Praxistipps IT

IT Due Diligence

Risiken und Synergien richtig bewerten und darstellen

Jonas Tritschler / Nertila Mucka

IDW VERLAG GMBH

1 Einführung in die IT Due Diligence

In Zeiten der digitalen Transformation genießt die Informationstechnologie in Unternehmen einen steigenden Stellenwert. Die Vernetzung von Geschäftspartnern über die gesamte Wertschöpfungskette, die Automatisierung und Autonomisierung großer Teile eines Produktionsbetriebs, schnelle Informationsflüsse und aussagekräftige Daten zur Entscheidungsfindung (dank Big Data, Cloud-Systemen und prädiktiver Algorithmen) sowie der Ausbau von lernenden Systemen (Künstliche Intelligenz) und sensorbasierten Mensch-Maschine-Schnittstellen ermöglichen den industriellen Quantensprung, den wir mit dem Buzzword „Industrie 4.0" belegen.

Im Transaktionsgeschäft (Kauf- und Verkauf von Unternehmen) bedeutet die beschriebene Entwicklung, dass der Blick vielmehr auf ein zukunftsgerichtetes Geschäftsmodell als auf historische Finanz- und Marktzahlen zu fokussieren ist. Um in diesem Zusammenhang „Red Flags" oder gar „Deal Breaker" zu identifizieren, ist bei einer Due Diligence im Rahmen einer Transaktionsvorbereitung verstärkt auf Prozesse, Systeme und Technologien einzugehen. Die Durchführung einer IT Due Diligence wird vor Abschluss eines Unternehmenskaufs somit unverzichtbar.

Wir beginnen dieses Buch zunächst mit einer Einordnung der IT Due Diligence in den Gesamtkontext der Durchführung einer Due Diligence, bevor wir das Vorgehensmodell einer IT Due Diligence beschreiben und einzelne Komponenten bis zur Berichterstattung beispielhaft erörtern.

1.1 Due Diligence im Rahmen einer Transaktion

Eine „Due Diligence" bezeichnet die sorgfältige Prüfung und Analyse eines Unternehmens im Rahmen einer Transaktionsvorbereitung.[1] Gegenstand einer solchen Prüfung ist regelmäßig die wirtschaftliche, finanzielle, rechtliche und steuerliche Situation des „Target-Unternehmens". Im Regelfall wird eine Due Diligence vom Käufer durchgeführt

[1] Vgl. https://wirtschaftslexikon.gabler.de/definition/due-diligence-35668 (zuletzt abgerufen am 30.03.2020).

(Buyer Due Diligence), kann aber auch vom Verkäufer veranlasst werden (Vendor Due Diligence).

Der gesamte Prozess einer Unternehmenstransaktion aus Sicht eines Käufers beginnt zunächst mit der Findung eines „Targets", sprich eines zu akquirierenden Unternehmens, welches dem Bedarf des Käufers am nächsten kommt. Aus Käufersicht findet der Ablauf üblicherweise in sechs Phasen statt (Abb. 1.1):[2]

1. Identifizierung eines „**Targets**" inkl. der Kontaktaufnahme,
2. **Absichtserklärung** des Käufers (Letter of Intent),
3. Durchführung der **Due Diligence,**
4. **Verhandlungen** über den Kaufgegenstand,
5. **Signing** – Kaufvertrag (Sales and Purchase Agreement) wird unterschrieben,
6. **Closing** – Kaufvertrag wird vollzogen/Abschluss.

Abb. 1.1 Phasen einer M&A-Transaktion

Nachdem das „Target" gefunden, der Kontakt aufgenommen und ein gegenseitiges Interesse der Parteien an der Transaktion signalisiert wurde, wird in aller Regel eine Absichtserklärung (Letter of Intent) unterschrieben. In dieser Absichtserklärung werden üblicherweise in Klauseln die Geheimhaltung (Non-Disclosure-Agreement) und die Kostenfrage der Vertragsanbahnung geregelt.

Mit diesen Klauseln ist der Letter of Intent (LOI) somit eine notwendige Vorbedingung, damit eine Due Diligence durchgeführt werden kann.

