

M&A REVIEW

MERGERS & ACQUISITIONS • Beteiligungen • Allianzen • Restrukturierungen • Divestments • Private Equity

www.ma-review.de

Publikationsorgan **BUNDESVERBAND
MERGERS &
ACQUISITIONS E.V.**

27. Jahrgang 7-8/2016

Standpunkt

„Alles wirkliche Leben ist
Begegnung“

Industry Special

Ein Blick auf die europäische Inter-
netindustrie: Weniger Deals – aber
größere Transaktionsvolumina

Industry Special

M&A-Transaktionen in der
Cleantech-Branche: Südostasien
2015 im Fokus

Austria Column

Was Unternehmen zu Wiederho-
lungstätern macht – österreichische
M&A-Stars im Fokus

Recht und Steuern

Steuerliche Berichtigungspflichten
im Nachgang einer Tax Due
Diligence

Deal des Monats

Zalando weiter auf Einkaufstour



Strategien und Visionen

**IT Due Diligence:
Schnell, ausführlich –
oder gar nicht?**

GoingPublicMedia

AKTIENGESELLSCHAFT

IT Due Diligence: Schnell, ausführlich – oder gar nicht?

Adrian Henke, PROCOMM IT Concepts AG, Brüttisellen

1. Einleitung

► In den letzten Jahren haben sich Fokus und Einsatzgebiet der IT Due Diligence deutlich verändert, insbesondere durch die fortschreitende Digitalisierung der Wirtschaft. Nebst der herkömmlichen Prüfung der IT liegen heute die Akzente auf den darauf abgebildeten Geschäftsprozessen entlang der Wertschöpfungskette des Unternehmens. Die IT-Systeme, welche diese Prozesse abbilden, sind ausschlaggebend für die Prozesseffizienz und somit für den Wert und das Potenzial des Unternehmens. Erfahren Sie in diesem Artikel, wie Sie ein Unternehmen entsprechend der Wichtigkeit der IT prüfen können. Eine methodisch und fachlich gut abgestützte IT Due Diligence schließt diese Lücke.

1.1 Was ist IT Due Diligence?

Bei der IT Due Diligence werden Werthaltigkeit, Zukunftssicherheit und Entwicklungsmöglichkeiten eines Unternehmens hinsichtlich dessen IT beurteilt. Die IT-Organisation, IT-Systeme sowie die darauf abgebildeten Geschäftsprozesse sind Teil der Untersuchung.

Während der Transaktion schafft die IT Due Diligence für den Investor Klarheit über Potenziale und Risiken in der IT und deckt kaufpreisrelevante Faktoren auf. Bei einem Post-Merger-Integrationsprojekt wurden zwei neue, redundante Rechenzentren mit einem Aufwand von rund 4 Mio. EUR aufgebaut. Erst bei der Inbetriebnahme stellte man fest, dass eine für die gesamte Einheit tragfähige IT-Infrastruktur in einem der akquirierten Unternehmen bereits vorhanden war.

In einem anderen Beispiel wurde ein Clearing Center im Bereich Medizintechnik anhand der immensen Datenbank aller Player im Markt sowie deren Materialbezüge über die vergangenen Jahre entspre-

chend hoch bewertet. Bei der späteren, operativen Übernahme wurde festgestellt, dass praktisch die gesamten Inhalte gravierende Mängel aufwiesen und Datenbereinigungsaktivitäten von mehr als 1 Mio. EUR aufgewendet werden mussten. Die vorgesehenen Garantien in den Kaufverträgen waren in diesem Fall nicht durchsetzbar.

Die Erkenntnisse aus diesen Prüfungen sind jedoch nicht nur für die Dauer der Transaktion relevant, sondern ebenso für die weitere Entwicklung des Unternehmens. Dem Finanzinvestor zeigt die IT Due Diligence mögliche Wege für Wertsteigerungen durch Maßnahmen in der IT. Dem strategischen Investor zeigt sie Synergie- und Effizienzpotenziale wie auch Integrationsszenarien im Falle einer Post-Merger-Integration. Nebst der Anwendung der IT Due Diligence im Rahmen einer Akquisition kann dieselbe Methode auch als internes Audit durchgeführt werden. Abbildung 1 zeigt den Einsatzzweck der IT Due Diligence in Bezug zu den Akteuren in der jeweiligen Phase.

