Technical Due-Diligence Checklist

Product:

- General overview
- Particularly challenging areas
- Points of differentiation
- Roadmap

Architecture:

- High-level overview
- Tech stack
- Future plans
- Known issues

Core algorithms:

- Basic approach
- Training data
- Validation

Integrations:

- APIs (both inbound and outbound)
- Other integrations and interfaces

Team:

- Structure
- Culture

Process:

- Approach (e.g., Scrum, Kanban, …)
- Local customisations (if any) of the above approach
- QA and testing
- Deployment

Operations:

- Monitoring
- Support
- Resilience
- Disaster recovery

Security and Data Protection:

- Security architecture and incident response plans
- Security tests, certifications, or other validation
- Data protection in general, GDPR

Intellectual Property:

- Defensibility
- Relevant 3rd party IP

Preparing for Tech DD

The above is a generic checklist; inevitably some areas will be of more or less relevance to a specific engagement (so don't worry if some seem irrelevant to your particular case).

Ahead of Tech DD it can be helpful to collect and forward any pre-existing documentation or reports such as:

- Product Roadmap
- Software Architecture
- Deployment Architecture
- DORA metrics or similar
- Test coverage and test results
- Penetration tests or other third-party audits
- Root cause analysis of any security breaches
- Uptime and root cause analysis of any outages
- etc…

Please don't spend any time creating any of the above if they aren't easily to hand; Tech DD can be a time-consuming distraction, and the object of the above is to avoid, not create, work. Questions which aren't already covered by existing documents are most efficiently answered through discussions with the CTO and other relevant members of the technical team.