ Gross margin by product and customer tier, with hosting, support and third-party costs allocated
- ☐ Net revenue retention by cohort, reconciled to product usage
- ☐ Multi-tenancy isolation testing: can one customer see another's data?
- ☐ Enterprise readiness the plan assumes: SSO, audit logs, data residency, uptime commitments
- ☐ Exposure to EU Data Act switching rules if retention relies on high exit costs for EU customers
- ☐ Seat-based pricing exposed to AI agents doing the users' work

Marketplace

Weight up data, security, third parties and product (the parking and mobility guide covers parking apps and marketplaces). Add:

- ☐ Liquidity metrics from raw data: listings, searches, match or fill rate, repeat use, by region
- ☐ Payments flow: who holds funds, and whether it relies on a regulated payment provider's permissions or needs its own
- ☐ Fraud, fake listings and reviews: detection, losses and chargeback rates
- ☐ Trust and safety tooling, and whether user-to-user features bring the service within the Online Safety Act 2023

- [ ] Dependence on one acquisition channel or platform (search, app stores, a single partner)

Tech-enabled services

Weight up IT and internal systems, data and AI exposure; weight down code. Add:

- [ ] Which delivery steps are automated, which are manual, and the cost per unit of service
- [ ] Data quality in the operational systems that the plan's efficiency case depends on
- [ ] Off-the-shelf systems and their renewal, pricing and integration limits
- [ ] How exposed the service is to AI doing the same work for less, using the AI disruption risk assessment
- [ ] Spreadsheet and person dependencies in billing and reporting

Hardware and IoT

Weight up security, IP, third parties and product. Add:

- [ ] Firmware update mechanism: signed, over the air, with rollback, and the share of the fleet on current firmware
- [ ] UK PSTI compliance for consumer connectable products, which has applied since 29 April 2024 (GOV.UK)
- [ ] EU Cyber Resilience Act readiness, including the vulnerability reporting process that has applied since September 2026
- [ ] Bill of materials, single-source components, end-of-life notices and the cost of a forced redesign
- [ ] Certification (UKCA, CE, radio) and the cost of recertifying after a hardware change
- [ ] Device fleet telemetry, field failure rates and warranty returns
- [ ] Long-term support obligations to customers for devices already in the field

22. Worked example

Illustrative example. Northgate Software Ltd is a fictional target. The buyer, the figures and the findings are invented to show the method and are not drawn from any real deal. The same register is filled in on the Example tab of the workbook.

The target and the question

Northgate Software Ltd, a fictional UK business, sells scheduling software to facilities management firms: field engineers, jobs, routes and customer reporting. It has £9.2m of ARR, EBITDA of £3.5m and an agreed enterprise value of £42m, 12 times EBITDA. There are 22 people in engineering and product: 15 employees and 7 through a nearshore agency. The co-founder CTO wrote much of the core.

The investment case rests on three assumptions: 2.5 times the customers in three years; an enterprise tier in year two; and an AI tier, sold as "AI route optimisation", reaching 60% of customers.

The buyer commissioned a full review over 15 working days. The red-flag note went to the deal team on day six with seven items and rough costs.

The findings register

#	FINDING	SEVERITY	COST (£K)	ROUTE
N01	Co-founder CTO wrote 64% of commits to the scheduling engine in 18 months, is sole owner of the cloud root account and domain, and plans to step back within a year	High	95 to 140	Structure
N02	Nearshore agency that built the mobile app (2019 to 2022) worked under a licence, not an assignment	High	5 to 15	Condition
N03	Customer web app built on AngularJS, out of support since the end of 2021; must be rebuilt before the enterprise tier	High	255 to 340	Price
N04	Database per customer on self-managed servers; each onboarding takes three engineer-days; plan assumes 2.5 times the customers	Medium	128 to 191	100-day plan
N05	Two high pen test findings open for seven months; MFA not enforced on customer admin accounts	High	10 to 20	Condition
N06	Personal data in application logs and the product analytics tool, not in the RoPA; DPAs missing for 3 of 14 sub-processors	Medium	12 to 25	SPA protection
N07	AGPL-licensed PDF library inside the hosted reporting service, with no commercial licence	Medium	15 to 35	SPA protection
N08	Cloud bill up 41% against revenue up 19%; no cost allocation; £70k to £110k a year judged avoidable	Medium	15 to 25	100-day plan
N09	"AI route optimisation" is a heuristic solver; the one LLM feature is used by 9% of customers; plan assumes 60% uptake with no inference cost	Medium	60 to 95 a year	Price
N10	Backups run nightly but a full restore has never been tested; RPO and RTO undocumented	Medium	8 to 15	100-day plan
N11	Shared Microsoft 365 global admin, 40% of laptops outside device management, Cyber Essentials lapsed in 2025	Low	6 to 12	100-day plan
N12	Largest customer (11% of ARR) can terminate on change of control and has an uncapped data protection indemnity	High	None (about £1.0m ARR at risk)	Condition
N13	Team delivered 38% of last year's roadmap on time; the plan books revenue from a new module in year one	Medium	None (timing)	Price

