Juli 2014

DIN SPEC 66286

ICS 35.240.01

Management von Cloud Computing Lösungen in kleinen und mittleren Unternehmen (KMU)

Management of Cloud Computing solutions in small and medium enterprises (SME)

Zur Erstellung einer DIN SPEC können verschiedene Verfahrensweisen herangezogen werden:
Das vorliegende Dokument wurde nach den Verfahrensregeln einer PAS erstellt.

Gesamtumfang 60 Seiten

Bereich Innovation

Preisgruppe 21
www.din.de
www.beuth.de

2146449

Inhalt

Bilder

Tabellen

Vorwort

Diese DIN SPEC wurde nach dem PAS-Verfahren erarbeitet. Die Erarbeitung von DIN SPEC nach dem PAS-Verfahren erfolgt in Workshops und nicht zwingend unter Einbeziehung aller interessierten Kreise.

Dieses Dokument wurde vom Normenausschuss NA 043-WS 01 „DIN SPEC (PAS) Management von Cloud Computing Lösungen in KMU“ erarbeitet.

Die Erarbeitung und Verabschiedung des Dokuments erfolgte durch die nachfolgend genannten Initiatoren und Verfasser:

— HITeC e.V. c/o Department Informatik Universität Hamburg
Müller-Wickop, Niels
Schultz, Martin

— antispameurope GmbH
Dehning, Oliver

— HDP Management Consulting GmbH
Dörhöfer, Thomas

— CyberTribe
Kossow, Roland

— FRITZ & MACZIOL Software und Computervertrieb GmbH
Mecke, Jörg

— Folker Scholz Unternehmensberatung
Scholz, Folker

— EuroCloud Deutschland eco e.V.
Weiss, Andreas

— GOD Gesellschaft für Organisation und Datenverarbeitung GmbH
Wolenski, Thomas

Für dieses Thema bestehen derzeit keine Normen. DIN SPEC sind nicht Teil des Deutschen Normenwerks.

Trotz großer Anstrengungen zur Sicherstellung der Korrektheit, Verlässlichkeit und Präzision technischer und nicht-technischer Beschreibungen kann der Workshop weder eine explizite noch eine implizite Gewährleistung für die Korrektheit des Dokuments übernehmen. Die Benutzung dieses Dokuments geschieht in dem Bewusstsein, dass der Workshop für Schäden oder Verluste jeglicher Art nicht haftbar gemacht werden kann. Die Anwendung der vorliegenden DIN SPEC entbindet den Nutzer nicht von der Verantwortung für eigenes Handeln und geschieht damit auf eigene Gefahr.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. DIN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Für diese DIN SPEC wurde kein Entwurf veröffentlicht.

1 Anwendungsbereich

Die DIN SPEC 66286 zum *Management von Cloud Computing Lösungen in kleinen und mittleren Unternehmen (KMU)* gibt Leitlinien für die Durchführung von Outsourcing-Vorhaben an Cloud-Service-Anbieter vor. Nachfolgend wird diese Art des Outsourcings als „Cloud-Sourcing“ bezeichnet (siehe hierzu Abschnitt 3. „Begriffe“). Dabei soll vor allem KMUs eine Hilfestellung gegeben werden, um Cloud-Sourcing-Vorhaben in die Cloud nach einem Standardvorgehen durchzuführen.

Für die Anwendung dieser DIN SPEC sollten die folgenden Rahmenbedingungen berücksichtigt werden:

- Die DIN SPEC ist überwiegend aus Sicht des Cloud-Sourcing-Gebers verfasst worden.
- Die DIN SPEC betrachtet abstrahierend Cloud-Sourcing-Gegenstände. Letztendlich bezieht der Cloud-Sourcing-Geber unabhängig vom Cloud-Sourcing-Gegenstand Dienstleistungen vom Cloud-Service-Anbieter. Aus Sicht des KMU werden diese als Prozesse und Services bezeichnet.
- Es wird nicht auf Spezifika besonderer Cloud-Sourcing-Gegenstände oder -Vorhaben eingegangen, damit das geschilderte Vorgehen hinreichende Allgemeingültigkeit behält.
- Das beschriebene Vorgehensmodell fokussiert den typischen Fall, dass ein Unternehmen bisher intern erbrachte Prozesse und Services zukünftig einem externen Cloud-Service-Anbieter übergeben möchte.
- Das beschriebene Vorgehensmodell darf in seiner Anwendung nicht streng sequentiell verstanden werden. In der Praxis kann sich die Reihenfolge der Bearbeitung der Phasen verschieben oder Phasen können sich parallel in Bearbeitung befinden. Die dargestellte Anordnung der Phasen ist insofern lediglich eine wahrscheinliche, nicht aber zwingende Abfolge.
- Die Relevanz einzelner Schritte im Phasenmodell hängt vom individuellen Projektkontext ab. In besonderen Fällen können einzelne Schritte gänzlich irrelevant sein. Bei Anwendung dieser DIN SPEC muss eine Nichtbeachtung einzelner Schritte oder Spezifikationsdokumente jedoch auf dokumentierten validen Gründen beruhen.

2 Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

DIN 69901 (alle Teile), *Projektmanagement — Projektmanagementsysteme*

DIN ISO 21500, *Leitlinien Projektmanagement*

DIN ISO/IEC 27001, *Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Anforderungen*

DIN ISO/IEC 27002, *Informationstechnik — IT-Sicherheitsverfahren — Leitfaden für das Informationssicherheits-Management*

DIN SPEC 1041:2010-05, *Outsourcing technologieorientierter wissensintensiver Dienstleistungen*

ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

ISO/IEC 38500, *Corporate governance of information technology*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1
Anforderungskatalog
interner Katalog der Cloud-Sourcing-Gegenstände, die an den Cloud-Service-Anbieter ausgelagert werden

3.2
Compliance
Einhaltung von Gesetzesvorschriften und organisationsintern vorgegebenen Regeln

3.3
Key Performance Indicators
KPI
Indikatoren, die helfen, den Fortschritt oder Erfüllungsgrad wichtiger Zielsetzungen bzw. zu erbringender Leistungen zu messen

3.4
Letter of Intent
LOI
Absichtserklärung zwischen Cloud-Sourcing-Geber und potenziellem Cloud-Service-Anbieter, um die Ernsthaftigkeit weiterer Verhandlungen beidseitig zu bekräftigen

3.5
Outsourcing
Auslagerung von Leistungen oder Funktionen eines Unternehmens an externe Dienstleister

Anmerkung 1 zum Begriff: In der hier vorliegenden DIN SPEC werden die externen Dienstleister als „Cloud-Service-Anbieter“ bezeichnet

Anmerkung 2 zum Begriff: „Outsourcing“ ist ein Kunstwort das sich aus den englischen Begriffen „outside“, „resource“ und „using“ zusammensetzt, es bezeichnet den externen Bezug von Services bzw. Dienstleistungen.