Die Due Diligence wird regelmäßig vor den eigentlichen Verhandlungen durchgeführt. Erkenntnisse aus der Due Diligence bilden die Verhandlungsbasis zur Abgrenzung des Kaufgegenstands und der Kaufpreisfindung sowie der Vereinbarung von Garantien und Gewährleis-

[2] Vgl. Dr. Christine Gömöry (2015), Grundwissen zum Ablauf von M&A-Transaktionen, Zeitschrift für das Juristische Studium; http://www.zjs-online.com/dat/artikel/2015_2_891.pdf (zuletzt abgerufen am 30.03.2020).

tungen. Vereinfacht gesagt, sind identifizierte Risiken („Red Flags“) wie aufgedeckte Mängel bei einem Gebrauchtwagenkauf zu sehen. Jeder „Kratzer“ kann den Kaufpreis beeinflussen.

Regelmäßig werden wesentliche betriebliche Funktionen von Spezialisten im Rahmen von Audits durchleuchtet. Typisch ist deshalb die Durchführung einer Due Diligence in Teilprojekten in folgenden Ausprägungen (Abb. 1.2):

- Financial Due Diligence (FDD): Bei der FDD wird ähnlich wie bei einer Jahresabschlussprüfung die Vermögens-, Finanz- und Ertragslage analysiert. Darüber hinaus werden schwerpunktmäßig Erkenntnisse aus dem internen Rechnungswesen gewonnen, um Kennzahlen, wie das „bereinigte EBIT“ oder das „bereinigte EBITDA“, zu bestimmen oder zu verifizieren. Diese gelten als Grundlage der „Multiples“ für eine vereinfachte Unternehmensbewertung gemäß der Multiplikatormethode.[3]
- Commercial Due Diligence (CDD): Bei der CDD wird darauf abgezielt, den Markt und das Geschäftsmodell zu verstehen und zu analysieren. Bei der CDD wird analysiert, wie das Unternehmen am Markt positioniert ist und wie schlüssig das Geschäftsmodell ist.
- Legal Due Diligence (LDD): Im Rahmen einer LDD wird eine umfassende Bestandsaufnahme sowohl der externen als auch der internen Rechtsverhältnisse eines Unternehmens erstellt. Sehr oft wird die LDD durch eine Compliance Due Diligence ergänzt, in welcher allgemeine Compliance-Risiken erhoben und beurteilt werden.
- Tax Due Diligence (TDD): Ziel einer TDD ist es, steuerliche Chancen und Risiken zu analysieren sowie Erkenntnisse zu gewinnen, die die Herleitung einer optimalen steuerrechtlichen Transaktionsstruktur ermöglichen.
- IT Due Diligence (ITDD): eine ITDD zielt darauf ab, alle relevanten technologischen Aspekte im Zusammenhang mit einer Transaktionsentscheidung bezüglich der relevanten IT Chancen und IT Risiken zu analysieren und zu bewerten.

Nach Abschluss der Verhandlungen wird der Kaufvertrag („Sales and Purchase Agreement“) unterschrieben. Dieser fällt in Abhängigkeit, ob

[3] Vgl. https://de.wikipedia.org/wiki/Multiplikatormethode (zuletzt abgerufen am 30.03.2020).

es sich beim Kauf/Verkauf um einen „Share Deal“ oder „Asset Deal“ handelt, unterschiedlich umfangreich aus. Bei einem „Share Deal“ wird das Unternehmen als Ganzes, also in seinem „Rechtskleid“ (z. B. GmbH) und allen dazugehörigen Vermögensgegenstände und Schulden, ge- bzw. verkauft. Der Kaufvertrag hierzu kann entsprechend kurz ausfallen. Bei einem Asset Deal hingegen werden im Rahmen der Einzelrechtsnachfolge einzelne Vermögensgegenstände und Schulden erworben. Die Auflistung und Abgrenzung dieser Vermögensgegenstände und Schulden zu nicht übergehenden Vermögensgegenständen und Schulden sowie Haftungsvereinbarungen für diese Vermögensgegenstände und Schulden können sehr umfangreich ausfallen.

Nach erfolgreichem „Signing“ des Kaufvertrags werden mit dem „Closing“ der Transaktion die Verpflichtungen der Parteien aus dem Kaufvertrag erfüllt, d. h., der Kaufpreis wird gezahlt und dingliche Rechte werden eingetragen.