Zu den anderen Aspekten der Due Diligence gibt es durchaus Berührungspunkte oder sogar Überschneidungen. Die IT Due Diligence unterstützt die Erschließung von operativen Wertsteigerungen, ebenso wie dies beispielsweise auch mit einer Operational Due Diligence beabsichtigt wird. Des Weiteren können sich die Themen Personal, Verträge, Lizenzierung und Compliance mit anderen Due-Diligence-Aktivitäten aus den Bereichen Finanzen, Recht und HR teilweise überschneiden, da die IT-Systeme und die IT-Organisation diese Prozesse in der Regel auch mit abdecken. Bei der IT Due Diligence wird diese Abdeckung mit untersucht. Ein Beispiel ist der Austrittsprozess im HR, der aus Sicherheitsgründen zwingend auch durch die IT-Organisation begleitet werden muss. Durch ein gezieltes Scoping werden Doppelspurigkeiten bei den Prüfungen vermieden.

Abb. 1 • Akteure und Einsatzzweck der IT Due Diligence

Quelle: Eigene Darstellung

Akteur	Phase	Einsatzzweck der IT Due Diligence
Finanzinvestor	Pre-Acquisition	<ul style="list-style-type: none"> • Transparenz über die „IT-Fitness“ von Targets und Portfolio-Gesellschaften • Screening mit minimalen Broken-Deal-Kosten
	Transaktion	<ul style="list-style-type: none"> • Kaufpreisoptimierung durch Transparenz hinsichtlich IT • Risikominimierung in der IT • Aufzeigen von EBIT-wirksamen Potenzialen in der IT
	Wertsteigerung	<ul style="list-style-type: none"> • Risikominimierung in der IT • Aufzeigen von EBIT-wirksamen Potenzialen in der IT • Beitrag zur Exit-Optimierung durch IT
Strategischer Investor	Pre-Acquisition	<ul style="list-style-type: none"> • Transparenz über die „IT-Fitness“ des Targets • Screening mit minimalen Broken-Deal-Kosten
	Transaktion	<ul style="list-style-type: none"> • Kaufpreisoptimierung durch Transparenz hinsichtlich IT • Risikominimierung in der IT • Aufzeigen von Potenzialen in der IT je nach Situation
	Integration	<ul style="list-style-type: none"> • Risikominimierung in der IT • Konzeption der IT-Integrationsszenarien
	Operative Verbesserung (losgelöst von M&A, jedoch mit den gleichen Verfahren)	<ul style="list-style-type: none"> • Standortbestimmung, Aufzeigen von Risiken sowie operativen Potenzialen in der IT (IT Due Diligence als interner Audit)

1.2 Werthaltigkeit versus Effizienz

Werfen wir einen Blick zurück. Im Nachgang des Börsencrashes Ende der 1920er Jahre hat das US-Gesetz *Securities Act of 1933* das Konzept der Due Diligence erstmals in den USA gesetzlich verankert.¹ Das Gesetz

regelte unter anderem die Informationsoffenlegung beim Wertschriftenhandel und legte fest, wie sich die Broker durch eine Due-Diligence-Prüfung aus der Haftung nehmen konnten. Auch heute noch richtet sich der Fokus der Due Diligence auf die Werthaltigkeit von Anlagen und die finanziellen, rechtlichen und steuerlichen Absicherungen. Wir beobachten in der Praxis häufig, dass die IT ausschließlich aus Sicht des

¹ Vgl. Securities Act of 1933, 27. Mai 1933, Kapitel 38, Titel I, 48 Stat. 74.

Anlagenwertes in der Buchführung beurteilt wird. Bei einem europäischen Industrieunternehmen mit weitreichenden Aktivitäten im Bereich Service-Außendienst waren dieser Anlagewert und auch die Lizenzierung durchaus in Ordnung. Dass die selbstentwickelte Mobile-Lösung für die 230 Außendienst-Techniker jedoch am Ende ihres Lebenszyklus angekommen war, wurde nicht erkannt. In Bezug auf die heutige Bedeutung der IT ist der Fokus auf den Anlagewert und die Lizenzen zwar durchaus weiterhin angebracht, aber bei weitem nicht mehr ausreichend.

