IT Due Diligence Checklist

A buyer-focused technology review intended to reveal operational risk, hidden cost and integration or separation complexity before they become post-transaction surprises.

Technology estate

[ ]	Sites, networks, cloud platforms, servers, devices and major applications are inventoried.	Yes / Partly / No
[ ]	Unsupported technology and material technical debt are identified.	Yes / Partly / No
[ ]	Capacity, availability, monitoring, backup and recovery arrangements are understood.	Yes / Partly / No
[ ]	Architecture and dependency documentation is available and current.	Yes / Partly / No
[ ]	Known outages, incidents and unresolved operational risks are disclosed.	Yes / Partly / No

Cybersecurity and compliance

[ ]	Identity, MFA, privileged access and joiner/mover/leaver controls are assessed.	Yes / Partly / No
[ ]	Material vulnerabilities, security incidents and remediation actions are reviewed.	Yes / Partly / No
[ ]	Regulatory, contractual, privacy and data-residency obligations are mapped.	Yes / Partly / No
[ ]	Security monitoring, incident response and cyber-insurance conditions are understood.	Yes / Partly / No
[ ]	Third-party and supply-chain security risks are included.	Yes / Partly / No

Applications, data and licences

[ ]	Critical applications, owners, interfaces and support status are documented.	Yes / Partly / No
[ ]	Licence ownership, renewal, transfer and change-of-control terms are checked.	Yes / Partly / No
[ ]	Data locations, quality, retention, migration and deletion obligations are understood.	Yes / Partly / No
[ ]	ERP, CRM, finance, HR and operational systems have credible transition plans.	Yes / Partly / No
[ ]	Separation constraints and transitional service requirements are identified.	Yes / Partly / No

People, suppliers and transaction plan

[ ]	Key-person dependencies and capability gaps are assessed.	Yes / Partly / No
[ ]	Supplier contracts, service levels, notice periods and concentration risks are reviewed.	Yes / Partly / No
[ ]	Day-one access, connectivity, support and security requirements are planned.	Yes / Partly / No
[ ]	Integration or separation costs include technology, licences, people and suppliers.	Yes / Partly / No
[ ]	A prioritised 30/60/90-day technology plan has owners and budget assumptions.	Yes / Partly / No

Priority actions

1. ____

2. ____

3. ____

This checklist is general guidance, not legal, regulatory or security assurance. The appropriate controls depend on your organisation, risks, contracts and regulatory obligations.