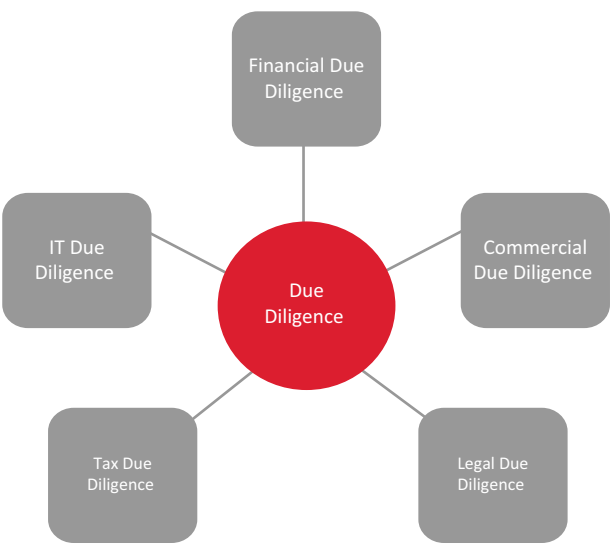

Abb. 1.2 Due-Diligence-Formen

3 Durchführung der IT Due Diligence

Nachdem wir nun die Vorgehensweise zur Durchführung einer IT Due Diligence kennengelernt haben (Kapitel 2), kommen wir zu den eigentlichen Inhalten einer IT Due Diligence. Die Beurteilung der IT-Funktion ist von vielen Faktoren abhängig. So sind einerseits branchen- und größenabhängige als auch unternehmensspezifische Faktoren zu nennen. In einigen Branchen ist die Ausgestaltung der IT-Funktion an feste „Standards" (MA-Risk, BAIT, TISAX, ISO27k, ...) gebunden. Aber auch das eigentliche Geschäftsmodell und die Reife des Unternehmens an sich sind von großer Bedeutung für die Beurteilung der IT-Funktion. Handelt es sich um ein Start-up oder um ein traditionelles Familienunternehmen in der vierten Generation, hat dies Auswirkungen auf die Ausgestaltung der IT-Funktion. Es mag zwar recht leicht sein, das Vorgehensmodell gemäß Kapitel 2 anzuwenden, die inhaltliche Beurteilung der IT-Funktion bedarf jedoch einer langjährigen Erfahrung des Beurteilers. Die in diesem Kapitel diskutierten Themen können nur als Grundgerüst gesehen werden. Risiken und Synergien werden nur beispielhaft skizziert und es bedarf immer eine Betrachtung des Einzelfalls. Das Werk an sich gibt lediglich Auszüge aus dem Erfahrungshorizont der Autoren wieder.

3.1 IT-Strategie

3.1.1 Mission-Vision-Values

Im besten Fall existiert eine dokumentierte IT-Strategie, die an der Unternehmensstrategie ausgerichtet ist. Idealerweise leitet sich die IT-Strategie aus den Mission-Vision-Values-Statements (MVV) des Unternehmens ab (Abb. 3.1). Die Strategie ergibt sich aus dem eigentlichen Auftrag der IT (Mission), dem Leitbild (Values) und der Zielvorstellung (Vision). Den Weg zum Ziel unter Berücksichtigung des Auftrags stellt die Strategie dar.

IT-Mission

Eine IT-Mission ist eine Beschreibung des Zwecks der IT-Funktion im Unternehmen, also dem Grund, warum es die IT-Funktion überhaupt gibt. Die Mission ist kurz gesagt der eigentliche Gesamtauftrag, den die IT im Unternehmen hat.

IT-Vision

Eine Vision ist die motivierende, positiv-formulierte Vorstellung des Zustandes, der erreicht werden soll. Mit einer Vision wird eine Richtung angegeben. Eine IT-Vision könnte z. B. ein vollkommen automatisierte und autonome Systemlandschaft, selbstwartende Schnittstellen und eine 100 %-ige Zufriedenheit der Anwender sein.

IT Values

Die „Values" beschreiben ethische Werte, an denen sich die IT-Organisation ausrichten soll. Die Werte sind z. B. Integrität, Verlässlichkeit, Verantwortlichkeit, Zusammenarbeit etc. Aus den Werten wird ein Verhaltenskodex, der als Leitbild für alle Mitarbeiter dient, gewonnen.

Abb. 3.1 Mission-Vision-Values-Statement als Basis für die Festlegung einer Strategie

3.1.2 Ableitung der IT-Strategie aus MVV

Ist die vorangestellte Übung (Kapitel 3.1.1) abgeschlossen und sind Mission, Vision und Values definiert, kann eine passende IT-Strategie abgeleitet werden.

