WHITE PAPER

Schlüsselfaktoren der IT Due Diligence

Risikominimierung bei Unternehmens-Akquisitionen. Februar 2016.

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

www.redflag-analysis.com

EINFÜHRUNG

Die IT ist einer der grossen Favoriten für immense und schwer abschätzbare Kosten nach der Akquisition eines Unternehmens. McKinsey hat ermittelt, dass 50% bis 60% der Initiativen zur Erschliessung von Synergien einen starken Bezug zur IT haben – und trotzdem wird die IT vor und während dem Deal oftmals nur unzureichend beachtet [1].

Durch mangelhafte oder fehlende IT Due Diligence werden wichtige Chancen und Risiken übersehen, welche signifikanten Einfluss auf den Kaufpreis haben.

Die Ursachen für die vernachlässigte Prüfung der IT sind vielseitig: Generell birgt die IT eine enorme Komplexität. Die Aufbereitung der Entscheidungsgrundlagen benötigt Expertenwissen und spezifische Methoden. Auch eine schwache Integration zwischen Deal-Team und Integrations-Team kann eine Ursache sein von vermeidbaren IT-Kostenfallen in der Post-Merger-Integration. Nicht zuletzt sind auch die IT Due Diligence Angebote auf dem Markt zu akademisch konzipiert, um in der Praxis rasch Ergebnisse bereitstellen zu können. Insbesondere bei mittleren und kleineren Transaktionen ist die Hürde häufig zu gross.

Dieses White-Paper richtet sich an M&A Professionals sowie an Corporate CIO's und zeigt auf, was die Schlüsselfaktoren für eine aussagekräftige IT Due Diligence sind.

DIE HERAUSFORDERUNG

Bei einer IT Due Diligence geht es darum, die IT des Zielunternehmens hinsichtlich Risiken und Chancen zu beurteilen. Die gängigen Chancen fallen in die folgenden Kategorien:

- Synergiepotentiale
- Effizienzpotentiale
- Strategische IT Assets

Gerade die letztgenannte Kategorie „Strategische IT Assets" fällt regelmässig dem Drang zur Kostenersparnis zum Opfer. Dabei gibt es in manch einem Unternehmen wahrhafte Perlen von IT Assets, die als werthaltige Bestandteile hochgehalten werden könnten. Beispiele hiervon sind ein hochkompetentes IT-Entwicklungsteam oder eine ausgereifte Produktionsplanungslösung im Zielunternehmen. Solche IT Assets gilt es zu identifizieren und vor möglichen politischen Grabenkämpfen zu schützen. Der Wert der Gesellschaft ist direkt davon abhängig.

Die Risiken dagegen können in die folgenden drei Dimensionen unterteilt werden:

Operative Risiken
Operative Risiken resultieren bei Eintritt in negativen Implikationen auf die wirtschaftliche und zuverlässige Durchführung der Geschäftsprozesse des Zielunternehmens.

Monetäre Risiken
Monetäre Risiken entsprechen möglichen, unvorgesehenen (Re-)Investitionen aufgrund von Ersatzbedarf oder externen finanziellen Forderungen an das Zielunternehmen.

Abhängigkeits Risiken
Abhängigkeiten zu Mitarbeitern, Lieferanten oder anderen Parteien, die in Beziehung zum Zielunternehmen stehen, können die Handlungsfähigkeit des strategischen Managements einschränken. Manche dieser Abhängigkeiten sind als Risiko einzustufen. Nicht selten ist die Weiterführung von Kernsystemen von einzelnen Personen abhängig.

Diese Risikoklassen sind dabei in verschiedenen Themengebieten der IT angesiedelt und können alleine mit einer oberflächlichen Aussensicht auf das Zielunternehmen nicht erkannt werden. Auch Schlüsselpersonen wie CIO's oder andere Knowhow-Träger erkennen nur einen Teil der

Risiken, denn die bekannten „Baustellen" überdecken die anderen Risiken. Auch verlangt die M&A Ausgangslage nach einer differenzierteren Bewertung als dies die rein operative Perspektive erfordert.

AUSSENSICHT VS REALITÄT AN DER BASIS

Die initiale Aussensicht vor der IT Due Diligence kann als direkter Gegenpol betrachtet werden zur Realität an der Basis (Abbildung 1).