3.6
Cloud-Sourcing
Outsourcing von Prozessen oder Services zu einem Cloud-Service-Provider

3.7
Cloud-Sourcing-Geber
Organisation, die bisher intern betriebene Prozesse zukünftig als Services von einem Cloud-Service-Anbieter beziehen möchte

3.8
Cloud-Sourcing-Gegenstand
Services und Prozesse, die aus Sicht des Cloud-Sourcing-Gebers ausgelagert werden sollen, aber noch nicht als Dienstleistung formuliert wurden

Anmerkung 1 zum Begriff: Cloud-Sourcing-Gegenstände sind eine Untermenge der Cloud-Sourcing-Kandidaten.

3.9
Cloud-Sourcing-Kandidat
Services und Prozesse, die sich prinzipiell für das Cloud-Sourcing eignen.

Anmerkung 1 zum Begriff: Im Kontext dieser DIN SPEC speziell Services und Prozesse die sich prinzipiell für das Cloud-Sourcing eignen.

3.10
Cloud-Service-Anbieter
Dienstleister oder Anbieter oder Organisation, die den Cloud Service erbringen

3.11
Cloud-Sourcing-Vorhaben
in ein Projekt umgesetzte Absicht eines Unternehmens, Cloud-Sourcing-Gegenstände als Services extern zu beziehen

3.12
Performance
Güte der Serviceerbringung durch den Cloud-Service-Anbieter in quantitativer oder qualitativer Hinsicht

3.13
Projekt
Vorhaben zur Lösung einer bestimmten, definierten Aufgabe, das üblicherweise durch Einmaligkeit, durch eine zeitliche Befristung mit definiertem Anfang und Abschluss, durch Komplexität und Innovation, durch begrenzte Ressourcen sowie durch Risikobehaftung gekennzeichnet ist

3.14
Prozess
Ablauf mit definierten Aktivitäten, definiertem Anfang und Ende und einem angestrebten Ergebnis

3.15
Rahmenvertrag
Vertrag, der die Grundlage für eine Reihe von Cloud-Sourcing-Verträgen bildet

Anmerkung 1 zum Begriff: Er enthält allgemeine Absprachen im Vertragswerk, die nicht auf Regelung einzelner Dienstleistungen abzielen.

3.16
Request for Information
RFI
unverbindliche Informationsanfrage eines Cloud-Sourcing-Gebers an potenzielle Cloud-Service-Anbieter zur Erteilung einer Selbstauskunft

Anmerkung 1 zum Begriff: Ein RFI enthält darüber hinaus i. d. R. die Aufforderung an die Cloud-Service-Anbieter, im Rahmen einer geplanten Ausschreibung einen Fragenkatalog zu bearbeiten, der i. d. R. Fragen zum Unternehmen des Cloud Anbieters aber auch eine Skizze des beabsichtigten Cloud-Sourcing-Vorhabens enthält. Das RFI dient zur Vorauswahl derjenigen Cloud-Service-Anbieter, die in die eigentliche Ausschreibung einbezogen werden und dann einen Request for Proposal (RFP) erhalten.

3.17
Request for Proposal
RFP
Aufruf an potenzielle Cloud-Service-Anbieter, sich auf eine Ausschreibung des Cloud-Sourcing-Gebers zu bewerben
Anmerkung 1 zum Begriff: Das RFP enthält i. d. R. eine ausführliche Beschreibung des Cloud-Sourcing-Vorhabens, detaillierte Angaben zu Mengengerüsten, erwarteten Services und Service Levels Agreement(s) (SLA) und einen genauen Zeitplan des Projektverlaufes. Ergebnis des RFP-Prozesses ist i. d. R. die Abgabe verbindlicher Angebote, einschließlich detaillierter Preisstrukturen als Basis für eine finale Kundenentscheidung über die Auswahl des Cloud-Service-Anbieters.

3.18
Dienstleistung
Erbringung eines Services bzw. Dienstes, der zwischen Cloud-Sourcing-Geber und Cloud-Service-Anbieter vereinbart wurde

3.19
Service Level Agreement
SLA
Vertragsvereinbarung über Qualität und Quantität der zu erbringenden Service-Leistungen anhand eindeutig nachweisbarer und nachvollziehbarer Kriterien (Service Level)

3.20
Cloud Computing
Modell zur Ermöglichung eines ubiquitären, komfortablen, auf Abruf verfügbaren Netzzugriffs auf einen gemeinsamen Pool aus konfigurierbaren Rechenressourcen der schnell und mit geringfügigem Verwaltungsaufwand bzw. minimaler Interaktion mit dem Dienstanbieter bereitgestellt und öffentlich verfügbar gemacht werden kann

Anmerkung 1 zum Begriff: Im Rahmen des Cloud Computings wird zwischen verschiedenen Dienstschichten und Betriebsmodellen unterschieden.

Anmerkung 2 zum Begriff: Rechenressourcen könne Netze, Server, Speicher, Anwendungen und Dienste sein.

3.20.1
Betriebsmodell
Charakterisierung der eigentums- und nutzungsrechtspezifischen Aspekte von Cloud Angeboten

3.20.1.1
Public Cloud
durch die Allgemeinheit nutzbare Cloud-Infrastruktur, deren Service mit anderen geteilt genutzt (Multi-Mandanten) und bei der der Zugriff auf Daten und Ressourcen logisch separiert wird

3.20.1.2
Private Cloud
für die ausschließliche Verwendung durch eine einzige Organisation mit unterschiedlichen Nutzern bereitgestellte Cloud-Infrastruktur

Anmerkung 1 zum Begriff: Die Bereitstellung kann durch den Anwender oder externe Dienstleister erfolgen.

3.20.1.3
Hybrid Cloud
Cloud-Infrastrukur-Mischung, in der exklusive interne mit öffentlichen Cloud-Aktivitäten kombiniert werden

3.20.1.4
Community Cloud
ausschließlich für die Verwendung durch eine bestimmte Gemeinschaft von Organisationen und deren Nutzern, welche gemeinsame Anliegen haben, bereitgestellte Cloud-Infrastruktur

Anmerkung 1 zum Begriff: Die Bereitstellung kann durch die Gemeinschaft von Organisationen oder externe Dienstleister erfolgen.

Anmerkung 2 zum Begriff: Gemeinsame Anliegen können z. B. ähnliche Missionen, Sicherheitsanforderungen, Richtlinien, Branchenzugehörigkeit, gemeinsame Lokation und Compliance-Überlegungen sein.