The arithmetic behind N03 is four engineers for nine to twelve months at £85k loaded: 4 × £85k × 0.75 = £255k, and 4 × £85k × 1.0 = £340k. N04 is three engineers for six to nine months: £128k to £191k. N01 is a senior hire at £110k loaded with a £20k fee, six months' overlap and a documentation sprint. The ranges exclude contingency, which the deal team added in the model.

The totals

Five findings are high and seven medium; none is critical. One-off remediation totals £549k to £818k. The single annual item, N09's inference cost at the plan's adoption rate, is £60k to £95k a year. By route, one-off costs split as follows: price £255k to £340k, structure £95k to £140k, conditions £15k to £35k, SPA protection £27k to £60k and the 100-day plan £157k to £243k.

Capitalised at 12 times, N09 is worth £720k to £1.14m of enterprise value, more than the largest one-off item. This is the finding most deal teams would have filed as "AI claims somewhat overstated".

What the deal team did with it

- **Verdict:** proceed with conditions, at a lower price.
- **Price:** N03 treated as a debt-like item at the midpoint, about £300k. N09 taken through the model as a margin adjustment at the midpoint, about £0.9m of enterprise value. N13 handled by moving the new module's revenue back six months in the plan, which the model team priced.
- **Conditions of completion:** cloud root account and domain moved to company ownership with two administrators (N01); confirmatory assignment from the agency (N02); pen test findings fixed and retested, MFA enforced (N05); written consent from the largest customer waiving its change-of-control right (N12).
- **SPA protection:** specific indemnities for pre-completion data protection breaches (N06) and the AGPL exposure (N07), and for any claim arising from the agency's pre-assignment work (N02).
- **Structure:** the CTO rolls over equity, and part of the CTO's consideration sits in escrow, released on handover milestones at six and twelve months: a second engineer leading releases, documentation tested by a new joiner, incidents resolved without the CTO.
- **100-day plan:** budget of £157k to £243k for N04, N08, N10 and N11, plus the senior hire under N01. N08's £70k to £110k a year saving is upside for the value creation plan, not a price chip.

The red-flag note on day six already contained N01, N02, N03, N05 and N09 with rough costs. That is what gave the deal team a week to negotiate rather than a day.

---

23. Red flags that should stop or reprice a deal

1. **Refusal of read-only code access** without a credible reason and an alternative (a clean room, a supervised session).
2. **Evidence of an incident that was not reported** to the ICO, customers or the insurer when it should have been.
3. **Core code the target does not own:** a founder, agency or contractor who never assigned, and will not.
4. **One person who holds the platform up** and is about to receive a large cheque with no reason to stay.
5. **A plan that needs volume or features the platform cannot carry** without a re-architecture nobody has costed.
6. **Copyleft code in a product whose distribution triggers its obligations**, discovered by you rather than disclosed.
7. **AI revenue with no usage and no unit cost.** If the feature cannot be shown working on real data, the revenue line depending on it is a hope.
8. **Hosting cost outgrowing revenue** with nobody able to explain the main lines.

9. **Customer contracts the technology cannot honour:** SLAs, data residency or security commitments that the evidence contradicts.
10. **An unplanned regulatory gate:** an NSI Act notification that was not scoped, or a high-risk AI use with no compliance plan.