3.9.3 Tabellarische Zusammenfassung: Risiken und Synergien

Die angeführte Tabelle gibt exemplarisch typisierte Risiken und Synergien wieder:

Nr.	Element IT-Organisation	Risiken	Synergien
1	IT-Dienstleister	Risiken ergeben sich aus der Abhängigkeit zum Dienstleister und dessen Zuverlässigkeit. Mangelnde vertragliche Ausgestaltungen (fehlende Service-Level-Agreements) können zu Unzufriedenheit beider Parteien führen.	Chancen ergeben sich bei der Bündelung von Dienstleistungen im Rahmen eines Unternehmenszusammenschlusses. Auch könnten einzelne Dienstleistungen von einer gruppeninternen Organisation übernommen werden (konzernweites Insourcing).
2	IT Outsourcing	Risiken ergeben sich aus der Abhängigkeit zum Dienstleister und dessen Zuverlässigkeit. Mangelnde vertragliche Ausgestaltungen (fehlende Service-Level-Agreements) können zu Unzufriedenheit beider Parteien führen. Insbesondere bei Outsourcing-Verhältnissen, bei denen große Teile der Rechnungslegung betroffen sind, sind auch Fehlerrisiken, bezogen auf den Jahresabschluss, gegeben. Auch besteht das Risiko, dass gegen datenschutzrechtliche Vorschriften verstoßen wird.	Möglicherweise können einige Dienstleistungen nach Abschluss des Deals anstelle von externen Dienstleistern von einer zentralen IT-Organisation (bei Integration in eine Unternehmensgruppe) abgebildet werden (Insourcing).

Tab. 3.16 IT-Dienstleister und Outsourcing: Risiken und Synergien

3.10 IT Compliance

IT Compliance beschreibt die Einhaltung der gesetzlichen, unternehmensinternen und vertraglichen Regelungen bzgl. der IT-Funktion in einem Unternehmen. In den letzten Jahren ist das Thema IT Compliance verstärkt in den Vordergrund gerückt. Einerseits sicherlich aufgrund der EU-Datenschutzgrundverordnung, die seit dem 25.05.2018 verbindlich für alle Unternehmen in der Europäischen Union anzuwenden ist, an-

dererseits aber auch aufgrund der Thematisierung von Cybersecurity und der Adressierung dieses Themas durch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Mit dem IT-Sicherheitsgesetz vom 17.07.2015 hat sich die Anwendung des BSI-Gesetzes von rein öffentlichen Stellen auf kritische Infrastrukturen privater Betreiber diverser Branchen (KRITIS) ausgeweitet. Auch verpflichten sich seither Unternehmen untereinander auf Einhaltung bestimmter IT-Sicherheitsstandards (ISO27001, TISAX, BSI-Grundschutz, BSI-C5 oder VdS 10000).

3.10.1 Allgemeine IT Compliance

Zu den allgemeinen Compliance-Anforderungen in der IT gehören hauptsächlich Informationssicherheit, Verfügbarkeit, Datenaufbewahrung und Datenschutz.[37] Diese Anforderungen betrifft jedes Unternehmen.

Die allgemeinen Anforderungen leiten sich aus dem Handels- und Steuerrecht sowie aus den datenschutzrechtlichen Vorschriften ab.

1. Ordnungsmäßigkeits- und Sicherheitsvorschriften gemäß Handels- und Steuerrecht nach §§ 238, 239 und 257 HGB sowie §§ 145 bis 147 AO sowie dem BMF-Schreiben (Bundesminister der Finanzen) „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)“ vom 28.11.2019
2. EU-Datenschutzgrundverordnung (EU-DSGVO)
3. Bundesdatenschutzgesetz (BDSG)
4. Sonstige IT-relevante Gesetze (TMG, TKG …).

Bezüglich des ersten Punktes kann erfragt werden, ob im Rahmen der Jahresabschlussprüfung nach § 317 HGB auch eine IT-Prüfung nach IDW PS 330 durchgeführt wurde. Idealerweise gibt es hierüber einen Prüfungsbericht oder eine Zusammenfassung des Abschlussprüfers, die eingesehen werden kann. Darüber hinaus ist der Prüfungsbericht einzufordern. Sind gravierende Mängel zur Ordnungsmäßigkeit und Sicherheit gegeben, sind diese im Prüfungsbericht unter Feststellungen zur Ordnungsmäßigkeit zur Buchführung beschrieben.