Die IT darf nicht nur als risikobehaftete Anlage betrachtet werden, sondern sie muss als digitalisierte Wertschöpfungskette des Unternehmens verstanden werden. Die IT-Systeme bilden die Prozesse dieser Wertschöpfungskette ab. Sie sind von maßgeblicher Relevanz für die Prozesseffizienz² und somit für den Wert des Unternehmens. Zukunftsorientierte Unternehmen optimieren diese digitale Wertschöpfungskette kontinuierlich und systematisch – man spricht hier auch von der digitalen Unternehmensentwicklung. Hierbei werden Prozesseffizienz, Auslastungsgrade der vorhandenen Ressourcen, Durchlaufzeiten sowie Gaps im Informationsfluss und andere EBIT-relevanten Einflussfaktoren gemessen. Dazu dienen betriebswirtschaftliche Verfahren zur Messung von vorhandenen Kapazitäten nach Geschäftsprozess oder Organisationseinheit. Diese Kapazitäten werden dann mit den tatsächlich durchgeführten Operationen und der daraus resultierenden Belastung verglichen. Es ergeben sich Auslastungs-Koeffizienten. Die auf diese Weise ermittelten Auslastungen identifizieren Potenzialfelder für die Automatisierung durch IT – respektive Digitalisierung. Darüber hinaus können Prozessketten auf manuelle Eingriffe untersucht werden, die durch Digitalisierung reduziert werden können. Bei einem Schweizer Bauzulieferer konnte beispielsweise die Durchlaufzeit für die Ausstellung von Kundenangeboten um 80% reduziert werden, weil nun bereits bei der Kundendatenaufnahme alle preisrelevanten Parameter in die Mobile-Applikation aufgenommen werden. Das Angebot wird somit vollautomatisch erzeugt und ausgestellt. Die gesamte Aufarbeitung im Verkaufsinendienst entfällt.

Die Ergebnisse dieser Messungen liefern die Informationsbasis für zunehmend treffsichere Entscheidungen des Managements im Sinne der Unternehmensstrategie. Um nun aus der digitalen Unternehmensentwicklung einen Erfolgsfaktor zu schaffen, ist die Komplexität der IT zu berücksichtigen. Für die Prüfung bei der IT Due Diligence sind entsprechend spezifische Methoden für die Prüfung notwendig, die deutlich über die konventionellen Ansätze hinausgehen.

2. Der Kampf gegen die Komplexität

Moderne IT Systeme sind äußerst komplex, wobei dies in der Außensicht meistens nicht vollständig wahrgenommen wird. Als praxisnahe Veranschaulichung dient an dieser Stelle ein europäisches Industrieunternehmen mit 1.200 Mitarbeitern in fünf Ländergesellschaften. Dieses Unternehmen hat im Jahr 2015 den Prozess-Schritt „Offert-Erstellung“ ungefähr 82.000 Mal durchlaufen. Dabei wurden mindestens 2,4 Mio. Einzelpreisberechnungen durchgeführt und digitale Offerten im Volumen von etwa 23 Mio. DIN-A4 Seiten erzeugt und archiviert. Während demselben Geschäftsjahr hat das Unternehmen gleichzeitig rund 69.000 Veränderungen der Berechnungsformeln rund um diese Einzelpreisberechnung vorgenommen. Diese Komplexität entlang der digitalen Wertschöpfungskette eines Unternehmens ist nichts Außergewöhnliches.

