

M&A IT

Due Diligence Checklist

A practical guide to identifying technology risk, cost and delivery considerations before a transaction completes.

The purpose of this checklist

Use this guide to frame early conversations, organise evidence and identify matters that may affect valuation, deal structure, transition planning or integration. It is designed as a starting point, not a substitute for detailed technical, commercial, cybersecurity or legal due diligence.

WHAT GOOD DUE DILIGENCE SHOULD REVEAL

- Where material technology risks sit
- What investment may be required after completion
- Whether the business can separate, integrate and continue operating
- Which decisions must be addressed before signing or completion

Clarity before commitment.

bushey.com.au

How to use this checklist

Work through each section with the deal team, technology leadership and relevant advisers. Mark items confirmed, flag gaps in evidence and record any issue that could affect the transaction or the first 100 days.

Status	Meaning	Impact	Action
Confirmed	Evidence is available and consistent	Known	Record and retain
Open	Evidence is incomplete or unclear	Possible	Request clarification
Concern	A material weakness or exposure exists	Likely	Quantify and escalate
Deal issue	May affect value, structure or completion	Material	Address before decision

Keep the focus on decisions

The value of due diligence is not the number of documents reviewed. It is whether the deal team understands the exposure, the options and the actions required.

01 TRANSACTION CONTEXT AND TECHNOLOGY PERIMETER

Start by establishing exactly what is being bought, sold or combined. Ambiguity here will undermine every later conclusion.

☐	Confirm the transaction structure, key dates and decision gates.
☐	Define the legal entities, business units, sites, products and geographies in scope.
☐	Identify technology, people, contracts and assets that are excluded or shared with the seller or group.

- | | |
|--------------------------|---|
| ☐ | Confirm whether the transaction requires separation, integration, standalone operation or a combination of all three. |
| ☐ | Map critical business services to the technology that supports them.
<i>Prioritise services whose interruption would materially affect customers, revenue, safety, regulation or reputation.</i> |
| ☐ | Identify known deal assumptions that depend on technology cost, capability or timing. |

02 TECHNOLOGY ESTATE AND ARCHITECTURE

Build a fact-based view of the current environment, its condition and its ability to support the investment case.

- | | |
|--------------------------|---|
| ☐ | Obtain a current inventory of applications, infrastructure, cloud services, networks, end-user technology and Data Centres. |
| ☐ | Identify unsupported, end-of-life, highly customised or single-vendor technologies. |
| ☐ | Assess whether architecture diagrams and asset records reflect the live environment. |
| ☐ | Identify critical integrations, manual workarounds and points of failure. |
| ☐ | Review capacity, performance, resilience and availability for critical systems. |
| ☐ | Identify technical debt and major remediation, refresh or migration commitments. |
| ☐ | Confirm ownership of source code, configurations, domains, certificates and other key technology assets. |

03 CYBERSECURITY AND RESILIENCE

Establish whether security exposure could create financial, operational or regulatory consequences for the buyer.

- | | |
|--------------------------|---|
| ☐ | Review the current cybersecurity strategy, governance model and accountable executives. |
| ☐ | Obtain recent penetration tests, vulnerability assessments, audit findings and remediation plans. |
| ☐ | Identify material incidents, breaches, ransomware events and regulatory notifications. |
| ☐ | Assess identity and access management, including privileged access and joiner, mover and leaver controls. |
| ☐ | Review endpoint, network, email, cloud and third-party security controls. |
| ☐ | Confirm backup integrity, recovery testing and protection from unauthorised alteration. |
| ☐ | Review business continuity, disaster recovery and crisis management arrangements. |
| ☐ | Identify cybersecurity obligations within customer, supplier and regulatory commitments. |

04 DATA, PRIVACY AND INFORMATION MANAGEMENT

Understand what data is held, where it moves, who controls it and whether it can be transferred or separated lawfully.

- | | |
|--------------------------|--|
| ☐ | Identify critical, sensitive, personal, regulated and commercially valuable data sets. |
| ☐ | Confirm data ownership, locations, flows, retention requirements and cross-border transfers. |
| ☐ | Review privacy compliance, consents, notices, assessments and unresolved complaints. |
| ☐ | Assess data quality, lineage, duplication and dependence on manual reconciliation. |
| ☐ | Identify data held in unsupported systems, shared repositories or uncontrolled end-user tools. |
| ☐ | Confirm how data will be transferred, retained, deleted or segregated at completion. |

- ☐ Review access to data by suppliers, offshore teams and other group entities.

05 APPLICATIONS AND SOFTWARE

Determine whether the application portfolio is supportable, appropriately licensed and aligned to the future operating model.

- ☐ Identify applications critical to revenue, operations, customer service, finance and regulatory reporting.
- ☐ Confirm application ownership, support arrangements, lifecycle position and roadmap.
- ☐ Review software licensing, assignment rights, usage compliance and potential true-up exposure.
- ☐ Identify applications that are shared with the seller or dependent on group services.
- ☐ Assess custom development, code ownership, documentation and key-person dependency.
- ☐ Identify planned replacements, major upgrades or programmes already committed.
- ☐ Confirm whether applications can scale or integrate to support the transaction thesis.

06 SUPPLIERS, CONTRACTS AND COMMERCIAL EXPOSURE

Technology value and continuity often depend on contract rights that do not automatically transfer with the transaction.