3.20.2
Dienstschicht
Betrachtungsdimension in der definiert wird, welcherlei Dienstleistungsart ein Cloud Service verkörpert

Anmerkung 1 zum Begriff:

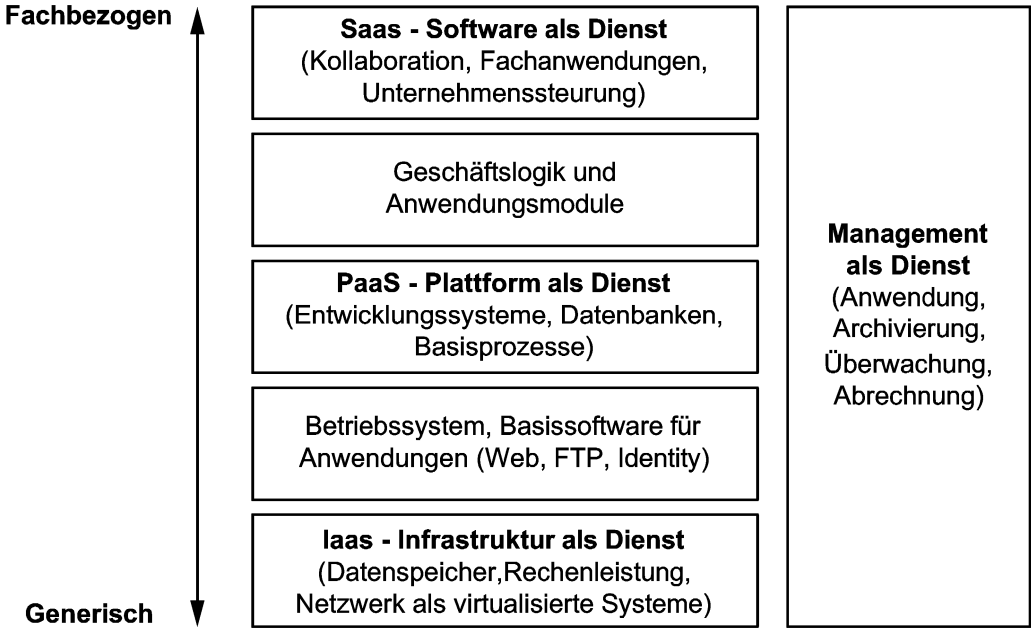

Bild 1 — Anmerkung zum Begriff Dienstschicht

3.20.2.1
Infrastruktur as a Service
IaaS
Dienstleistungen, die es einem Anwender erlauben, über bereitgestellte Hardware-Ressourcen wie Prozessoren, Speicher, Netzwerkinfrastruktur und andere grundlegende IT-Ressourcen zu verfügen

Anmerkung 1 zum Begriff: Auf der bereitgestellten Infrastruktur ist der Kunde in der Lage, eigenständig Software wie Betriebssysteme und weitere Anwendungen zu installieren und zu betreiben. Dabei administriert und kontrolliert der Kunde jedoch nicht die zugrundeliegende Infrastruktur der Cloud, sondern hat lediglich die Verfügung über das Betriebssystem, Speicher und installierte Anwendungen, sowie eingeschränkte Kontrolle über ausgewählte Komponenten der Netzwerkinfrastruktur.

3.20.2.2
Plattform as a Service
PaaS
Dienstleistungen, die es einem Anwender erlauben, selbsterstellte oder erworbene Anwendungen auf der bereitgestellten Cloud-Infrastruktur zu installieren

Anmerkung 1 zum Begriff: Die Anwendungen verwenden Programmiersprachen, Bibliotheken, Dienste und Software-Werkzeuge die vom Cloud Anbieter bereitgestellt werden. Dabei administriert und kontrolliert der Kunde jedoch nicht die zugrundeliegende Infrastruktur der Cloud wie Netzwerk, Server, Betriebssystem oder Speicher, sondern hat lediglich die Verfügung über die eigenen Anwendungen und unter Umständen über ausgewählte Konfigurationseinstellungen der zugrundeliegenden Anwendungsumgebung.

3.20.2.3
Software as a Service
SaaS
Dienstleistungen, die es einem Anwender erlauben, Anwendungen eines Anbieters zu nutzen, die über eine Cloud-Infrastruktur bereitgestellt werden

Anmerkung 1 zum Begriff: Auf die Anwendungen kann über unterschiedliche Nutzerschnittstellen wie Web-Browser oder Programmierschnittstellen (API) zugegriffen werden. Dabei administriert und kontrolliert der Kunde jedoch nicht die zugrundeliegende Cloud-Infrastruktur wie Netzwerk, Server, Betriebssystem, Speicher oder spezifische Anwendungsfunktionalitäten, sondern lediglich eine begrenzte Auswahl nutzerspezifischer Konfigurationseinstellungen.

4 Phasenmodell

4.1 Allgemeines

Das in diesem Dokument beschriebene Phasenmodell zum Management von Cloud Computing Lösungen umfasst fünf Hauptphasen:

1) Festlegen von Verantwortlichkeiten und Zielen;
2) Service Auswahl;
3) Cloud-Service-Anbieter Auswahl;
4) Implementierung;
5) Betrieb.

Jede Phase ist in detaillierte Unterpunkte untergliedert. Diese Strukturierung soll potenziellen Cloud-Sourcing-Gebern als Entscheidungs- und Implementierungshilfe dienen. Für die Beschreibung innerhalb der Phase „Service Auswahl“ und „Cloud-Service-Anbieterauswahl“ wird im Rahmen dieser DIN SPEC eine gleichbleibende Gliederung verwendet:

1) Wesentliche Fragen: Wesentliche zu beantwortende Fragen aus Sicht eines potenziellen Cloud-Sourcing-Gebers.
2) Beschreibung allgemein: Beschreibung der Phase und Schilderung von Anforderungen.
3) Verantwortlichkeiten: Mit Hilfe einer RASCI-Matrix werden die Verantwortlichkeiten für wesentliche Aktivitäten innerhalb einer Phase dargestellt. Hierbei wird zwischen den folgenden Verantwortlichkeiten/Zuständigkeiten unterschieden:

— R: Responsible – verantwortlich (Durchführungsverantwortung)
— A: Accountable – rechenschaftspflichtig (Kostenverantwortung)
— S: Supportive – unterstützend (Unterstützungsfunktion)
— C: Consulted – konsultiert (Fachverantwortung)
— I: Informed – zu informieren (Informationsrecht)

Tabelle 1 — Beispiel RASCI-Chart

Nr.	Task	Rolle 1	Rolle 2	Rolle 3	Rolle n
1	**Task**				
1.1	Sub Task	A	R	I	
1.2	Sub Task	A	R		
2	**Task**				
2.1	Sub Task	A	C		
2.2	Sub Task	A		S	

Wesentliche Rollen, welche innerhalb der DIN SPEC Berücksichtigung finden, sind die Geschäftsleitung, der Einkauf, der Projektleiter (stellvertretend auch für das Projektteam), die Fachbereiche, der Cloud-Service-Anbieter, der Compliance Beauftragte bzw. der Betriebstrat, die IT (IT-Leitung, IT-Entwicklung, IT-Betrieb) und der IT-Sicherheitsverantwortliche.

4. **Ergebnisdokumente**: Liste von Dokumenten/Hilfestellungen, die während der Phase genutzt werden sollten und somit Ergebnis der Phase sein können.

Tabelle 2 — Beispiel Ergebnisdokumente

Dokument ID	Dokument Bezeichnung	Dokument Beschreibung	Dienst-schicht	Betriebsmodell
D.X.01	Generischer Kriterienkatalog	Verzeichnis aller Kriterien, deren Eigenschaften und möglichen Ausprägungen	IaaS PaaS SaaS	Private Public Hybrid Community

4.2 Festlegen von Zielen und Verantwortlichkeiten

4.2.1 Wesentliche Fragen

- Welche generellen Ziele sollen durch das Cloud-Sourcing-Vorhaben erreicht werden?
- Welche Personen sind im Rahmen des Cloud-Sourcing-Vorhabens grundsätzlich wofür verantwortlich?

