

INVESTOR-GRADE · v2026.1

The IT Due Diligence Checklist

Sixty questions across ten sections used by Beyond M&A; on real PE and VC engagements — to surface red flags early and quantify the value at stake.

-
- | | |
|-------------------|---|
| ● RED FLAG | Issue likely to affect price, structure or speed of the deal. |
| ● VALUE | Evidence of strength — defensible in IC and useful in post-deal planning. |
-

How to use · Walk each section with the target's CTO or equivalent. Score each item Green / Amber / Red. Capture evidence references (docs, dashboards, demos). Convert Reds into price-chip items or conditions precedent; convert Greens into post-deal value-creation hypotheses.

Contents

01	Strategy & Operating Model	Does technology serve the business strategy — or constrain it?
02	Architecture & Platform	Will the architecture scale through the investment thesis?
03	Security	Would a breach materially impair the deal value?
04	Data & AI	Is data an asset you can defend, monetise and govern?
05	Engineering & Delivery	Can the team ship reliably, frequently and safely?
06	People & Organisation	Is the team the right shape, size and quality for the plan?
07	Vendors, Licensing & IP	Do you own what you think you own?
08	Operations & Resilience	Will the lights stay on through the value-creation plan?
09	Compliance & Regulatory	Are the obligations identified, evidenced and current?
10	Integration Readiness (Buy-Side)	How fast and how cheaply can this be integrated — or carved out?

01

Strategy & Operating Model

Does technology serve the business strategy — or constrain it?

#	Question	Marker
1	Is there a written tech strategy aligned to the 3-year business plan?	● RED FLAG if absent.
2	Who owns the tech roadmap, and is it reviewed quarterly with the board?	● VALUE: clear accountability.
3	How are build / buy / partner decisions made and documented?	
4	What is the current vs target operating model (in-house, hybrid, outsourced)?	
5	Are OKRs / KPIs in place for engineering and operations?	● VALUE: measurable delivery.
6	How is technical debt tracked, prioritised and funded?	● RED FLAG if no register exists.

Evidence / notes:

02

Architecture & Platform

Will the architecture scale through the investment thesis?

#	Question	Marker
1	Is there a current-state architecture diagram (apps, data, integration, infra)?	● RED FLAG if missing.
2	Which components are bespoke vs commodity SaaS — and why?	
3	What are the top 5 scalability bottlenecks at 3x volume?	● VALUE: known and costed.
4	Is the platform cloud-native, lift-and-shift, or on-prem? Single or multi-region?	
5	Are environments (dev / test / staging / prod) parity-managed and reproducible?	
6	What is the disaster recovery RTO / RPO — and when was it last tested?	● RED FLAG if untested in 12m.

Evidence / notes:

03

Security

Would a breach materially impair the deal value?

#	Question	Marker
1	Is there a named CISO or security owner with a board reporting line?	
2	Which security framework is followed (ISO 27001, SOC 2, NIST CSF, Cyber Essentials+)?	● VALUE: certified.
3	When was the last independent penetration test — and were findings remediated?	● RED FLAG if >12 months.
4	Is MFA enforced for all staff and privileged access reviewed quarterly?	
5	Is there an incident response plan — and has it been rehearsed in the last 12 months?	
6	Are customer data, PII and secrets encrypted at rest and in transit, with rotation policy?	● RED FLAG if secrets in repos.

Evidence / notes:

04

Data & AI

Is data an asset you can defend, monetise and govern?

#	Question	Marker
1	Is there a single source of truth for core entities (customer, product, transaction)?	● RED FLAG if conflicting masters.
2	Is data lineage documented end-to-end for material reporting?	
3	What AI / ML is in production — and is its decisioning explainable and logged?	
4	Are training data sources licensed and free of IP / privacy contamination?	● RED FLAG if unclear provenance.
5	Is there an AI usage policy covering staff use of third-party LLMs?	● VALUE: governed adoption.
6	How is data quality measured — and who is accountable for it?	

Evidence / notes:

05

Engineering & Delivery

Can the team ship reliably, frequently and safely?

