WHITE PAPER

Key Factors of IT Due Diligence

Minimising risks in business acquisitions. February 2016.

PROCOMM IT Concepts AG | Zürichstrasse 38 | 8306 Brüttisellen
info@procomm-it.com | +41 44 820 77 77

www.redflag-analysis.com

INTRODUCTION

IT is one of the most common causes for immense and unpredictable costs after the acquisition of a company. McKinsey has determined that 50% to 60% of initiatives to develop synergies are strongly connected to IT – yet nevertheless, insufficient attention is often being paid to IT before and after the deal [1].

A flawed or complete lack of IT diligence may result in oversights of important opportunities and risks that have a significant impact on the purchasing price.

The reasons for an insufficient examination of IT can vary: Generally, IT is host to issues of enormous complexity. Expert know-how and a specific methodology are required to process the basis for decisions. A weak integration between the deal team and the integration team may also cause preventable IT cost traps in the post-merger integration phase. Last but not least, the IT due diligence choices available on the market are too academic in terms of their conception and thus unfit to quickly deliver practical results. Mid-sized and smaller transactions, in particular, are often faced with an unsurmountable hurdle.

This white paper addresses M&A professionals as well as corporate CIOs and demonstrates the key factors for a convincing IT due diligence.

THE CHALLENGE

IT due diligence aims at examining the IT of the target company in terms of risks and opportunities. Established opportunities fall into the following categories:

- Synergy potentials
- Efficiency potentials
- Strategic IT assets

Especially the latter, "strategic IT assets", often falls victim to the urge to save costs. At the same time, many an enterprise possesses a wealth of IT assets that could be highlighted as valuable components. For example, a highly competent IT development team or a sophisticated production planning solution in the target company. Such IT assets must be identified and protected from potential political trench warfare. The value of an enterprise directly depends on it.

There are three dimensions to potential risks:

Operative Risks
At their occurrence, operative risks result in negative implications on the economic and reliable execution of business processes in the target company.

Monetary Risks
Monetary risks correspond to potential unforeseen (re)investments due to replacement needs or external financial demands on the target company.

Dependency Risks
Dependencies on employees, suppliers or other parties that bear a relation to the target company may limit strategic management in its ability to act. Some of these dependencies are to be classified as risks. It is often the case that the continuation of central systems is dependent on individuals.

At the same time, these risk categories are connected to different subject matters in IT and are difficult to spot from a superficial outsider's view on the target company. Key persons like CIOs or other experts only recognise a part of the risks since the known "construction sites" cover up the other risks. What is more, M&A as a starting point demands for a more nuanced assessment than what is usually grasped from a purely operative perspective.

OUTSIDER'S VIEW VS REALITY AT THE BASE

The initial outsider's view before IT due diligence can be seen as a direct antipole to the reality at the base (figure 1).

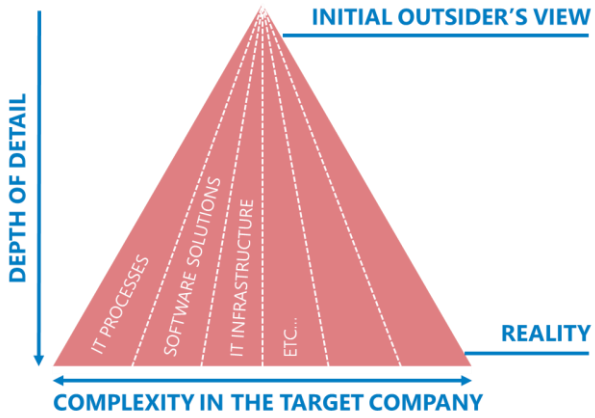

Figure 1: Complexity pyramid

Time restrictions and available budget are thus to be reconciled with depth of detail per subject area. The challenge consists of identifying risks and opportunities in an accurate manner and under time pressure, performing financial estimates and demonstrating courses of action according to the corporate context. These courses of action also include potential integration scenarios.

The following passages describe the key factors required to successfully meet these challenges.

A COMPETENT TEAM

The first key factor consists of assembling a competent and preferably small team that comprises all subject-specific and methodological skills. The subject-specific skills may vary depending on the concrete situation. For example, in addition to IT know-how (infrastructure, security, development, architecture, etc.), the team should also represent expertise in areas such as business processes and corporate strategy. Initially, the team is tasked with determining relevant informants in the target company. Afterwards, the team executes a balanced provision of information.

PROVISION OF INFORMATION

The second key factor consists of the balanced and cross-departmental provision of information in the target company. This provision of information should be carried out in an unbiased manner and may not be prematurely limited by existing knowledge. Otherwise, significant opportunities and risks may be overlooked. In this phase, depth of detail is purposely kept shallow.

The means to obtain information are interviews with relevant informants in the target company. Software-supported tools assist in covering all relevant points in the interviews and in calculating risks from the answers (figure 2). The psychological aspect must not be underestimated in interviews, since significant facts and connections may be detected "between the lines."