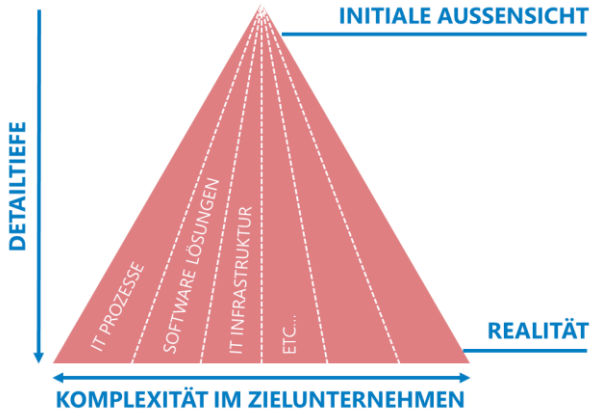

Abbildung 1: Komplexitäts-Pyramide

Zeitliche Restriktionen und verfügbares Budget gilt es dabei mit der der Detailtiefe pro Themengebiet in Einklang zu bringen. Die Herausforderung besteht darin, die Risiken und Chancen treffsicher und unter Zeitdruck zu identifizieren, finanzielle Schätzungen zu tätigen und dem Auftraggeber die Handlungsoptionen je nach Unternehmenskontext darzulegen. Darunter befinden sich auch mögliche Integrationsszenarien.

Die folgenden Abschnitte beschreiben die Schlüsselfaktoren um diesen Herausforderungen erfolgreich zu begegnen.

EIN KOMPETENTES TEAM

Der erste Schlüsselfaktor ist das Zusammenstellen eines möglichst kleinen aber kompetenten Teams, in welchem alle fachlichen und methodischen Fähigkeiten vorhanden sind. Die fachlichen Fähigkeiten variieren dabei je nach konkreter Situation. Es sollte beispielsweise nebst dem IT Wissen (Infrastruktur, Sicherheit, Entwicklung, Architektur, etc.) auch Wissen in den Bereichen Geschäftsprozesse und Unternehmensstrategie vertreten sein. Das Team hat zu Beginn die Aufgabe, die relevanten Informanten im Zielunternehmen zu ermitteln. Danach führt das Team eine ausgewogene Informationsbeschaffung durch.

INFORMATIONSBESCHAFFUNG

Der zweite Schlüsselfaktor ist eine ausgewogene und bereichsübergreifende Informationsbeschaffung im Zielunternehmen. Diese Informationsbeschaffung sollte unvoreingenommen stattfinden und darf nicht durch bestehendes Wissen frühzeitig eingeschränkt werden. Wird dagegen das Spektrum zu früh eingeschränkt, können wichtige Chancen und Risiken übersehen werden. Die Detailtiefe wird in dieser Phase bewusst klein gehalten.

Das Mittel für die Informationsbeschaffung sind Interviews mit den relevanten Informanten im Zielunternehmen. Software-gestützte Tools helfen dabei, in den Interviews alle relevanten Punkte abzudecken und aus den Antworten die Risiken zu kalkulieren (Abbildung 2). Die psychologische Ebene ist bei den Interviews nicht zu unterschätzen, können doch wichtige Sachverhalte und Zusammenhänge „zwischen den Zeilen" erkannt werden.

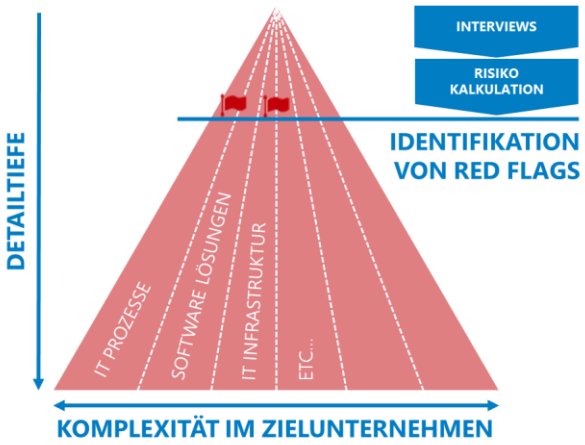

Abbildung 2: Interviews und Risiko-Kalkulation

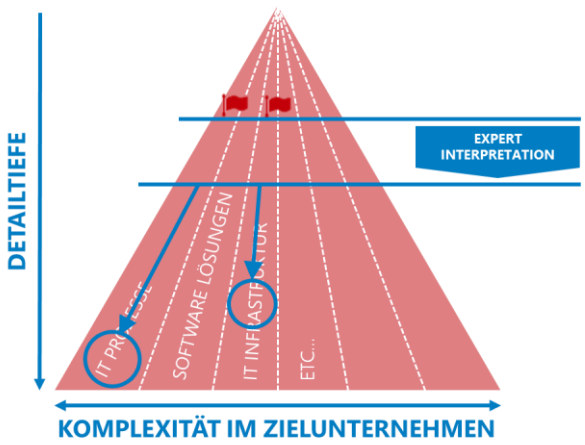

Abbildung 3: Gezielte Analysen

Themengebiete mit einer Häufung von Risiken sollen als „Red Flag" herausgehoben werden, da hier eine Untersuchung mit einer höheren Detailtiefe angemessen ist.