24. Common mistakes

Starting technical diligence after financial and legal. The findings most likely to move price (missing assignments, key-person dependency, an uncosted rewrite) take longest to fix and negotiate. Scope tech DD first, or at least at the same time.

Reporting maturity scores instead of money. A score of 2.8 out of 5 for "engineering practices" gives the lawyers nothing to draft and the model nothing to price.

Adding opportunity cost to remediation cost. Count the engineers' cost once, and give the model team the delay in months so they can price the revenue effect.

Treating annual and one-off costs alike. A missing £80k a year belongs in run-rate EBITDA and is worth the multiple.

Making cheap fixes 100-day actions. Access transfer, confirmatory assignments and critical security fixes cost little before completion and much more after, when the seller has the money and no reason to cooperate.

Taking certificates as conclusions. SOC 2 and ISO 27001 tell you a process existed during an audit window and within a stated scope. Check the scope covers the product you are buying, then read the pen test.

Interviewing only the CTO. The second engineer and the newest hire are where the accurate account of deployment, documentation and key-person risk comes from.

Asking questions with predictable answers. "Do you follow agile?" and "Is your code documented?" get a yes from everyone. Ask to see the tests for the billing code and the document the last new joiner used.

Scanning only the main web app. Mobile apps, on-premise builds, firmware and internal tools have their own licence and security profiles, and are often where the AGPL or the hard-coded secret sits.

Forgetting what the report is for. Lenders and insurers read the scope section. Lawyers read the register. The investment committee reads one page. Write each part for its reader.

25. Glossary

Bus factor (truck factor). The smallest number of people whose departure would stall a project.

Condition (condition precedent). Something that must happen before completion, such as an IP assignment or a customer consent.

Copyleft. Open source licences (GPL, AGPL) that require derivative work to be released under the same terms in some circumstances. AGPL extends this to software offered over a network.

Debt-like item. A known future cost treated as a reduction in the price, in the same way as debt.

DORA metrics. Software delivery measures from the DORA research programme: deployment frequency, change lead time, change fail rate, recovery time and rework rate.

DPA. Data processing agreement between a controller and a processor under UK GDPR.

Loaded cost. Salary plus employer costs, benefits, equipment and overhead for one person for a year.

RoPA. Record of processing activities required under UK GDPR.

RPO and RTO. Recovery point objective (how much data you can afford to lose) and recovery time objective (how long you can afford to be down).

SBOM. Software bill of materials: a list of every component in a piece of software, with versions and licences.

SPA. Share purchase agreement: the contract that carries warranties, indemnities, conditions and the price mechanism.

TSA. Transitional services agreement, under which a seller keeps providing systems or services to a carved-out business for a period after completion.

W&I insurance. Warranty and indemnity insurance, covering loss from breach of warranty. Known issues found in diligence are usually excluded.

26. Sources and further reading

Statistics and regulation cited

- Black Duck, 2026 Open Source Security and Risk Analysis: 947 commercial codebases; licence conflicts, vulnerabilities, outdated components and AI-generated code.
- Department for Science, Innovation and Technology, Cyber Security Breaches Survey 2025/26, published April 2026.
- IBM, Cost of a Data Breach 2025, UK findings, July 2025.
- Information Commissioner's Office, Advanced Computer Software Group fine, March 2025.
- Google, 2025 DORA report, and DORA's software delivery metrics.
- Avelino, Passos, Hora and Valente, A novel approach for estimating truck factors, ICPC 2016.
- MIT Sloan, Your acquired hires are leaving: here's why, on Daniel Kim's research.
- Copyright, Designs and Patents Act 1988, section 11.
- Mishcon de Reya, data protection complaints duty from 19 June 2026, 2026.
- Skadden, Cyber Resilience Act reporting FAQs and checklist, September 2026.
- Gibson Dunn, EU AI Act omnibus agreement, 2026.
- Latham & Watkins, EU Data Act switching requirements, August 2025.
- Herbert Smith Freehills Kramer, government response on NSI Act mandatory sectors, 2026.
- GOV.UK, UK product security regime (PSTI).
- Paul Hastings, Insuring the deal: the role of W&I insurance, 2026.