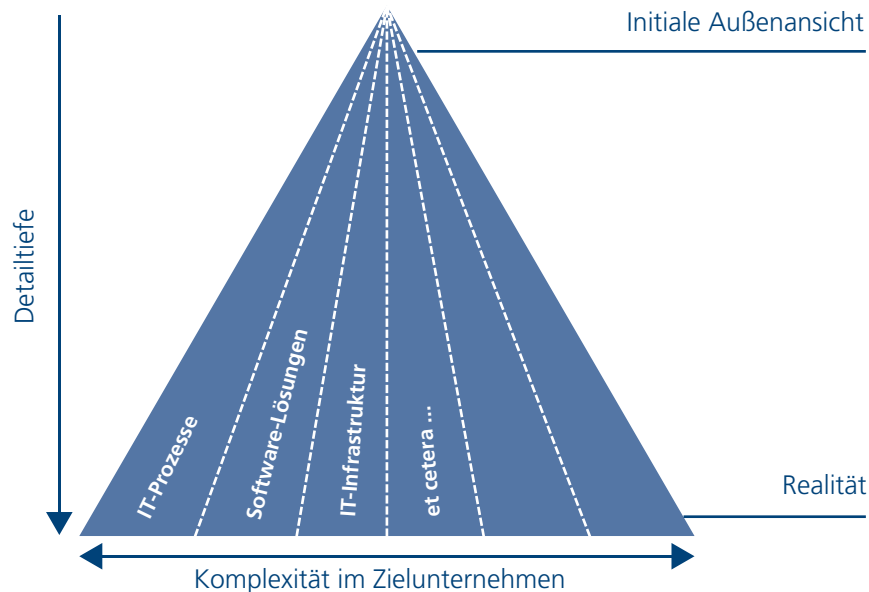
Bei der Due Diligence steht man vor dem Dilemma, dass ein äußerst komplexes Gebilde von IT-Systemen und Geschäftsprozessen möglichst detailliert und vollständig bewertet werden soll. Als Betrachtungsmodell für diese Herausforderung dient die Komplexitätspyramide (s. Abb. 2). Diese stellt die Komplexität im Zusammenhang mit der Betrachtungstiefe dar. Im oberen Bereich wirkt die Komplexität überschaubar, unten an der Basis dagegen ist sie immens. Da die tatsächlichen Kostenfolgen und auch Chancen im Zusammenhang mit der IT typischerweise an der Basis der Pyramide entstehen, kann nur eine Untersuchung auf dieser hohen Komplexitätsstufe an der Basis der Pyramide Aufschluss verleihen. Da jedoch die Zeit und Budgets bei einer Akquisition knapp sind, ist eine Untersuchung sämtlicher Details an der Basis der Pyramide undenkbar. Einerseits besteht somit der Anspruch der Untersuchung in hohem Detailierungsgrad – andererseits sind Zeit und Budget knapp bemessen. Die Pyramide dient der nachfolgenden Diskussion dieses Dilemmas.

Bei der Abspaltung des Zielunternehmens wie auch bei einer Integration im Falle eines Mergers ergibt sich eine zusätzliche Komplexität. Unter anderem müssen Datenbestände und Systeme aufgetrennt und migriert werden unter Einhaltung von Datenschutzrichtlinien und anderen rechtlichen und regulatorischen Anforderungen. Diese situativen Gegebenheiten müssen bei einer IT Due Diligence zwingend mitberücksichtigt werden. Um bei der IT Due Diligence die Ressourcen am richtigen Ort einzusetzen, sind spezialisierte und effektive Methoden, wie nachfolgend erläutert, zwingend.

² Vgl. Michael Hammer: Reengineering Work: Don't automate, obliterate. In: Harvard Business Review, Juli-August, 1990, S. 104-112.

Abb. 2 • Komplexitätspyramide

Quelle: Eigene Darstellung



2.1 Effektivitätssteigerung durch bewusste Segmentierung

Wie kann die Komplexitätspyramide bewältigt werden? Einen Teil der Lösung finden wir im Feld der Erkenntnistheorie. Die Erkenntnislogik fußt auf den drei Schlussverfahren Deduktion, Induktion und Abduktion:³

- *Deduktion* ist die Schlussfolgerung von der Regel und dem Fall auf die Konsequenz.
- *Induktion* ist die Schlussfolgerung von der Konsequenz und dem Fall auf die Regel.
- *Abduktion* ist die Schlussfolgerung von der Regel und der Konsequenz auf den Fall.


Diese drei Schlussverfahren besitzen unterschiedliche Eigenschaften. Die Deduktion beweist, dass etwas *sein muss*, während die Induktion zeigt, dass etwas *ist*. Die Abduktion hingegen legt dar, was *sein kann*, analog einer Hypothese. Das Anwendungsgebiet dieser Schlussverfahren ist in der Praxis breit abgestützt, unter anderem werden sie in der Medizin, der Justiz und der Psychologie eingesetzt. In der Medizin bedienen sich beispielsweise Computersysteme der Abduktion, indem sie anhand der Symptome des Patienten („Konsequenz“) in Kombination mit Wissensdatenbanken („Regel“) die Wahrscheinlichkeiten der konkreten Krankheitsursache („Fall“) berechnen und so den Arzt bei der Diagnose unterstützen.