4.2.2 Beschreibung allgemein

Bevor erste Planungsschritte des **Projekts** unternommen werden, sollten allgemeine Regeln und Verantwortlichkeiten auf oberster Ebene der Organisation festgelegt werden. Zunächst muss die Geschäftsführung eine klare Absicht und Verantwortung übernehmen, dass Cloud Computing zur Erbringung von Services evaluiert wird. Dies schließt auch die Verantwortung für die Einhaltung gesetzlicher Regelungen ein, die erst im Verlauf des Projekts relevant werden. Allen Entscheidern muss bewusst sein, dass die Verantwortung für ausgelagerte betriebliche Prozesse bzw. Services beim Cloud-Sourcing-Geber verbleibt und eine befreiende Abwälzung von Verantwortlichkeiten auf den Cloud-Service-Anbieter nicht möglich ist.

Die Festlegung der allgemeinen Rahmenbedingungen beinhaltet zunächst die Formulierung der generellen **Ziele** zur Nutzung einer Cloud-Lösung. Diese Ziele sind abzuleiten aus der allgemeinen Geschäftsstrategie, der speziellen Einkaufs- und Beschaffungsstrategie, dem Geschäftsmodell des Unternehmens sowie den Problembereichen, welche durch eine Auslagerung möglicherweise gelöst werden können. Übergeordnete Ziele können u. a. Beschleunigung, Agilität, Elastizität, Kosteneinsparungen und/oder die Nutzung aktueller IT/Software und den damit einhergehenden Vorteilen sein. Weiterhin sollte ein grober **Zeitplan** mit ersten Meilensteinen erarbeitet werden. In Zusammenhang mit dem Zeitplan sind erste Überlegungen und Abschätzungen hinsichtlich des benötigten **Budgets** vorzunehmen. Darüber hinaus sollte die **Organisation** des Projekts dokumentiert werden (Aufbauorganisation) und welche Entscheidungsgremien einzurichten sind. Es sollten Überlegungen angestellt werden, welche Interessengruppen ab welchem Zeitpunkt zu informieren sind (insbesondere Arbeitnehmervertretungen). Ein **strukturiertes Vorgehen** für die interne Kommunikation und Einbindung des Management sowie unterstützender Funktionen ist für eine erfolgreiche Umsetzung nötig. Hiervon hängt die Qualität der späteren Umsetzung maßgeblich ab.

Bei einem Cloud-Sourcing-Vorhaben handelt es sich um ein Projekt (siehe zum Projektmanagement auch die Normenreihe DIN 69901 sowie die DIN ISO 21500.). Das Scheitern von Projekten kann das wirtschaftliche Ergebnis des Unternehmens entscheidend beeinflussen oder sogar die Existenz des Unternehmens gefährden (siehe 4.3.4).

Tabelle 3 — Verantwortlichkeiten bei der Festlegung von Zielen und Verantwortlichkeiten

Nr.	Aufgabe	Geschäftsleitung	Einkauf	Projektleiter	Fachbereich	Cloud-Service-Anbieter	Compliance-Beauftragter/ Betriebsrat	IT
1	**Definition von Zielen**							
1.1	Strategische Ziele	A	R	C	C			
1.2	Operationale Ziele	A	R	C	C			
1.3	Organisationale Ziele	A	R	C	C			
2	**Zeit- und Budgetplan**							
2.1	Meilensteinplanung	A	R	C	C	R		
2.2	Budgetierung	A	R	C	C	R		
3	**Organisation**							
3.1	Festlegen von Verantwortlichkeiten	A	I	I	C	R		
3.2	Festlegen der Organisations- / Projektstruktur	A	I	I	C	R		

Tabelle 4 — Ergebnisdokumente der Phase „Festlegung von Zielen und Verantwortlichkeiten“

ID	Dokument Bezeichnung	Dokument Beschreibung	Dienst-art	Dienst-modus
3.2 – A	Zieldefinition	Protokoll/Dokumentation über generell zu erreichende strategische/operationale, organisationale Ziele im Rahmen eines Cloud-Sourcing-Vorhabens	Alle	Alle
3.2 – B	Grober Projektplan	Aus dem groben Projektplan sollte ersichtlich werden, welche Zeit das Cloud-Sourcing-Vorhaben in Anspruch nehmen soll und welche wesentlichen Meilensteine als Zwischenergebnisse zu welchem Zeitpunkt erreicht sein sollten. Wichtige Meilensteine sollten vom Verantwortlichen schriftlich freigegeben werden (Sign-Off). Weitere wichtige Komponenten im Projektplan: 1) Projektstruktur 2) Projektaufbauorganisation 3) Projektablauforganisation	Alle	Alle
3.2 – C	Organigramm	Aus dem Organigramm sollte hervorgehen, welche Personen in welchen Rollen in dem Cloud-Sourcing-Vorhaben teilnehmen. In dem Organigramm sollten auch wesentlichen Entscheidungsgremien vermerkt sein.	Alle	Alle
3.4 – E	Grobe Budgetplanung	Kurzfristiger, monetärer Projektplan. Hier ist es ausreichend, den Finanzbedarf pro Projektphase zu planen und auf Bedarfsspitzen hinzuweisen.	Alle	Alle

4.3 Service Auswahl

4.3.1 Prozess- und Serviceanalyse

4.3.1.1 Wesentliche Fragen

- Welche (IT-gestützten) Prozesse/IT-Applikationen/IT-Infrastruktur sind im betrachteten Unternehmensbereich vorhanden?
- Welche (IT-gestützten) Prozesse/IT-Applikationen/IT-Infrastruktur kommen unter Berücksichtigung der gesetzten Ziele des Cloud-Sourcing-Vorhabens grundsätzlich für die Auslagerung an einen Cloud-Service-Anbieter in Frage (Cloud-Sourcing-Kandidaten)?

4.3.1.2 Beschreibung allgemein

Im Kontext von Cloud Computing handelt es sich bei Cloud-Sourcing-Vorhaben um ein selektives IT-Cloud-Sourcing, bei dem bisher intern erbrachte Services zukünftig von einem Cloud-Service-Anbieter bezogen werden sollen [1].

Gegenstand des Cloud-Sourcing sind demgemäß (IT-gestützte) Prozesse, IT-Anwendungen und/oder IT-Infrastruktur-Services oder eine Kombination aus diesen.