[37] Vgl. https://de.wikipedia.org/wiki/IT-Compliance (zuletzt abgerufen am 30.04.2020).

4 Gesamtbetrachtung und Berichterstattung

In der Gesamtbetrachtung sind nun alle Erkenntnisse aus den erhaltenen Unterlagen und den geführten Gesprächen in den zehn Bereichen IT-Strategie, IT-Kosten, IT-Organisation, IT Policies, Procedures und -Prozesse, IT-Infrastruktur, IT Hardware, Software, IT-Projekte, IT-Dienstleister und Outsourcing und IT Compliance im Hinblick auf das Vorhaben des Käufers zu beurteilen. Idealerweise werden alle identifizierten Risiken und Synergien/Chancen tabellarisch zusammengeführt und wenn möglich monetär bewertet (4.1). Im Anschluss kann von einem geschätzten Kaufpreis die untere und eine obere Grenze auf Basis der Erkenntnisse aus der IT Due Diligence ermittelt werden.

4.1 Zusammenfassung von Risiken und Synergien/Chancen

Nachfolgend werden einzelne Risiken und Synergien/Chancen exemplarisch dargestellt und beispielhaft bewertet. Diese Übung dient dazu, die eigene Position in einer Kaufpreisverhandlung zu stärken, in dem zur Vorbereitung auf die Gespräche eine Obergrenze für den Kaufpreis ermittelt wird. Eine Zusammenfassung aller Risiken liefert Argumente für eine Anpassung des Kaufpreises nach unten. Die monetäre Auswirkung kann einmaliger oder wiederkehrender Natur sein. Wiederkehrende Sachverhalte (z. B. wiederkehrende Einsparungen) sind in der Tabelle dadurch gekennzeichnet, dass sie ein p.a. (per anno) tragen.

Nr.	Element	Risiken	Synergien/ Chancen	Monetäre Auswirkung
1	IT-Strategie	Nicht definiert	Nicht definiert	Keine
2	IT-Kosten		Kosteneinsparung in Lizenzkosten aufgrund größerer Stückzahlen	T€ +50 p.a.
3	IT-Organisation	Schlüsselpersonen könnten das Unternehmen verlassen	Einsparung in IT-Personalkosten von zwei Mitarbeitern	T€ +150 p.a.
4	IT Policies & Procedures und Prozesse	Keine ausreichende Dokumentation, Notfallplan fehlt		T€ –30

Nr.	Element	Risiken	Synergien/ Chancen	Monetäre Auswirkung
5	IT-Infrastruktur	Unternehmensweite Verkabelung auf CAT5, Umstellung auf CAT6		T€ –20
6	IT-Hardware	Veraltete Hardware, Storage-Systeme an der Kapazitätsgrenze		T€ –300
7	Software und Schnittstellen		ERP-System kann in Käufersystem migriert werden	T€ –250 T€ 100 p.a.
8	IT-Projekte	Projekt DSGVO nicht ausreichend budgetiert		T€ –150
9	IT-Dienstleister u. Outsourcing	Kein monatliches Berichtswesen		Keine
10	IT Compliance	Zertifizierung nach TISAX ausstehend		T€ 40 T€ –15

Tab. 4.1 Beispielhafte Zusammenfassung aller Risiken und Synergien/Chancen

4.2 Einfluss von Risiken und Synergien auf den Kaufpreis

Bei einem geschätzten Kaufpreis, der üblicherweise aus einem Vielfachen („Multiple“) einer Gewinngröße abgeleitet wird, können die Erkenntnisse aus der IT Due Diligence als Anpassungen dienen.

Nehmen wir an, dass sich die Kaufbereitschaft auf einen Multiple-Ansatz[43] stützt und dieser sich auf € 10 Mio. beläuft (EBIT von € 1 Mio. und Multiple von 10), so ergibt sich auf Basis der Erkenntnisse eine Kaufpreisspanne, in der der Käufer bereit wäre, den Kaufgegenstand zu erwerben. Die Untergrenze ermittelt sich aus den bewerteten Risiken der IT-Funktion und die Obergrenze aus der Summe der Synergien. Bei einem „Multiple“ von 10 ergibt sich auf Basis der Tabelle 4.1 das folgende Bild (Tabelle 4.2 und Tabelle 4.3):

[43] Siehe Kapitel 1.1.