Nebst der Erkenntnistheorie ist das Konzept der Verallgemeinerung von Nutzen. Informationen können grundsätzlich durch drei Wege verallgemeinert werden:⁴

- Extrapolation von der Stichprobe zur Gesamtheit
- Analytische Verallgemeinerung
- Fall-zu-Fall Übertragung

Der erste Weg, die Extrapolation, umfasst die Selektion von Stichproben und deren Verallgemeinerung zur Gesamtheit. Der zweite Weg umfasst die analytische Verallgemeinerung durch die Bildung einer erklärenden Theorie. Der dritte Weg überträgt Erkenntnisse von einem Fall auf den anderen, um zu einer neuen Erkenntnis zu gelangen.

Der IT-Due-Diligence-Experte kann sich nun der Induktion sowie auch der Extrapolation bedienen, um dem Komplexitätsdilemma entgegenzutreten. Durch seine Tätigkeit in der IT- und PMI-Welt kennt der IT-Due-Diligence-Experte eine Vielzahl von gesunden und weniger gesunden Unternehmen („Konsequenz“) sowie die konkreten Symptome dazu („Fall“). Aus diesem Expertenwissen leitet er eine Vielzahl von Kontrollpunkten ab („Regeln“) – analog der Induktion. Als Beispiele für Kontrollpunkte können folgende Fragen dienen:

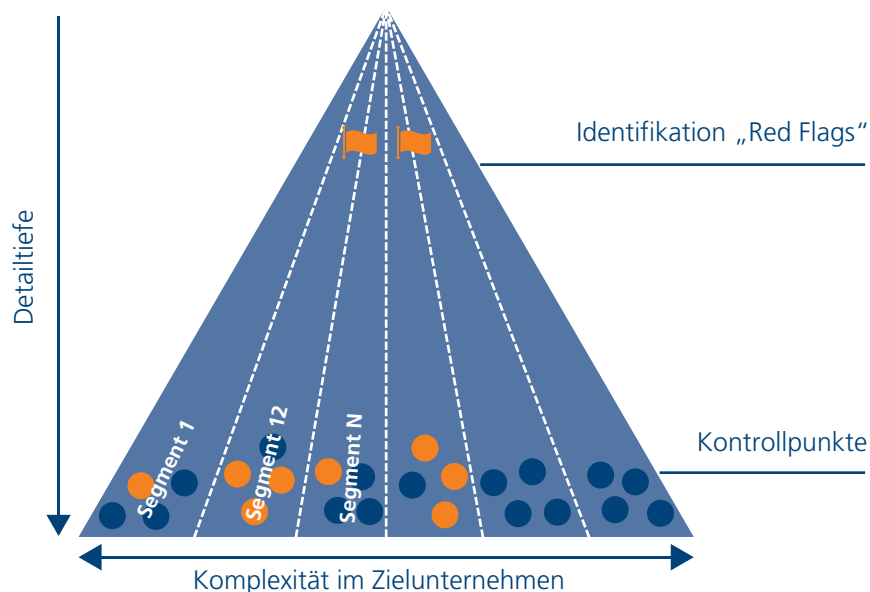
- Ist sichergestellt, dass die IT-Investitionen sich klar nach den strategisch wichtigen Business-Units und Absatzkanälen richten? 

³ Vgl. Peirce: Collected Papers, Vol. 5, 3. Aufl., S. 14-212, 1965.

⁴ Vgl. Firestone: Alternative Arguments for Generalizing from Data as Applied to Quantitative Research, Educational Researcher, Vol. 22, No. 4, 1993.