- ☐ Create a schedule of material technology suppliers, services, term dates and annual spend.
- ☐ Identify change-of-control, assignment, termination, volume and minimum-commitment provisions.
- ☐ Confirm whether licences and services can be novated, separated or continued after completion.
- ☐ Review service levels, credits, disputes, outstanding claims and supplier performance concerns.
- ☐ Identify concentration risk and reliance on strategic or difficult-to-replace suppliers.
- ☐ Assess whether current pricing depends on group-wide purchasing power or bundled agreements.
- ☐ Identify renewal, exit, transition and data-return obligations that may affect the deal timetable.

07 TECHNOLOGY ORGANISATION AND CAPABILITY

Understand whether the target has the leadership, capability and capacity to operate and change after completion.

- ☐ Review the technology organisation structure, roles, locations and reporting lines.
- ☐ Identify critical individuals, scarce skills, contractors and key-person dependencies.
- ☐ Confirm which people are transferring, remaining with the seller or shared across the group.
- ☐ Assess leadership capability, operational maturity and the ability to deliver the future roadmap.
- ☐ Review attrition, vacancies, succession plans and retention risks.
- ☐ Identify outsourced functions and clarify retained accountability.
- ☐ Estimate additional capability required for separation, integration and business-as-usual support.

08 GOVERNANCE, DELIVERY AND CHANGE PORTFOLIO

A crowded or poorly governed change portfolio can create hidden cost and distract the organisation during transition.

- ☐ Review technology decision rights, governance forums, risk management and financial controls.
- ☐ Obtain the current portfolio of projects, programmes and committed investment.

- ☐ Identify initiatives that are critical, delayed, over budget, under-resourced or supplier-dependent.
- ☐ Assess whether reported status, costs, benefits and completion forecasts are credible.
- ☐ Identify regulatory, customer or contractual change commitments that cannot be deferred.
- ☐ Confirm how programmes will be governed during the transaction and transition period.
- ☐ Identify initiatives that should stop, continue, accelerate or be re-planned after completion.

09 SEPARATION AND TRANSITIONAL SERVICE AGREEMENTS

For carve-outs, determine what must be disentangled and what support is required until the buyer can operate independently.

- ☐ Identify every shared platform, service, team, contract, process, network and data dependency.
- ☐ Define the minimum technology capability required for legal completion and operational continuity.
- ☐ Confirm proposed Transitional Service Agreement scope, service levels, pricing, duration and exit responsibilities.
- ☐ Assess whether the seller can provide the proposed services reliably and securely.
- ☐ Identify dependencies that could extend Transitional Service Agreements or increase separation cost.
- ☐ Confirm requirements for identity, connectivity, data migration, licences, domains and support tooling.
- ☐ Develop an initial separation roadmap with critical path, decision dates and buyer responsibilities.

10 INTEGRATION READINESS AND FIRST 100 DAYS

Convert due diligence findings into an executable plan that protects the business while capturing value.

- ☐ Confirm the intended target operating model and technology principles for the combined organisation.
- ☐ Identify Day 1 controls needed for access, cybersecurity, communications, support and incident management.
- ☐ Prioritise risks that require immediate containment after completion.
- ☐ Identify integration dependencies, sequencing constraints and decisions that cannot be delayed.
- ☐ Validate synergy assumptions against realistic cost, timing and delivery capacity.
- ☐ Define governance, leadership, reporting and escalation for the integration programme.
- ☐ Prepare a 30, 60 and 100-day action plan with accountable owners and measurable outcomes.

11 FINANCIAL EXPOSURE AND DEAL IMPLICATIONS

Bring technology findings back to the investment decision in clear commercial terms.

- ☐ Estimate one-off separation, integration, remediation and transformation costs.
- ☐ Identify recurring cost increases, stranded costs and duplicate services.
- ☐ Validate technology-related synergy assumptions and the timing of benefit realisation.
- ☐ Identify capital expenditure, licence true-ups, contract exit charges and retention costs.
- ☐ Distinguish immediate risk containment from longer-term modernisation investment.

- ☐ Confirm which issues may require a price adjustment, indemnity, warranty, condition precedent or specific completion action.
- ☐ Present the most material findings in plain language for the investment committee or Board.

Due diligence findings summary

Use this page to capture the matters that require a decision, not every observation made during the review.

Finding	Status	Deal impact	Owner	Required by

QUESTIONS FOR THE DEAL TEAM

- ☐ What could stop the transaction achieving its intended value?
- ☐ What must be resolved before signing or completion?
- ☐ What must be stabilised on Day 1?
- ☐ What investment is required in the first 12 to 24 months?
- ☐ Which assumptions remain untested?

A final sense check

Can the organisation continue to operate safely, lawfully and effectively through the transaction, and is the technology plan credible enough to support the investment case?

WHEN THE TRANSACTION NEEDS A DEEPER REVIEW

Consider specialist support where the technology environment is complex, the evidence is incomplete, the timetable is compressed, the target operates critical services, or the transaction includes significant separation or integration risk.

How Bushey helps

Bushey provides independent technology due diligence, separation and integration planning, transaction governance and delivery leadership. We help M&A Executives understand what they are buying, what it will take to change it, and where the risks need to be controlled.

Clarity. Accountability. Delivery.

bushey.com.au