Im Rahmen der Festlegung der Ziele (siehe 4.2) kann zunächst ein Unternehmensbereich bestimmt werden, für den Optionen für ein Cloud-Sourcing-Vorhaben mittels eines Cloud-Service-Anbieters analysiert werden sollen. Diese Eingrenzung ist bei größeren Unternehmen sinnvoll um den Aufwand in einer angemessenen Größenordnung zu halten. Auf Basis dieser zielorientierten Eingrenzung sind für den ausgewählten Unternehmensbereich zunächst die relevanten (IT-gestützten) Prozesse, IT-Applikationen bzw. IT-Infrastrukturkomponenten systematisch und vollständig zu erheben. Die erhobenen Informationen dienen als Ausgangspunkt, um nachfolgend bewerten zu können, welche Komponenten grundsätzlich für die Auslagerung an einen Cloud-Service-Anbieter in Frage kommen. Ergebnis dieser Phase ist somit eine Aufstellung von Cloud-Sourcing-Kandidaten unter Berücksichtigung der gewählten Zielstellung für das Cloud-Sourcing-Vorhaben.

Bei der Betrachtung von Cloud-Sourcing-Vorhaben im Umfeld von Cloud Computing sollte die Erhebung der oben genannten Komponenten differenziert nach IT-Applikationen oder differenziert nach Technologieebenen der IT-Infrastruktur erfolgen. Für eine geographische oder organisatorische Differenzierung gleichartiger IT-gestützter Geschäftsprozesse bzw. -varianten wird an dieser Stelle auf die DIN SPEC 1041, siehe 3.2 verwiesen. Bei der Differenzierung nach IT-Applikationen ist eine Übersicht aller wesentlichen IT-Applikationen inkl. wesentlicher Schnittstellen sowie der unterstützen Prozesse zu erstellen. Für eine technologieorientierte Differenzierung ist eine Übersicht der installierten Software, Daten(banken), System- und Netzwerkinfrastruktur, deren Beziehungen untereinander und Schnittstellen zu externen Systemen zu erarbeiten. Bei der Erhebung kann – sofern vorhanden – auf existierende Dokumentationen des Unternehmensbereichs zurückgegriffen werden. Sofern aus der übergeordneten Zielstellung des Cloud-Sourcing-Vorhabens (siehe 4.2) bereits eine Eingrenzung auf eine Dienstschicht oder Betriebsmodell des Cloud Computing ableitbar ist (z. B. Kostenreduktion beim Betrieb der IT-Infrastruktur), kann die Erhebung auf die entsprechenden Komponenten (z. B. IT-Applikationen bei SaaS, IT-Infrastruktur bei IaaS) beschränkt werden.

Aus den erstellten Übersichten sind im nächsten Schritt geeignete Cloud-Sourcing-Kandidaten auszuwählen. Hierfür müssen zunächst geeignete Entscheidungskriterien festgelegt werden, die darauf folgend im Rahmen einer Bewertung für die einzelnen Komponenten erhoben, gewichtet und systematisch ausgewertet werden. Für die Auswahl von Cloud-Sourcing-Kandidaten im Kontext von Cloud Computing sind zunächst aggregierte, qualitative Bewertungskriterien geeignet wie der **strategische Wert**, der **Grad der Spezifität**, die **Kritikalität** und die **Komplexität** der betrachteten Komponente. Als Betrachtungsgegenstand bietet sich die Ebene der IT-Applikationen an, da mit einer Bewertung dieser sich auch die Bewertung der unterstützen Prozesse und der zugrundeliegenden IT-Infrastruktur ableiten lassen:

- **Strategischer Wert** beschreibt die Bedeutung einer IT-Applikation für ein Unternehmen in Bezug auf die Abgrenzung vom Wettbewerb und auf die Schaffung von Wettbewerbsvorteilen.
- **Spezifität** beschreibt den Grad, zu dem eine IT-Applikation unternehmensspezifisch angepasst ist und sich damit von standardisiert am Markt verfügbaren Lösungen unterscheidet.

— **Kritikalität** umschreibt den potenziellen Schaden, den ein Ausfall oder Fehlverhalten einer IT-Applikation für ein Unternehmen verursachen würde, sowie die Kritikalität der verarbeiteten Informationen in Bezug auf Compliance/Vertraulichkeit/Datenschutz.

— **Komplexität** beschreibt die Komplexität der IT-Applikation selbst sowie deren Integration in die Prozesse und IT-Infrastruktur.

Die genannten aggregierten Bewertungskriterien lassen sich in detaillierte Kriterien untergliedern, um sie auf diese Weise für eine strukturierte Erhebung zu operationalisieren. Als Bewertungskriterium können folgende Aspekte in Frage kommen:

Tabelle 5 — Bewertungskriterien für die Identifikation von Cloud-Sourcing-Kandidaten

	Kriterium	**Wirkung**	**Mögliche Quantifizierung**
Strategischer Wert / Spezifität	IT als Wettbewerbsfaktor	Je wichtiger die Komponente für die Wettbewerbsfähigkeit ist, desto weniger ist sie für die Auslagerung geeignet (eine Private-Cloud-Lösung kann jedoch sinnvoll sein).	Nähe der Komponente zur Kernwert-schöpfung des Unternehmens, Potenzial zur Abgrenzung von Wettbewerbern.
	Notwendiges Wissen	Je höher, desto weniger für Cloud-Sourcing in Bereichen der Kernkompetenz des Unternehmens geeignet. In anderen Bereichen kann es gerade das Ziel sein, solches Detailwissen nicht vorhalten zu müssen, sondern extern zu beziehen.	Grad der notwendigen Fachexpertise der Beteiligten.
	Spezifizität	Je höher, desto weniger für Cloud-Sourcing geeignet.	Individualität der Komponente gegenüber Wettbewerbern bzw. existierenden Lösungen am Markt.
	Reifegrad	Je höher der Reifegrad, desto einfacher sollte sich ein Cloud-Sourcing-Vorhaben gestalten. Jedoch: Je höher der Reifegrad, desto schwieriger ist eine Prozess- und Kostenverbesserung durch Cloud-Sourcing.	Anhand verschiedener Reifegradmodelle.
Kritikalität / Komplexität	Komplexität	Je höher, desto weniger für ein direktes Cloud-Sourcing ohne Redesign geeignet. Es kann jedoch ein strategisches Ziel sein, diese Komplexität auszulagern – dabei ist auf eine Vereinfachung der Schnittstellen zu achten. Je heterogener und individueller die Komponente, desto weniger für Cloud-Sourcing geeignet.	Anzahl der Verzweigungen und Rückkopplungen der Komponente mit den Unternehmensabläufen. Anzahl der Systeme, die den Prozess unterstützen.
	Schnittstellen	Je mehr, desto weniger für ein direktes Cloud-Sourcing ohne Redesign geeignet.	Anzahl der Schnittstellen zu anderen Komponenten.
	Risiken	Je höher das Risiko, desto weniger für Cloud-Sourcing geeignet.	Größe des Schadens bei Störung und Wahrscheinlichkeit einer Störung. Risikokompensierende Maßnahmen müssen berücksichtigt werden (Nettorisiko), (siehe 3.3.4).
	Verarbeitete Daten/-Informationen	Je kritischer die verarbeiteten Daten/ Informationen, desto weniger für Cloud-Sourcing geeignet.	Einstufung der Sicherheitsanforderungen für unterschiedliche Daten/Informations-kategorien.