Abb. 3 • Identifikation von „Red Flags“ in einzelnen Segmenten

Quelle: Eigene Darstellung



- Sind die physischen Zugänge zu den Rechenzentren ausreichend geschützt?
- Gibt es definierte Wartungsintervalle von Sicherheitseinrichtungen?
- Werden Änderungen an ERP Systemen (beispielsweise SAP) erst nach einer Kosten-Nutzen-Analyse durch ein definiertes Gremium für die Umsetzung freigegeben? (Change-Management)

Die Kontrollpunkte sind Stichproben, die im Rahmen von Interviews oder bei der Sichtung von Dokumenten geprüft werden. Bei der Durchführung einer IT Due Diligence analysiert der Experte punktuell einzelne Kontrollpunkte in hoher Detailtiefe, um segmentweise Rückschlüsse auf das Ganze zu ziehen – analog der Extrapolation. Sind die Ergebnisse auf dieser Detailtiefe unbefriedigend, so wird das betroffene Segment für weitere Untersuchungen markiert („Red Flag“). Auf Basis dieser Kontrollpunkte kann rasch und dadurch kostengünstig ermittelt werden, welche Segmente einer weiteren Untersuchung bedürfen. Die Effektivität wird so optimiert, da ein erhöhter Aufwand nur in gezielt ausgewählten Segmenten erbracht wird. Abbildung 3 zeigt schematisch den Rückschluss von negativ ausgefallenen Kontrollpunkten (rote Punkte) auf Segmente, die weitere Untersuchungen benötigen („Red Flag“).

Ein Beispiel aus der Praxis lautet wie folgt: Im Rahmen der IT Due Diligence wird ein Red Flag im Segment „Software Lösungen“ identifiziert, da in diesem Segment 75% der Kontrollpunkte negativ ausgefallen sind. Bei der gezielten Untersuchung dieses Segments stellt sich heraus, dass die Anzahl der eingesetzten

Applikationen innert neun Monaten auf die Hälfte reduziert werden könnte. Nebst Einsparungen für Wartung und Unterhalt ergeben sich dadurch effizientere Prozesse, da die Mitarbeiter keine Mehrfacheinfassungen in verschiedenen Systemen mehr tätigen müssen.

2.2 Limitationen und Fallstricke

Die dargelegte Vorgehensweise beruht zwar auf wissenschaftlichen Ansätzen, ist jedoch mathematisch nur ein erster Versuch der Annäherung und somit nicht hieb- und stichfest. So wird das Ergebnis markant dadurch beeinflusst, wie geschickt die Kontrollpunkte gewählt und auf das zu untersuchende Unternehmen angepasst sind. Gerne werden Sicherheit, Datenschutz und IT-Infrastruktur gut durchleuchtet, organisatorische Prozesse (wie Software-Entwicklung oder Änderungen) jedoch genauso oft vernachlässigt. Um das Unternehmen weiterzuentwickeln, sind jedoch Verbesserungen der Prozesseffizienz viel wichtiger. Deshalb müssen die Kontrollpunkte breit gestreut sein und dürfen nicht durch die vorhandene Expertise sowie die berufliche Herkunft des Experten verzerrt werden. Bei einem britischen Facility-Management-Unternehmen wurden in den vergangenen Jahren mehrere hundert Anpassungen am ERP-System programmiert und auch individuelle Zusatzprogramme entwickelt. Im Rahmen einer von den Autoren durchgeführten Untersuchung wurde festgestellt, dass 70% dieser Programme und Anpassungen von den Benutzern nie verwendet wurden. Wie sich herausstellte, wurden die Änderungswünsche von den Linienvorgesetzten direkt bei der IT-Organisation bestellt, welche in der Regel auch rasch lieferte. In diesem Fall fehlte ein Change Advisory

Board, welches unter anderem die Querabhängigkeiten und Konsequenzen sowie Kosten und Nutzen von Änderungen vor der Freigabe abklärt.

Ohne umfassendes, betriebswirtschaftliches Wissen fokussiert der Experte zu sehr auf Technik und vernachlässigt die darauf abgebildeten Geschäftsprozesse und deren Ökonomie. Diese Problematik ist mitunter ein Grund, wieso in der Praxis die IT in kleinen Transaktionen unzureichend geprüft wird und ab mittleren Transaktionen mit schwerem Vertragswerk abgesichert wird.