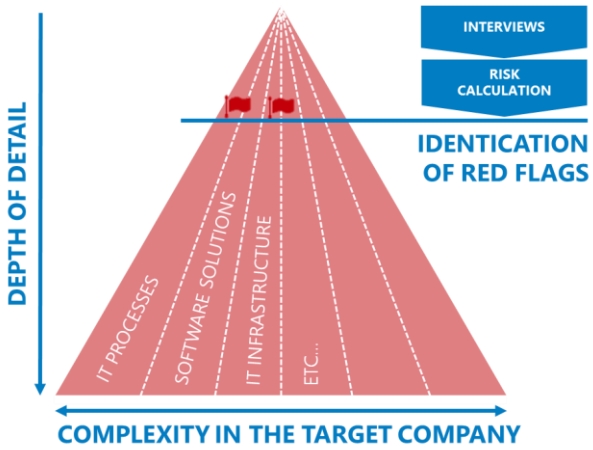

Figure 2: Interviews and risk calculation

Subject areas with an accumulation of risks should be emphasised as "Red Flags", indicating that an examination at greater depth of detail is appropriate.

Pitfalls:
In practice, one often encounters self-made or purchased checklists for interviews. Many of these checklists are rather one-sided and only adequately portray IT infrastructure and security, but fail to recognise other subject areas like software development or corporate applications such as ERP systems (e.g. SAP).

TARGETED ANALYSES

The third key factor consists of targeted analyses in the right places with appropriate depth of detail (figure 3). This task resides with the experts in the team who, based on the obtained information, now have to come to the right conclusions and should adequately allocate resources to the conspicuous spots in the target company.

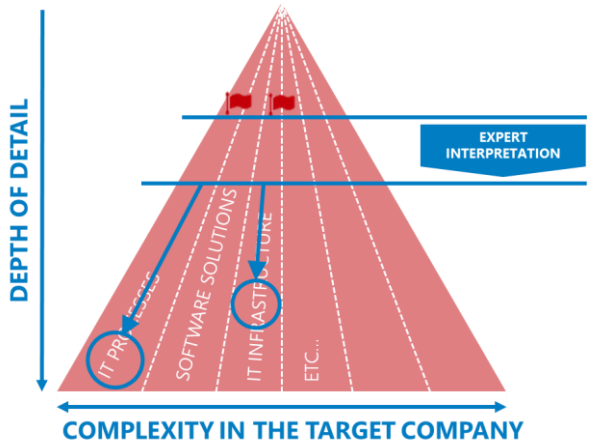

Figure 3: Targeted Analyses

The experts on the team must now provide the gathered insights with specific financial estimates and courses of action. A matching range of possible integration scenarios must be included at this point.

Pitfalls:
In practice, in-depth analyses are often performed in areas with a high concentration of in-house expertise.

This approach may entail high follow-up costs. It may lead to an investigation of e-mail systems, for example, although the risks may clearly be otherwise located in applications in high need of investments.

SUITABLE PRESENTATION

The forth key factor consists of delivering the insights and courses of action to IT due diligence clients in a suitable format. Since clients are required to base their decisions on solid grounds, they depend on a suitable and comprehensible presentation that takes into account their respective context.

CONCLUSION

IT is one of the most common causes for post-acquisition costs that are difficult to estimate. The following key factors of IT due diligence are essential in the timely recognising of opportunities and risks relating to purchasing costs:

- A competent team, as small as possible and still equipped with all subject-specific and methodological skills
- A balanced, cross-departmental provision of information with little depth of detail to ensure overview
- Targeted analyses in the right places and at the right depth of detail, incl. possible scenarios
- Suitable presentation of insights and courses of action as a solid basis for decision to the IT due diligence client

THE REDFLAG ANALYSIS™ METHOD

IT due diligence in accordance with the REDFLAG ANALYSIS™ method minimises risks in M&A transactions. PROCOMM has extrapolated this method from many years of practical experience and has perfected it using a specifically developed software tool. This tool guides the whole process of due diligence assessments and automatically executes the risk calculation. This enables the PROCOMM expert to conduct an IT due diligence assessment in a very short amount of time. The specific insights and courses of action to minimise risk and develop potentials are expressed in a language that is both clear and comprehensible for the client. Due to the REDFLAG ANALYSIS™ method, management is able to guide the further development of the company in a targeted manner and according to their own priorities.

CONTACT

PROCOMM IT Concepts AG
Zürichstrasse 38
8306 Brüttisellen, Switzerland

Web www.redflag-analysis.com
Email adrian.henke@procomm-it.com
Phone +41 44 820 77 77

Author: Adrian Henke

[1] H. Sarrazin and A. West, "Understanding the strategic value of IT in M&A" *McKinsey Quarterly,* vol. January 2011, p. 3, 2016.