Für eine zusammenfassende Bewertung der genannten Kriterien eignet sich ein Portfolio-Ansatz, bei dem die Betrachtungsgegenstände (z. B. IT-Applikationen) in einer zweidimensionalen Matrix bewertet werden. Auf Basis der Dimensionen und ihrer Ausprägungen lassen sich Geschäftsfeldstrategien bzw. -empfehlungen ableiten, die bei der Identifikation von Cloud-Sourcing-Kandidaten unterstützen. Bild 2 stellt einen entsprechenden Portfolio-Ansatz am Beispiel des Betrachtungsgegenstands IT-Applikation dar.

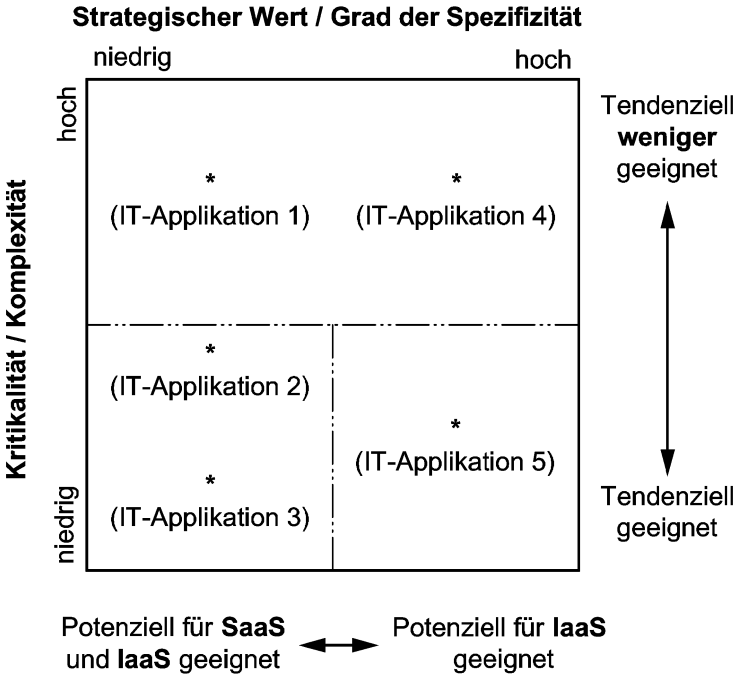

Bild 2 — Strategisches Portfolio für die Auswahl von Cloud-Sourcing-Kandidaten (in Anlehnung an [1])

Hieraus lässt sich eine erste Liste möglicher Cloud-Sourcing-Kandidaten ableiten. Für diese Cloud-Sourcing-Kandidaten ist es empfehlenswert, eine erste grobe Erhebung bestehender Angebote von Cloud-Service-Anbietern durchzuführen, die für die identifizierten Cloud-Sourcing-Kandidaten grundsätzlich als Lösung in Frage kommen. Ziel dieser Erhebung ist es, die Liste der Cloud-Sourcing-Kandidaten auf diejenigen Kandidaten zu reduzieren, für die überhaupt passende Lösungen am Markt existieren. Dieser Schritt liegt darin begründet, dass Cloud Services i. d. R. als hoch standardisierte Dienstleistungen angeboten werden, die ihre Vorteile am besten ausprägen, wenn die Services mit möglichst geringem Anpassungsbedarf zum Einsatz gebracht werden können. Die so gekürzte Liste der Cloud-Sourcing-Kandidaten stellt das zentrale Ergebnis dieser Phase dar. Die übrigen Cloud-Sourcing-Kandidaten können nach gängigen Vorgehensweisen des Cloud-Sourcing weiterverfolgt werden (z. B. DIN SPEC 1041).

Tabelle 6 — Verantwortlichkeiten bei der Prozess- und Serviceanalyse

Nr.	Aufgabe	Geschäftsleitung	Einkauf	Projektleiter	Fachbereich	Cloud-Service-Anbieter	Compliance-Beauftragter/ Betriebsrat	IT
1	**Erhebung der relevanten Komponenten**							
1.1	IT-gestützte Prozesse	I		A	R		I	R
1.2	IT-Applikationen	I		A	R		I	R
1.3	IT-Infrastruktur	I		A	R		I	R
2	**Identifikation von Cloud-Sourcing-Kandidaten**							
2.1	Festlegung der Bewertungskriterien	I		A	R		I	R
2.2	Durchführung der Bewertung	I		A	R		I	R

Tabelle 7 — Ergebnisdokumente der Phase „Prozess und Serviceanalyse“

ID	Dokument Bezeichnung	Dokument Beschreibung	Dienst-art	Dienst-modus
3.3 – A	Übersicht (IT-gestützter) Prozesse	Stellt alle wesentlichen Prozesstypen sowie deren Beziehungen untereinander dar, sowie die wesentlichen im Prozess verarbeiteten Geschäftsinformationen.	Alle	Alle
3.3 – B	Übersicht IT-Applikationen	Übersicht aller IT-Applikationen inkl. wesentlicher Schnittstellen sowie deren Zuordnung zu Prozessen, die von den Applikationen unterstützt werden.	Alle	Alle
3.3 – C	Übersicht IT-Infrastruktur	Gibt eine Übersicht der installierten Software, Daten(banken), System- und Netzwerkinfrastruktur, deren Beziehungen untereinander sowie Schnittstellen zu externen Systemen (IT Architektur). Die Übersicht enthält zudem eine Zuordnung zu den jeweiligen IT-Applikationen.	Alle	Alle
3.3 - D	Bewertungskriterien und -modell	Bewertung je Prozess anhand der gewählten Bewertungskriterien, der Gewichtung der Kriterien und den Ausprägungen der Kriterien. Je Betrachtungs-gegenstand erfolgt eine Einschätzung, inwiefern sie für Cloud-Sourcing an einen Cloud-Service-Anbieter geeignet sind.	Alle	Alle
3.3 – E	Cloud-Sourcing-Kandidaten	Liste identifizierter Cloud-Sourcing-Kandidaten als Resultat der Bewertung.	Alle	Alle

4.3.2 Auswahl Services

4.3.2.1 Wesentliche Fragen

- Welche Ausprägungen ergeben sich für die identifizierten Cloud-Sourcing-Kandidaten hinsichtlich Nutzen, Aufwand und Risiko einer Auslagerung an einen Cloud-Service-Anbieter?
- Welche der identifizierten Cloud-Sourcing-Kandidaten sollen als Cloud-Sourcing-Gegenstände für eine weitere Planung des Cloud-Sourcing-Vorhabens ausgewählt werden?

4.3.2.2 Beschreibung allgemein

Nachdem die Cloud-Sourcing-Kandidaten identifiziert wurden, sind diese einer genaueren Analyse zu unterziehen, insbesondere hinsichtlich des Nutzens, Aufwands und Risikos einer Auslagerung an einen Cloud-Service-Anbieter. Diese Analyse dient als Grundlage für eine spätere Entscheidung bezüglich der Fortführung des Cloud-Sourcing-Vorhabens.