Weitere Fallstricke sind „Problemzonen“, die im Zielunternehmen bereits als solche bekannt sind. Diese Zonen bergen die Gefahr, andere mitunter ebenso wichtige Potenziale und Risiken zu verdecken. Der IT-Due-Diligence-Experte darf deshalb nicht der Versuchung erliegen, auf diese Problemzonen zu fokussieren. Stattdessen muss er konsequent einen austarierten Wertmaßstab anlegen, um zu schlüssigen Ergebnissen zu kommen. Beispiel: Der CIO eines Dienstleistungsunternehmens in Spanien nimmt die geplante Verschiebung von Servern in die Cloud als große Herausforderung wahr. Was aus seiner operativen Sicht stimmig sein mag, ist im Kontext der Akquisition weniger zentral. Von größerer Bedeutung ist hier beispielsweise die Einführung eines belastbaren Change-Managements in der IT, um das Unternehmen bei der digitalen Transformation zu unterstützen. Diese Fallstricke lassen sich zwar nicht gänzlich vermeiden, aber bereits die Kenntnis davon kann in der einen oder anderen Situation zur richtigen Entscheidung führen.

3. Verschiedene Arten von Risiken

Die IT Due Diligence kann verschiedene Arten von Risiken aufdecken. Die in der IT anzutreffenden Risiken können grundsätzlich in operative, monetäre sowie Abhängigkeitsrisiken kategorisiert werden. Alle drei Risikoklassen beziehen sich auf das Zielunternehmen im operativen Betrieb.

3.1 Operative Risiken

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

Ein Beispiel für ein operatives Risiko sind geschäftskritische Systeme im Zielunternehmen, die nicht ausfallsicher betrieben werden. Im Falle eines Call-Centers für die Außendienst-Disposition können die Telefonisten weiterhin eingehende Anrufe beantworten, jedoch sind sie nicht mehr auskunftsfähig, da die Systeme offline sind. Im Falle des slowakischen Produktionsstand-

ortes eines Schweizer Herstellers stehen sämtliche Produktionsstraßen während zwei Schichten still, da die einzelnen Arbeitsgänge nicht mehr via Barcodes abgeschlossen werden können.

3.2 Monetäre Risiken

Monetäre Risiken entsprechen möglichen, oft ungeplanten (Re-)Investitionen aufgrund von Ersatzbedarf oder finanziellen Forderungen an das Zielunternehmen wie beispielsweise für Unterhalt oder Upgrade.

Ein Beispiel für ein monetäres Risiko ist ein End-of-Life-System im Kernprozess einer deutschen Energieversorger-Gesellschaft. Das System ist zwar ein namhaftes deutsches ERP-System, jedoch in einer älteren Version, welche durch den Hersteller in Kürze nicht mehr unterstützt werden wird. Durch diese Situation ist nun ein Versionswechsel finanziell gleichbedeutend mit einem kompletten Neubau des Systems, der 24 Monate Projektlaufzeit erfordert. Da der Lieferant den Support für die alte Version des Systems innerhalb von 18 Monaten einstellt, ist das Unternehmen zu einer Re-Investition gezwungen. Bei einer belgischen Handelsfirma wurde erst kurz vor der Expansion in die Niederlande festgestellt, dass das bestehende ERP-System nicht den internationalen Rechnungslegungsstandards entsprechen kann. Die Expansion verzögert sich administrativ um zwölf Monate, da das ERP-System vorgängig ersetzt werden muss.

3.3 Abhängigkeitsrisiken

Abhängigkeiten zu Mitarbeitern, Lieferanten oder anderen Parteien, die in Beziehung zum Zielunternehmen stehen, können die Handlungsfähigkeit des Zielunternehmens einschränken.

Ein Beispiel für ein Abhängigkeitsrisiko ist ein Mitarbeiter in der Software-Entwicklung des Zielunternehmens, der seit über zehn Jahren eine Software für eine hochspezifische Preis- und Margenberechnung entwickelt und unterhält. Ohne diese Software ist das Unternehmen nicht mehr in der Lage, Offerten zu den bestmöglichen Marktpreisen automatisiert zu erstellen. Die Software ist nicht dokumentiert und es gibt sonst niemanden, der an dieser Software jemals eine Änderung vorgenommen hat. Das Zielunternehmen ist in hohem Grade von diesem Mitarbeiter abhängig, was auch erst mehrere Jahre nach der Akquise schmerzhaft bemerkbar werden könnte.

Solche Risiken sind nicht per se als Deal-Stopper zu betrachten, sondern sie zu erkennen, im Sinne von zusätzlichen Investitionskosten einzuschätzen und zu quantifizieren. Manche dieser Risiken sind durchaus kaufpreisrelevant.



