VOLKER JOHANNING
STRATEGIEN FÜR DEN DIGITALEN WANDEL

Checkliste IT Due Diligence (IT DD)

Es sind insgesamt sieben Checklisten dargestellt, die Ihnen helfen die erforderlichen Unterlagen strukturiert zu beschaffen, auszuwerten und einen möglichen Reifegrad abzuleiten.

1. IT-Strategie / IT-Governance
2. IT Organisation und Personal
3. IT-Systemlandschaft und Architektur
4. IT-Infrastruktur / IT-Betrieb / IT-Security
5. IT Projekt und Portfoliomanagement
6. IT Finanzen und Compliance
7. IT-Prozesse und IT-Einkauf

Bei Fragen oder weitergehenden Informationen wenden Sie sich gerne unverbindlich an:

Volker Johanning

E-Mail: volker@johanning.de

Checkliste 1: IT-Strategie / IT-Governance

#	Untersuchungsgegenstand	Benö-tigt?	Gelie-fert?	Reife-grad	Beurteilung / Bemerkungen
1.1	Existiert eine dokumentierte IT-Strategie und enthält diese alle wesentlichen Parameter wie zum Beispiel strategische Ziele, Vision, erkennbare Ableitungen aus der Unternehmens- oder den Fachbereichsstrategien und sind Engpässe erkannt und Lösungen ausreichend beschrieben?				
1.2	Inwieweit passt die IT-Strategie zu dem Target-Unternehmen?				
1.3	Existiert eine Roadmap für einen mittel- bis langfristigen Zeitraum (3-5 Jahre) mit klaren Projekten, die zur IT-Strategie passen?				
1.4	Enthält die IT-Strategie Risiken, die für eine Übernahme relevant sein könnten?				
1.5	Wie sieht die Geschäftsführung bzw. die Fachbereiche die IT strategisch aufgestellt?				
1.6	Sind mögliche Risiken in der IT-Strategie dargestellt, die für eine Übernahme relevant sein könnten?				
1.7	Wird für die IT-Governance-Strukturen das COBIT-Rahmenwerk eingesetzt oder sind klare individuelle Standards im Einsatz?				
1.8	Sorgen IT-Governance-Prozesse dafür, dass die Risiken durch IT im Unternehmen minimiert werden?				
1.9	Haben IT-Audits von externen Prüfern stattgefunden? Welche Ergebnisse sind dabei herausgekommen? (Prüfberichte anfordern)				

Zur Bewertung der Fragen und Ermittlung des Reifegrades kann eine einfache Logik anhand von Schulnoten herangezogen werden. Dabei wird jede Frage mit einer Schulnote (von 1= sehr gut bis 6=ungenügend) bewertet. Abschließend werden die Noten addiert und durch die Anzahl der Fragen geteilt: Dies ist der Reifegrad.

Checkliste 2: IT-Organisation und Personal

Generelle Anmerkungen:

Neben den typischen Organigrammen und Stellenbeschreibungen der IT-Organisation, ist es vor allem wichtig, in den Befragungen herauszufiltern, inwieweit es eine „inoffizielle IT“ im Target Unternehmen gibt und welchen Einfluss diese hat. Wo gibt es Schatten-IT, in welchem Maße und Reifegrad? In welchen Bereichen ist viel IT Know how vorhanden und welchen eher wenig?

#	Untersuchungsgegenstand	Benötigt?	Geliefert?	Reifegrad	Beurteilung / Bemerkungen
2.1	Ist die Aufbauorganisation der IT passend zur IT-Strategie, den Herausforderungen des Unternehmens aufgestellt? (Organigramm der IT-Abteilung geben lassen)				
2.2	Wie ist die Berichtslinie (direct report) des CIOs (zu wem)?				
2.3	Gibt es dokumentierte und ausführliche Stellenbeschreibungen sowie klare Rollendefinitionen für jeden IT-Mitarbeiter?				
2.4	Sind die Kompetenzen und Skills jedes IT-Mitarbeiters ausreichend dokumentiert (nicht nur IT-Skills,				

	sondern auch Führungserfahrung, Weiterbildungen, soft skills, etc.)? (Skill-Matrix anfordern)				
2.5	Gibt es Schlüsselpersonen? (mit alleinigem Wissen / herausragender Kunden-/Fachbereichskontakt?) – Liste anfordern				
2.6	Wie schätzen Sie die Kompetenz der IT-Führungskräfte ein (neben Führungserfahrung vor allem auch Change-Erfahrung, Agiles Denken und Handeln, wie wird geführt (Command&Order oder Management by Objectives, etc.)?				
2.7	Existiert eine detaillierte Sourcing-Strategie und sind klare Regeln erkennbar nach denen IT-Lieferanten ausgewählt werden und überprüft werden?				
2.8	Existiert eine Stellenplanung für die IT? Wie passt die zu Ihren Zielen bzw. welche Überschneidungen gibt es?				
2.9	Gibt es Zielvereinbarungen? Wie sind die Bewertungen bzw. Ergebnisse?				

