An introduction to
TECHNICAL DUE DILIGENCE
An introduction to technical due diligence

Technical due diligence is an audit, investigation or review performed on a technical/software company (i.e. a company that is tech native, meaning that its core products or services are digital).

What technical due diligence is not:

• An evaluation of the IT environment of a non-tech target company
• Just a complement to the operational and commercial due diligence
• A code review (although Implement Consulting Group can perform a code inspection health check if needed)
What is technical due diligence and why should you conduct it?

**WHAT**
Technical due diligence is an audit, investigation or review performed on a tech company (i.e. a company that is tech native, meaning that its core products or services are digital).

In the investment decision process for tech companies, technical due diligence replaces the role of the commercial and operational due diligence. The rationale being that for tech companies, other topics are important in order to evaluate the possible risks and opportunities for the target company.

Tech due diligence includes an evaluation of the target’s tech strategy, product and/or services, IT architecture and infrastructure, IT processes and security, tech organisation and software development lifecycle and the tech financials.

**WHY**
A technical due diligence is better suited for tech companies, as it captures the topics that traditional commercial due diligence would miss, including:

- A sound technical setup is key for performance and significantly affects commercial abilities (such as scalability).
- A legacy (old) platform/product requires significant investment in competences and time in order to modernise.
- A thorough key person risk analysis, as it is particularly important for tech companies which are dependent on certain competences and company-specific knowledge.

**HOW**
Like traditional due diligence, technical due diligence requires access to certain information to be successful. The process is similar to that of commercial due diligence.

- It requires access to the target’s data and technical setup and management, including CPO and CTO.
- Normally, technical due diligence would take 2-3 weeks, given that the target has capacity to provide all necessary information in that timeframe.
- In order to conduct technical due diligence, a combination of deep commercial and technical expertise is required.
Components of technical due diligence

With a starting point in the investment thesis and key questions, technical due diligence includes a thorough evaluation of the target. This includes its tech strategy, product and/or services, IT architecture and infrastructure, IT processes and security, tech organisation and software development lifecycle and the tech financials.

The foundation of technical due diligence lies in the investment thesis and the underlying key questions that are specific for the acquisition.

**Investment thesis and key questions**

The foundation of technical due diligence analysis lies in the investment thesis that is provided and agreed upon together with the acquiring firm. It entails the main rationale/hypothesis that should be tested.

The investment thesis is split into several key questions, which tests different aspects of the thesis. The key questions are often developed in collaboration with Implement, as we know from experience which issues are important to stress test.

In addition to an overall assessment of the target company from a technical viewpoint, the answers to the key questions and a validation if they support the investment thesis are the main deliverables.

**Illustrative examples**

**INVESTMENT THESIS**

Company “X” is interested in investing in “Target” with the rationale of increasing market shares and gaining knowledge in their technology domain.

**KEY QUESTIONS**

1. How sticky is the business? (I.e. what is the risk that Target’s customers leave after the acquisition?)

2. Is Target well positioned to create new products and services from a technical and commercial point of view?

3. How well are Target’s current applications and capabilities in ML/AI?
Implement’s approach for technical due diligences is built on six key pillars with four supporting elements

Description

- The technical due diligence framework consists of six primary domains (centre) and four supporting domains (sides).
- The primary domain reflects a subset of a company’s ability to support the daily business operations.
- The supporting or secondary domain provides the boundaries and guidelines for the primary domains.

Figure 1: Technical due diligence framework
Technical strategy

A validation of how well the technical and product strategy is aligned with the overall business strategy

**KEY QUESTIONS**

1. Does the target have a formulated tech and product strategy, and how does it align with the overall business strategy?

2. What are the required and planned investments in tech going forward?

3. How does the target use emerging technologies such as ML/AI, and what capabilities does it currently have?

**analyses - example**

**Product roadmap**

- What products/services/improvements are planned going forward?
- What is the focus and relation to new technologies?
- How mature is the target when it comes to the product road map?

**Market outlook and competition**

- What is the market size and growth rate?
- Who are the key competitors, and how do they perform in relation to the target?
- Are there any other aspects that might affect market attractiveness going forward?

**Strategic partnerships**

- How does the target work with strategic partnerships and integrations?
- What are the business risks associated with said partnerships?

**Technical strategy**

- How does the target use emerging technologies such as ML/AI, and what capabilities do they currently have?
- What areas will the target invest in going forward?
- How does the tech strategy align with the overall business strategy?

**Data sources**

- Internal documentation
- Interviews with CTO and CPO
- External market research
Platform, architecture, applications

Are products kept up to date and is the underlaying architecture scalable and modern?

**KEY QUESTIONS**

1. What are the products/services offered to customers, and how are they maintained?

2. What are the back-office applications in place, and how are they maintained?

3. How is the IT architecture structured, and how does this affect product performance, scalability and business outlook and risks?

**Data sources**

- Internal documentation
- Interviews with CTO, CPO and IT architects
- External market research

**analyses - example**

**Service offering landscape**
- An overview of the service offering landscape, including buyer, business benefit/value proposition and performance relative to competition (for all commercial applications)

**Applications in use**
- A list of all commercial applications in use
- A list of all back-office applications in use
- A list of third-party key vendors/service providers

**IT architecture**
- Architecture diagram for all key commercial and custom (in-house developed) back-office applications
- Integration points to other systems (internal or external)
- Definition of architectural layers as well as potential integration platforms

**Integrations**
- What are the ingoing and outgoing integrations to the products/services offered?
- How does external integrations affect business? Do some of them pose a business risk?
People and software development lifecycle

How does the current organisational setup support operations and processes?