Other good free checklists, credited

- AKF Partners frames diligence around the investment thesis and the cost of closing critical gaps, across people, process and technology. Its preparation guide is useful for targets.
- Crosslake sets out a broad scope including SDLC, business continuity, customer support and enterprise systems, and offers a pre-LOI review.
- Thomas Prommer's technology due diligence checklist covers ten domains with evidence lists and deal levers.
- Peony's technical due diligence guide has a clear data-room folder structure and ranked red flags.
- TechCrunch's prep checklist for startups is a good founder-side starting point.
- madewithlove on what is in a technical due diligence report is a candid practitioner view of the deliverable.

Most of these stop at the inventory: areas and documents, sometimes red flags. Few cost findings, route them into the SPA or the model, separate one-off from annual costs, or give a numbered request list and a working tracker.

Related Anyway Ventures articles: technology due diligence checklist, technical due diligence questions, what a technical due diligence report should contain, technical due diligence cost UK and key person risk in due diligence. The service is described on technical due diligence.

27. About this resource

Written by Anyway Ventures, the York technology and AI practice led by Brannan Coady, who has been on both sides of technical due diligence as a founder, CEO and investor. Version 1.0, October 2026. Free to use, adapt and share with attribution. Not legal, tax or investment advice.

ABOUT ANYWAY VENTURES

Senior hands for technology and AI decisions

Technology and AI work for private equity funds, venture investors and UK mid-market management teams: before a deal, during the hold and at exit. Every engagement is led by Brannan Coady, an exited founder and former CEO. Fixed price, built to be handed over.

FOR INVESTORS

Technical due diligence

Code, architecture, security, IP and one-to-one team interviews, every material finding costed. Red-flag review in five to seven days.

ANYWAYVENTURES.COM/TECHNICAL-DUE-DILIGENCE

AI due diligence

Whether a target's AI claims are real, defensible and theirs, and a costed AI value-creation plan for the IC.

ANYWAYVENTURES.COM/AI-DUE-DILIGENCE

AI disruption risk review

Is AI a threat to the business or its moat? One deal, or every holding in a portfolio ranked by exposure.

ANYWAYVENTURES.COM/AI-DISRUPTION-RISK

Technical due diligence for VCs

A two to three day check before the term sheet: the product tested on evidence, not the demo.

ANYWAYVENTURES.COM/VC-TECHNICAL-DUE-DILIGENCE

Retained AI operating partner

Senior AI capacity held by the fund and deployed into the company with the strongest AI value case.

ANYWAYVENTURES.COM/AI-OPERATING-PARTNER

Exit readiness and vendor technical due diligence

Find what a buyer's diligence will find, 12 to 24 months out, fix it, then publish a report buyers can rely on.

ANYWAYVENTURES.COM/EXIT-READINESS

FOR OPERATORS

AI audit and readiness assessment

Two to three weeks to a ranked, costed list of AI opportunities, the gaps to close and a 90-day plan.

ANYWAYVENTURES.COM/AI-AUDIT

Embedded AI delivery

Internal tooling, automation and AI agents in production inside your business, built with your team.

ANYWAYVENTURES.COM/EMBEDDED-AI-DELIVERY

Fractional Chief AI Officer

One senior person who owns AI on your leadership team, two to four days a month.

ANYWAYVENTURES.COM/FRACTIONAL-CHIEF-AI-OFFICER

Hands-on AI training

In-person training where every attendee builds a working tool on their own job.

ANYWAYVENTURES.COM/AI-TRAINING

Board and NED roles

Non-executive seats where technology, product and AI decide the outcome.

ANYWAYVENTURES.COM/BOARD-AND-NED

Every enquiry starts with the same free 30-minute call.

A straight answer on whether we can help, what it would cost and how long it would take.

EMAIL
brannan@anywayventures.com

BOOK A CALL
anywayventures.com/contact

MORE RESOURCES
anywayventures.com/resources

Anyway Ventures Limited · Registered in England and Wales, company number 16318119 · Registered office: Newbury House, Main Street, Little Ouseburn, York, YO26 9TD. This resource is general guidance, not legal, tax or investment advice. Free to use, adapt and share with attribution to Anyway Ventures. Version 1.0, October 2026.