Checkliste 3: IT Systemlandschaft und Architektur

#	Untersuchungsgegenstand	Benötigt?	Geliefert?	Beurteilung / Bemerkungen
3.1	Gibt es eine Übersicht zu allen Applikationen? (Architekturmappe, Soll-Bebauungsplan, etc.)			
3.2	Gibt es eine dokumentierte IT-Architektur und einen Bebauungsplan (Ist/Soll)?			

3.3	Welchen Reifegrad hat die IT-Architektur in Bezug auf Skalierbarkeit?			
3.4	Passt die IT-Architektur in Ihre IT-Architektur in Bezug auf Doppelungen oder sinnvollen Ergänzungen?			
3.5	Sind IT-Lösungen standardisiert, modular und sourcingfähig?			
3.6	Sind die Haupt-IT-Systeme (wie ERP, CRM, PLM) als Produkt gekauft und weiterhin im Standard oder stark gecustomized oder sogar individuell entwickelt worden?			
3.7	Bei Individualentwicklung: Wem gehört der Source-Code? Welche Ressourcen sind kritisch was den Code angeht?			
3.8	Gibt es klar definierte Vorgehensmodelle in der Softwareentwicklung? Ist die Dokumentation der Software auch im Quellcode eingearbeitet, so dass Dritte daran weiterarbeiten können?			
3.9	Werden in allen IT-Softwareprojekten detaillierte Lasten- und Pflichtenhefte als Grundlage für die Programmierung eingefordert?			
3.10.	Ist die Dokumentation der Software auch im Quellcode eingearbeitet, so dass Dritte daran weiterarbeiten können?			
3.11	Sind die verwendeten Programmiersprachen gängig und in Ihrem Hause bekannt?			
3.12	Ist eine Übersicht über Schatten-IT-Systeme (ohne offizielle Unterstützung der IT entstandene oder gekaufte IT-Systeme in den Fachbereichen) vorhanden und wird an der Integration dieser Schatten-Systeme im Rahmen der IT-Architektur gearbeitet?			
3.13	Ist der erstellte Quell-Code für wesentliche Applikationen vollständig und wird geprüft, so dass Dritte Änderungen und Erweiterungen vornehmen können?			

3.14	Ist die Ablösung von bestehenden Legacy-Systemen in die IT-Architekturplanung integriert und gibt es einen klaren Plan bis wann diese abgelöst sind?			
3.15	Gibt es klare Verantwortlichkeiten und Rollen für das Management und die Pflege der IT-Architektur?			

Checkliste 4: IT-Infrastruktur / IT-Betrieb / IT-Security

Vorliegen sollte hier eine vollständige (Inventur)-Liste aller Hardwaregeräte, die da wären: PCs/Notebooks, Drucker (Unterscheidung Einzelplatz, Multifunktion), Server (physisch als auch virtuell), Smartphones, Netzwerkgeräte (Firewalls, Switches, Hubs, WLAN-Access Points, etc.), Telefonanlagen und Telefone.

#	Untersuchungsgegenstand	Benötigt?	Geliefert?	Beurteilung / Bemerkungen
4.1	Gibt es eine Trennung zwischen Applikationsbereitstellung und Betrieb?			
4.2	Sind die Service Management Prozesse nach einem Best Practice Ansatz und/oder ITIL standardisiert?			
4.3	Basiert der IT-Betrieb auf standardisierten Service Design Prozessen (Availability (Diensteverfügbarkeit), Continuity (Wiederherstellung der Dienste im Katastrophenfall) sowie Capacity Management (Planung/Überwachung der notwendigen Ressourcen))?			
4.4	Ist ein professionelles Service Desk mit Hotline und Ticket-System eingerichtet?			
4.5	Wird auf Basis von klar abgestimmten Service Level Agreements mit Lieferanten und intern gegenüber Kunden gearbeitet?			

4.6	Wird auf Basis von standardisierten Service Operations Prozessen (Incident-, Problem-, Change- und Release Management) gearbeitet?			
4.7	Sind Dokumentationen zu den Softwareentwicklungsvorgaben vorhanden?			
4.8	Gibt es ein detailliertes IT-Sicherheitskonzept im Unternehmen und wird die Durchführung vom IT-Management geprüft und eingefordert			
4.9	Existiert ein Notfallplan/Disaster Recovery Prozess, der regelmäßig getestet wird?			
4.10	Sind die Prozesse im Bereich Availability Management (Sicherstellen und Optimieren der Dienstverfügbarkeit) sowie des Continuity Managements (Wiederherstellen der notwendigsten Dienste im Katastrophenfall) standardisiert?			
4.11	Sind alle IT-Infrastruktur-Endgeräte im Unternehmen, wie zum Beispiel Notebook/Desktop, Monitor, Maus, Tastatur standardisiert?			
4.12	Gibt es ein Monitoring mit klaren Warn- und Prüfmechanismen für das Rechenzentrum, so dass Fehler frühzeitig erkannt und behoben werden können?			
4.13	Sind funktionierende Datensicherungen für alle Server vorhanden und wird dieser Sicherungsmechanismus ständig geprüft und gewartet?			
4.14	Wird die Auslastung der Server konsequent analysiert, sind Last-Spitzen bekannt und werden möglichst vermieden?			