Abb. 4 • Faustregel für die empfohlenen Minimalaufwendungen

Quelle: Eigene Darstellung

Anzahl Mitarbeiter	Beratertage	Interviews	Interner Aufwand (Tage)
< 100	3	3	3–6
< 500	4	6	4–8
< 2.000	8	13	8–16
≥ 2.000	13	23	13–26

4. Empfohlene Minimalaufwendungen

Ist eine IT Due Diligence notwendig? In der heutigen digitalisierten Wirtschaft gilt nicht mehr die Frage, ob eine IT Due Diligence gemacht werden, sondern welcher Aufwand investiert werden soll. Dies wohlweisend, dass heute in der Praxis gerade bei kleineren Transaktionen die IT oft gänzlich unbeachtet bleibt. Aus der Erfahrung haben wir eine Faustregel abgeleitet, welche besagt, wieviel Aufwand für die Erstuntersuchung in der IT Due Diligence mindestens getätigt werden soll. Die Faustregel ist in der Abbildung abgebildet und gilt für eine einzelne Gesellschaft. Die Erstuntersuchung deckt die Herleitung der „Red Flag“-Segmente ab. Der Aufwand für die weitere Untersuchung eines Segments ist an dieser Stelle nicht aufgeführt, da dies enorm unterschiedlich ist und stark von den Ergebnissen der Erstuntersuchung abhängt. Wir empfehlen in jedem Fall zunächst die Erstuntersuchung, weiterführende Untersuchungen werden nur dann empfohlen, wenn dies durch die Ergebnisse der Erstuntersuchung klar induziert wird.

Die Empfehlung basiert auf der Annahme, dass modernste Softwarewerkzeuge und Verfahren durch erfahrene IT-Due-Diligence-Experten eingesetzt werden. Andere Faktoren, wie die geografische Verteilung oder Diversität der Geschäftstätigkeit, können den empfohlenen Mindestaufwand beeinflussen. Der interne Zeitaufwand im Zielunternehmen beträgt durchschnittlich 100 bis 200% des Wertes, welcher als Mindestaufwand für Beratertage angegeben wird.

5. Zusammenfassung und Ausblick

Dieser Artikel zeigt auf, wie die IT eines Unternehmens mittels IT Due Diligence geprüft wird. Wo früher die Akzente auf der Werthaltigkeit der IT lagen, rücken heute vermehrt die darauf abgebildeten Prozessketten in den Fokus. Die IT Due Diligence ist eine Standortbestimmung im Prozess der digitalen Unternehmens-

entwicklung. Die im Artikel beschriebenen Methoden der Induktion und Extrapolation bieten einen praxiserprobten Ansatz zur Bewältigung der inhärenten Komplexität in der IT.

Selbstverständlich garantiert eine ausgereifte Methode keineswegs eine aussagekräftige IT Due Diligence. Die ausgewogene Wahl der Kontrollpunkte sowie die interdisziplinären Fähigkeiten des IT-Due-Diligence-Experten sind gefordert. Fallstricke sind die Dominanz von bereits bekannten Problemzonen, einseitige Checklisten und die fehlenden strategischen und betriebswirtschaftlichen Fähigkeiten bei zu technisch orientierten IT-Due-Diligence-Beauftragten.

Für die Zukunft ist zu erwarten, dass das Thema „Digitalisierung“ verstärkt Einzug hält in die Überlegungen beim Screening, bei der Akquisition wie auch bei der Wertsteigerung eines Unternehmens. Wo befindet sich das Unternehmen unter dem Gesichtspunkt der Digitalisierung? Hat das Unternehmen das nötige IT-Fundament? Was ist der Investitionsbedarf, um die nötigen Kompetenzen und Systeme aufzubauen? Es ist absehbar, dass diese Fragen in Zukunft vermehrt mittels einer IT Due Diligence beantwortet werden. ■



Adrian Henke ist Architekt für strategische IT-Landschaften. Er erstellt Gesamtkonzepte und leitet die Umsetzung aus der Unternehmensperspektive. Mit Fokussierung auf die strategischen Ziele umfasst dies die Auswahl der Lösungen und Technologien, die Erstellung der Realisierungspläne sowie die Betreuung der Umsetzung bis hin zum operativen Betrieb. adrian.henke@procomm-it.com