Zunächst erfolgt eine detaillierte Analyse (Ist-Analyse) der identifizierten Cloud-Sourcing-Kandidaten. Ziel ist es, ein gemeinsames Verständnis für die Kandidaten zu entwickeln und zu dokumentieren. Die Ist-Analyse dient zudem dazu, zu entscheiden, ob identifizierte Cloud-Sourcing-Kandidaten ggf. in kleinere Komponenten zerlegt werden können, so dass ein Cloud-Sourcing-Kandidat nicht in Gänze ausgelagert werden muss. Es ist dann zu entscheiden, welche Komponenten ggf. im Unternehmen verbleiben können bzw. müssen. Hieraus lassen sich organisatorische (Prozessschnittstellen) und informationstechnische Schnittstellen (Systemschnittstellen) klar herausarbeiten und dokumentieren.

In einem nächsten Schritt ist zu bewerten, welches Nutzen-, Risiko- und Aufwandspotenzial für die einzelnen Cloud-Sourcing-Kandidaten bei einer Auslagerung an einen Cloud-Service-Anbieter besteht. Diese Bewertung sollte differenziert nach Dienstschicht/Betriebsmodell erfolgen, um zu belastbaren Einschätzungen zu gelangen. Insbesondere in Bezug auf die Dimensionen Nutzen und Aufwand sollten für eine fundierte Bewertung die existierenden Angebote je Cloud-Sourcing-Kandidat berücksichtigt werden (siehe 4.3.1). Der Grund hierfür ist die Tatsache, dass Cloud Services i. d. R. als hoch standardisierte Dienstleistungen angeboten werden. Die Höhe bzw. Ausprägung der entsprechenden Nutzen- bzw. Aufwandspotenziale ergeben sich somit überwiegend in Abhängigkeit vom Grad der notwendigen Anpassung bei Nutzung eines spezifischen Angebots eines Cloud-Service-Anbieters.

Grundsätzlich lassen sich für die drei Dimensionen Nutzen, Risiko und Aufwand Treiber identifizieren, anhand derer eine detaillierte Bewertung erfolgen kann [1].

Nutzen (Verbesserte Umsetzung fachlicher Anforderungen, verminderte Kosten):

- Effiziente Ressourcennutzung (z. B. bei Nutzungsschwankungen);
- Effizienterer Betrieb;
- Kosteneinsparungspotenzial;
- Standardisierungspotenzial.

Bei der Bewertung sollte der Umfang der Nutzung des Cloud-Sourcing-Kandidaten (z. B. Anzahl verarbeiteter Geschäftsvorfälle) und die damit verbundenen Kosten berücksichtigt werden.

Risiko (fachliche und technische Risiken des externen Bezugs des Services):

- Performance-Anforderungen;
- Datenvolumen (Speicher, Transfer);
- Verfügbarkeitsanforderungen;
- Technische Kompatibilität;
- Datenschutz und –sicherheit;
- Vendor Lock-in, Anpassbarkeit.

Aufwand (für die Migration an den Cloud-Service-Anbieter)

Die Bewertung einzelner Treiber kann anhand einer ordinalen Skala erfolgen (von gering bis hoch). Werden die Skalenwerte mit einem nummerischen Wert hinterlegt, lässt sich eine einzelne Dimension zusammenfassend bewerten (z. B. Mittelwert der jeweiligen Treiber). Diese Vorgehensweise ermöglicht eine erste Richtungsaussage für die einzelnen Cloud-Sourcing-Kandidaten. Für die zusammenfassende Bewertung der drei Dimensionen bietet sich dann wiederum ein Portfolio-Ansatz an (siehe Bild 3).

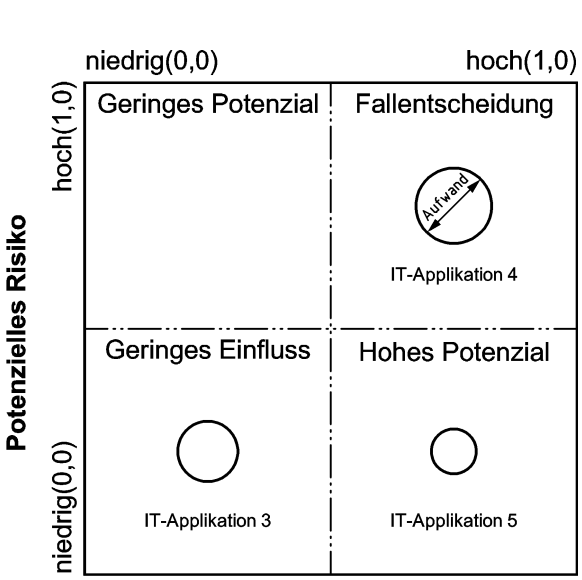

Bild 3 — Portfolio für die Auswahl von Cloud-Sourcing-Gegenständen (in Anlehnung an [1])

Folgende Geschäftsfeldstrategien lassen sich für die einzelnen Quadranten ableiten:

- Hohes Potenzial: Berücksichtigung als Cloud-Sourcing-Gegenstand und Priorisierung anhand des Aufwands;
- Fallunterscheidung: weitere Berücksichtigung als Cloud-Sourcing-Gegenstand in Abhängigkeit vom Aufwand;
- Geringer Einfluss: weitere Berücksichtigung als Cloud-Sourcing-Gegenstand in Abhängigkeit vom Aufwand, jedoch im Vergleich zu den zuvor beschriebenen zwei Quadranten mit geringerer Priorität;
- Geringes Potenzial: keine weitere Berücksichtigung.

Tabelle 8 — Verantwortlichkeiten bei der der Auswahl von Services

Nr.	Aufgabe	Geschäftsleitung	Einkauf	Projektleiter	Fachbereich	Cloud-Service-Anbieter	Compliance-Beauftragter/ Betriebsrat	IT
1	**Erhebung der Informationen zu Cloud-Sourcing-Kandidaten**							
1.1	Potenzieller Nutzen	I		A	R		I	R
1.2	Potenzielles Risiko	I		A	R		I	R
1.3	Aufwand	I		A	R		I	R
2	**Auswahl von Cloud-Sourcing-Gegenständen**							
2.1	Festlegung der Bewertungskriterien	I		A	R		I	R
2.2	Durchführung der Bewertung	I		A	R		I	R

Tabelle 9 — Ergebnisdokumente der Phase „Auswahl Services“

ID	Dokument Bezeichnung	Dokument Beschreibung	Dienst-art	Dienst-modus
3.3 – F	Prozess- und Systemschnittstellen	Erste Dokumentation zwingender Prozess- und Systemschnittstellen unter Berücksichtigung der auszulagernden und zurückzubehaltenden Komponenten der Cloud-Sourcing-Gegenstände. Grundlage sind die Dokumente aus der Prozess- und Serviceanalyse.	Alle	Alle
3.3 – G	Cloud-Sourcing-Gegenstände	Die Liste und Dokumentation der identifizierten Cloud-Sourcing-Gegenstände.	Alle	Alle

4.3.3 Detaillierung Services

4.3.3.1 Wesentliche Fragen

- Wie sollten Services beschrieben werden?
- Welcher Detaillierungsgrad wird zur Dokumentation von Services benötigt?
- Welchen Mehrwert bieten die einzelnen Services?
- Wie häufig und in welcher Ausprägung werden die Services aufgerufen?
- Welche Services werden von welchen Anwendergruppen aufgerufen?
- Welche IT-Services benötigen die Anwender in welcher Qualität?
- Welcher Standardisierungsgrad soll erreicht werden?
- Welche Leistungen erbringt die IT?
- Welche technischen Abhängigkeiten sind zu beachten?
- Wie viel kosten die Leistungen im Einzelnen?