KEY QUESTIONS

1. What is the key person risk? (i.e. which employees are critical to the operations and in what way?)

2. What does the organisational setup look like? Is the organisation formed in a way that is suitable to support operations and growth (e.g. agile teams etc.)?

3. What is the target’s HR situation and strategy (e.g. recruitment etc.)?

HR KPIs

• What is the average and median tenure?

• What percentage of employees are tech workers?

• How diverse is the workforce?

Key person risk

• Which (and how many) employees are critical to operations?

• How easily could critical employees be replaced?

Organisational setup

• What does the organisational setup look like?

• Are teams organised in a way that supports an agile development?

Data sources

• Internal documentation
• Interviews with CTO, CPO and HR
• External market research
Tech financials

Are past and planned tech expenditures in line with the strategy and investment thesis?

**KEY QUESTIONS**

1. Are past tech expenditures in line with planned investments?
2. Do planned tech investments support the investment thesis?
3. What estimated OPEX and CAPEX are needed to support the tech strategy and the investment thesis?

**Data sources**

- Internal documentation
- Interviews with CTO and CFO
- External market research/benchmarks

**analyses - example**

**Tech financials**

- Which technologies/tech areas does the target plan to invest in going forward, and what do they plan to solve by doing so?
- How has CAPEX developed over time, and what are the projections going forward?
- Do projections include needed investments to replace legacy technology?
- How has OPEX developed, and what savings potential is there?
IT infrastructure

Does the infrastructure in place support current processes as well as future expansions?

KEY QUESTIONS

1. What is the general state of the IT infrastructure (servers, cloud etc.)?
2. How well does the IT infrastructure support its current purpose?
3. How well is the IT infrastructure suited for future plans and user growth? How much legacy is in place that will have to be replaced in the short/medium/long term?

analyses - example

IT infrastructure

- How and where are systems hosted? Does the target rely on physical servers or cloud services?
- Are there relevant current or planned regulations that will have to be taken into account?
- If necessary, how easy would it be to migrate data?
- How well is the IT infrastructure suited for future plans and user growth? How much legacy is in place that will have to be replaced in the short/medium/long term?
- What are the risks associated with the current setup?

Data sources

- Internal documentation
- Interviews with CTO, CPO and IT architects
IT processes and security

How secure is the target in terms of its capability to withstand an unintentional loss of information?

**KEY QUESTIONS**

1. What IT documentation is in place, available and of good quality?
2. What are the security procedures and processes? (i.e. disaster recovery, penetration tests, FOSS scans etc.)

**Data sources**

- Internal documentation
- Interviews with CTO, CPO and IT security management.
- External/third-party reports and audits

**analyses - example**

<table>
<thead>
<tr>
<th>TYPE OF DOCUMENTATION (ANONYMISED)</th>
<th>AVAILABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information security policy</td>
<td>✗</td>
</tr>
<tr>
<td>IT policy</td>
<td>✓</td>
</tr>
<tr>
<td>IT usage policy</td>
<td>✓</td>
</tr>
<tr>
<td>IT development policy</td>
<td>✓</td>
</tr>
<tr>
<td>IT documentation 4</td>
<td>✗</td>
</tr>
<tr>
<td>IT documentation 5</td>
<td>✗</td>
</tr>
<tr>
<td>IT documentation 6</td>
<td>✓</td>
</tr>
<tr>
<td>IT documentation 7</td>
<td>✓</td>
</tr>
<tr>
<td>IT documentation 8</td>
<td>✗</td>
</tr>
<tr>
<td>IT documentation 9</td>
<td>✗</td>
</tr>
<tr>
<td>IT documentation 10</td>
<td>✓</td>
</tr>
</tbody>
</table>

**IT security**

- What is the level of detail of IT documentation?
- Is the IT documentation available to the necessary people?
- Have penetration tests been carried out?
- Has FOSS scanning been carried out?
- Is real-time monitoring available?

**IT processes**

- What are the procedures for handling personal data? Are they GDPR compliant on all levels?
- Who has access to backups and the production environment?
- What is the incident response plan?
- What disaster recovery procedures are in place?
- What is the procedure/cadence for backups/read-backs?
Typical technical due diligence at Implement takes around 2-3 weeks and consists of desk research as well as interviews with the target and industry experts.

A core team experienced in technical due diligence is complemented by consultants with M&A or industry experience, and subject matter experts on the target industry are consulted.
TECHNICAL DUE DILIGENCE PROJECT PLAN (2-3 WEEKS)

General project plan
- Kick-off and mobilisation
- Main due diligence phase
- Consolidations

Project management
- Kick-off
- Check-in
- Check-in
- Final report

Key activities
- Team mobilisation
- Final scope adjustments
- Develop interview guides
- Plan, book and conduct initial interviews
- Conduct customer and expert interviews
- Desktop and digital tools research
- Deep-dive analysis on the selected topic
- Finalise analyses, summarise interviews and prepare final green/red flag report
- Additional interviews as needed
- Finalise report and green/red flag evaluations
- Distribute IRL

Targets’ required participation
- Management team presentation and expert session
- Interviews with digital leaders
- Provide responses to clarifying questions and validate findings
Contact

For more information please contact:

Andreas Lodhammar
+46 733 211 665
anlo@implement.se

Mike Polczynski
+45 4138 0006
mipo@implement.dk

Torbjörn Månsson
+46 727 326 068
torm@implement.se

Lennart Lundberg
+46 738 080 953
lelu@implement.se