Fallstricke:
In der Praxis sind selbstgestrickte oder eingekaufte Checklisten für die Interviews anzutreffen. Viele dieser Checklisten sind eher einseitig gestaltet und decken Beispielsweise nur die IT Infrastruktur und Sicherheit ordentlich ab, nicht aber andere Themengebiete wie Software Entwicklung oder Unternehmensanwendungen wie beispielsweise ERP Systeme wie SAP.

GEZIELTE ANALYSEN

Der dritte Schlüsselfaktor umfasst gezielte Analysen an den richtigen Stellen mit der richtigen Detailtiefe (Abbildung 3). Diese Aufgabe obliegt den Experten im Team, welche auf Basis der Informationsbeschaffung nun die richtigen Schlüsse ziehen müssen und die Ressourcen passend auf die auffälligen Stellen im Ziel-unternehmen lenken sollen.

Die gesammelten Erkenntnisse müssen durch die Experten im Team mit konkreten finanziellen Einschätzungen und Handlungsoptionen versehen werden. Eine abgestimmte Auswahl von möglichen Integrationsszenarien darf an dieser Stelle nicht fehlen.

Fallstricke:
In der Praxis werden gerne mal dort tiefergehende Analysen gemacht, wo auch inhouse-Kompetenzen vorhanden sind. Dieser Ansatz kann hohe Folgekosten nach sich ziehen. Beispielweise werden so E-Mail Systeme untersucht, obwohl die Risiken eindeutig bei einer Reihe von ganz anderen Applikationen mit hohem Investitionsbedarf gelegen hätten.

PASSENDE AUFBEREITUNG

Der vierte Schlüsselfaktor besteht darin, die Erkenntnisse und Handlungsoptionen dem Auftraggeber der IT Due Diligence in passender Form zu übergeben. Der Auftraggeber muss seine Entscheidungen auf Basis von soliden Entscheidungsgrundlagen treffen und ist daher auf eine passgenaue und verständliche Aufbereitung in den jeweiligen Kontext angewiesen.

FAZIT

Die IT ist einer der häufigsten Ursachen für schwer abschätzbare Kosten nach der Akquisition. Die folgenden Schlüsselfaktoren sind massgeblich, um mit einer IT Due Diligence die kaufpreisrelevanten Chancen und Risiken rechtzeitig zu erkennen:

- Ein kompetentes Team, möglichst klein und dennoch mit allen fachlichen und methodischen Fähigkeiten ausgestattet
- Eine ausgewogene, bereichsübergreifende Informationsbeschaffung mit geringer Detailtiefe, um die Gesamtsicht sicherzustellen
- Gezielte Analysen an den richtigen Stellen und in der richtigen Detailtiefe inkl. möglicher Szenarien
- Passende Aufbereitung von Erkenntnissen und Handlungsoptionen als solide Entscheidungs-grundlage für den Auftraggeber der IT Due Diligence

DIE REDFLAG ANALYSIS™ METHODE

IT Due Diligence nach der REDFLAG ANALYSIS™ Methode minimiert das Risiko in M&A Transaktionen. PROCOMM hat diese Methode aus langjähriger Praxiserfahrung abgeleitet und mittels eines eigens dafür entwickelten Software Tools perfektioniert. Dieses steuert den gesamten Prozess des Due Diligence Assessments und führt die Kalkulation der Risiken automatisiert durch. Der PROCOMM Experte ist damit in der Lage, ein IT Due Diligence Assessment in kürzester Zeit durchzuführen. Die konkreten Erkenntnisse und Handlungsempfehlungen zur Risikominimierung und Erschliessung von Potenzialfeldern werden in einer für den Auftraggeber klaren und verständlichen Sprache dargestellt. Dank der REDFLAG ANALYSIS™ Methode ist das Management in der Lage, die weitere Entwicklung des Unternehmens zielsicher nach eigenen Prioritäten zu lenken.

KONTAKT

PROCOMM IT Concepts AG
Zürichstrasse 38
8306 Brüttisellen, Schweiz

Web www.redflag-analysis.com
Email info@procomm-it.com
Tel +41 44 820 77 77

Autoren: Adrian Henke, Stefan Boller

[1] H. Sarrazin und A. West, «Understanding the strategic value of IT in M&A» *McKinsey Quarterly,* Bd. January 2011, p. 3, 2016.