Checkliste 5: IT-Projekte und Portfolio Management

#	Untersuchungsgegenstand	Benötigt?	Geliefert?	Beurteilung / Bemerkungen
5.1	Welche laufenden IT-Projekte gibt es? (Projektübersichtsliste, CR-Liste)			
5.2	In welchem Zustand sind diese Projekte (budget, quality, time)?			
5.3	Sind diese IT-Projekte für das Target Unternehmen relevant und wichtig?			
5.4	Wie hoch ist das Projektvolumen der einzelnen Projekte und gesamt?			
5.5	Gibt es ein Projektportfolio?			
5.6	Wie sind die Projekte aus Risikosicht zu bewerten?			
5.7	Gibt es klare Richtlinien für Projekte (Projektmanagement Handbuch) inkl. Rollenverständnis, Vorlagen und Meilensteinen?			
5.8	Gibt es ausgebildete (zertifizierte) Projektmanager in der IT?			

Checkliste 6: IT-Finanzen und IT-Controlling

#	Untersuchungsgegenstand	Benötigt?	Geliefert?	Beurteilung / Bemerkungen
6.1	Unterliegt das Kostenmanagement der IT klaren Regeln nach Kostenstellen, -arten und -trägern; sind diese zugänglich und wie sind diese zu bewerten?			
6.2	Gibt es spezifische Kostentreiber oder Risiken			
6.3	Gibt es für IT-Systeme, IT Operations und IT-Projekte spezifische IT-Kennzahlen und KPIs; wie sind diese zu bewerten?			
6.4	Gibt es ein Monitoring- und Reportingsystem – beispielsweise auf Basis einer IT-Balanced Scorecard?			
6.5	Gibt es Wirtschaftlichkeitsrechnungen und Prozess- und Projektkostenübersichten? Wie sind diese zu bewerten und welche Risiken gibt es?			
6.6	Benchmark für IT: Wie verhalten sich die IT-Gesamtausgaben und der Personalbestand im Vergleich zu anderen in dieser Branche?			

Checkliste 7: IT-Prozesse und IT-Einkauf

In diesem Analysefeld sind die Kern- und unterstützenden IT-Prozesse zu dokumentieren und bzgl. ihrer Eignung zur Leistungserbringung im fusionierten Unternehmen zu untersuchen.

Zu den Kernprozessen gehören z. B. der User-Support für Hard und Software, regelmäßige Software- Updates und der Prozess zum Einkauf von IT-Dienstleistungen. Prozesse zur Sammlung, Dokumentation und Priorisierung von Change Requests oder Genehmigungsverfahren für IT-Nutzer (insbes. Applikationen) sind eher zu den unterstützenden Prozessen zu zählen. Eine relativ einfache Methode zur Bestimmung der unternehmenskritischen und somit Kernprozesse ist die Abschätzung, welcher Prozessausfall innerhalb von kurzer Zeit zum Zusammenbruch der wesentlichen Unternehmensfunktionen führen könnte, d.h. das Unternehmen daran hindern würde, die hergestellten Produkte (auch Dienstleistungen) am Markt anzubieten bzw. zu fakturieren (Business-Continuity- Ansatz).

#	Untersuchungsgegenstand	Benötigt?	Geliefert?	Beurteilung / Bemerkungen
7.1	Gibt es eine Übersicht aller IT-Dienstleister und Lieferanten? (Lieferantenliste anfordern)			
7.2	Alle Softwareverträge, Wartungs- und Lizenzverträge müssen geprüft werden			
7.3	Alle Outsourcingverträge bzgl. Betrieb und Infrastruktur und Arbeitsplatzsysteme müssen geprüft werden			
7.4	Entsprechen die vertraglich festgelegten Preismodelle mit Lieferanten dem tatsächlichen Verbrauch und sind sie variabel gestaltet (zum Beispiel durch „pay-per-use“)?			
7.5	Bestehen Exit-Klauseln in den Verträgen mit Lieferanten, welche ermöglichen ohne Mehrkosten flexibel zu einem anderen Anbieter zu wechseln			
7.6	Gibt es klar gegliederte EIT Einkaufsprozesse? (Wer kauft ein? Genehmigungsinstanzen, etc.)			
7.7	Ist ein durchgehender Compliance-Prozess nach COBIT-Kriterien vorhanden?			

7.8	Gibt es ein Lizenzmanagement? Sind alle Produkte lizensiert? Besteht die Gefahr eine Über- bzw. Unterlizensierung?			
7.9	Ist die GDPdU-konforme Archivierung aller notwendiger Dokumente gewährleistet?			
7.10	Kann sichergestellt werden, dass alle im Unternehmen benutzten Softwareprodukte auch rechtmäßig erworben wurden?			
7.11	Ist im Unternehmen eine Datenschutzrichtlinie vorhanden, die sicherstellt, dass alle Daten geschützt werden?			