#	Question	Marker
1	What is the change failure rate and mean time to recover (DORA metrics)?	● VALUE: top-quartile.
2	Is CI/CD in place across all production services with automated tests?	● RED FLAG if manual deploys.
3	What is test coverage for critical paths — and is it trended?	
4	How are feature flags, blue/green or canary deploys used to de-risk releases?	
5	Is the code reviewed, with branch protection and signed commits?	
6	Are observability (logs, metrics, traces) and SLOs in place for tier-1 services?	● VALUE: data-driven ops.

Evidence / notes:

06

People & Organisation

Is the team the right shape, size and quality for the plan?

#	Question	Marker
1	Org chart — is there clear ownership for product, platform, security and data?	
2	What is the bus factor on critical systems — and is knowledge documented?	● RED FLAG if <2 on key systems.
3	Voluntary attrition by team and seniority over the last 24 months?	
4	Engineering compensation vs market benchmark for the geographies hired in?	
5	Is there a hiring plan aligned to the roadmap and budget?	
6	Are contractors / offshore vendors integrated into the SDLC and security model?	● RED FLAG if shadow access.

Evidence / notes:

07

Vendors, Licensing & IP

Do you own what you think you own?

#	Question	Marker
1	Is there a current vendor / SaaS register with renewal dates and owners?	● RED FLAG if missing.
2	Any single-vendor lock-in that materially affects price, exit or roadmap?	
3	Open source: SBOM in place, licenses reviewed for copyleft exposure?	● RED FLAG if GPL in SaaS core.
4	Is all IP assigned to the company (employees, contractors, founders, acquisitions)?	● RED FLAG if assignments missing.
5	Are customer contracts free of unusual IP, source code escrow or MFN clauses?	
6	Cyber insurance — limits, exclusions, and last claim history?	

Evidence / notes:

08

Operations & Resilience

Will the lights stay on through the value-creation plan?

#	Question	Marker
1	Uptime / availability for tier-1 services over the last 12 months vs SLO?	● VALUE: ≥99.9% with evidence.
2	Top 5 production incidents — root cause, customer impact, corrective actions?	
3	Capacity headroom on compute, storage and database for next 18 months?	● RED FLAG if <30%.
4	Backup strategy — frequency, retention, off-site, restore-tested?	
5	Run-book coverage and on-call rotation for tier-1 services?	
6	Cost of cloud / hosting trend over 24 months and committed-spend exposure?	

Evidence / notes:

09

Compliance & Regulatory

Are the obligations identified, evidenced and current?

#	Question	Marker
1	Which regulations apply (GDPR, UK GDPR, HIPAA, FCA, PCI DSS, EU AI Act)?	
2	Is there a current Record of Processing Activities (Art. 30) and DPIAs where required?	● RED FLAG if absent.
3	Sub-processor list maintained and surfaced to customers?	
4	Data residency: where is customer data stored, and does it match contracts?	● RED FLAG if mismatched.
5	Cookie / consent management deployed and audited?	
6	Any open regulatory investigations, complaints or breach notifications in last 36 months?	

Evidence / notes:

10

Integration Readiness (Buy-Side)

How fast and how cheaply can this be integrated — or carved out?

#	Question	Marker
1	Is the target separable from its parent (shared services, identity, finance)?	
2	TSAs required — for what, for how long, and at what cost?	
3	Identity & access: can users be merged into the acquirer's IdP within 90 days?	● VALUE: SSO-ready.
4	Data migration: are core entities mappable to the acquirer's model?	
5	Integration cost estimate — one-off and run-rate — with confidence interval?	● RED FLAG if no estimate.
6	Day-1, Day-30, Day-100 IT integration plan with owners and milestones?	● VALUE: plan exists pre-close.

Evidence / notes:

Next steps

If you'd like Beyond M&A; to run this checklist against a target — or to use Lens, our scoring platform — get in touch. We turn checklist findings into a board-ready Tech DD report with price-chip evidence and a costed remediation plan.

beyond-ma.com · hello@beyond-ma.com