4.3.3.2 Beschreibung allgemein

Die nachfolgenden Ausführungen besitzen nicht für jedes Cloud-Service-Projekt Gültigkeit. Die Notwendigkeit einer Vollständigen Durchführung diese Arbeitsschritts hängt von Art und Umfgang des Projekts ab. Kleine, übersichtliche Projekte, mit einem geringen Service-Umfang sowie geringer personeller Besetzung benötigen im Normalfall keinen vollständigen Servicekatalog. Es sollte jedoch darauf geachtet werden, dass ein allgemeines Verständnis über die Beschaffenheit der betrachteten Services existiert.

Das Vorgehen bei der Erstellung eines Servicekatalogs ist in fünf wesentliche Schritte unterteilt:

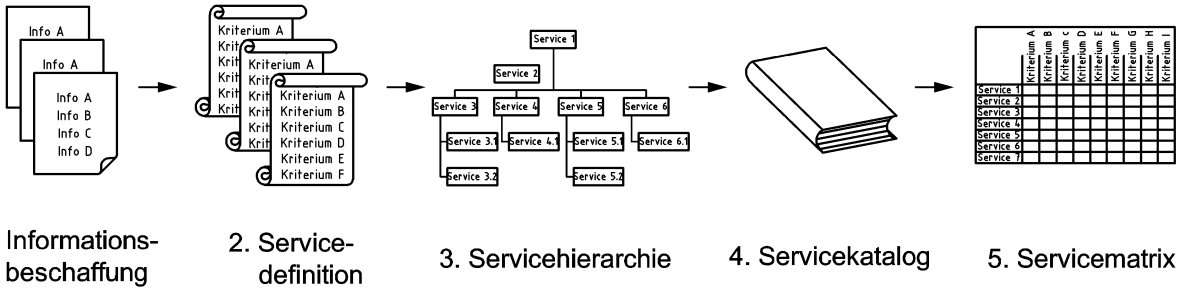

Bild 4 — Vorgehen bei der Erstellung eines Servicekatalogs

Die bisherigen Ausarbeitungen und Vorüberlegungen sollten als Basis der hier folgenden Vorgehensweise genutzt werden. Darüber hinaus sind in der Phase der **Informationsbeschaffung** alle nötigen Informationen aus den Fachabteilungen oder von den Fachanwendern zu beziehen.

Zu beachten ist, dass die zu detaillierenden Services dabei hinreichend abgrenzbar voneinander sein sollten. Bei der **Servicedefinition** sollten alle Ausprägungen von Geschäftsvorfällen, die eine Inanspruchnahme des Services nach sich ziehen, durch die Servicebeschreibung abgedeckt sein. Es ist darauf zu achten, dass es sich bei den Services um Regeldienstleistungen mit Wiederholungscharakter handeln sollte und weniger um Services mit umfangreichem Projektcharakter. Weiterhin ist darauf zu achten, dass es sich nicht um reine Produktbeschreibungen aus IT-Sicht (z. B. Speichervolumen oder CPU-Stunden), sondern vielmehr um vom Nutzer wahrnehmbare Services handelt. Die Services sollten dabei nach Möglichkeit nicht technikorientiert beschrieben werden. Auch um die spätere Nutzbarkeit und vor allem die Akzeptanz des Servicekataloges sicherzustellen, empfiehlt es sich, Services stets aus Nutzersicht zu definieren und sich dabei eng an den Anforderungen der Anwender zu orientieren. Nur, wenn die Nutzer bereits in die Gestaltung der einzelnen Leistungen mit einbezogen werden, ist gewährleistet, dass die Services in Umfang und Qualität deren Erwartungen entsprechen. Um die Akzeptanz der Services bei den Anwendern zu sichern, sollte darauf folgend eine Abstimmung mit den betroffenen Fachabteilungen (sofern im Unternehmen existent) erfolgen. Die Anzahl und Granularität der zu definierenden Services sollte dem Prinzip „so viel wie nötig, so wenig wie möglich“ entsprechen.

Aufbauend auf den erhobenen und definierten Services ist es möglich einen Überblick über die **Servicehierarchie** zu erstellen. Die Servicehierarchie setzt die einzelnen definierten Services in Verbindung zueinander. Für die Erhebung der Servicehierarchie kann u. a. die in 4.3.2 erstellte Übersicht über die Prozesse- und Systemschnittstellen als Grundlage dienen. Die zugrunde liegenden – und teilweise von mehreren Services gleichzeitig genutzten – Basis-Infrastrukturdienste (z. B. Server, Netzwerk) werden in der Regel in Form von Servicekomponenten dargestellt. Sie bilden die Grundlage für die Bereitstellung der von den Anwendern in Anspruch genommenen Services. Gegenseitige Abhängigkeiten sind zu berücksichtigen, so kann es sein, dass z. B. eine Servicekomponente eine andere voraussetzt. Die Zusammensetzung der Services aus verschiedenen Servicekomponenten spielt auch im Rahmen der späteren Cloud-Service-Anbieter Auswahl eine entscheidende Rolle. Zum einen sind solche Abhängigkeiten zu berücksichtigen und vom Cloud-Service-Anbieter zu unterstützten, zum anderen können diese maßgeblich die entstehenden Kosten beeinflussen. Der Servicepreis errechnet sich – zumindest teilweise - aus den Preisen der zugrunde liegenden Servicekomponenten. Services, welche grundsätzlich vom Nutzer in Kombination abgerufen werden, lassen sich zu Service-Bundles zusammenfassen. Dies erleichtert den späteren Abgleich des Servicekatalogs mit dem Angebot der Cloud-Service-Anbieter. Das Ziel des zu erstellenden **Servicekatalogs** sollte die Bereitstellung relevanter Informationen aller in 3.3.2 ausgewählten Services sein: Im Servicekatalog sind die Basisinformationen modelliert, die für die Bestellung, den Betrieb und die Auswertung der Services

erforderlich sind. Das Ergebnis bildet eine strukturierte und standardisierte Definition des Serviceportfolios eines Unternehmens. Abschließend besteht die Möglichkeit der Erstellung einer **Servicematrix**. Sie spiegelt alle Informationen des Servicekatalogs in übersichtlicher Weise in Matrixform wieder. Dies kann vor allem bei dem später folgendem Abgleich zwischen dem Angebot der Cloud-Service-Anbieter und dem Servicekatalog eine erheblich Reduktion des Arbeitsaufwandes bedeuten.

Die Vorteile des hier beschriebenen Vorgehens sind mannigfaltig. Erstens wird die Transparenz über die geleisteten IT-Services deutlich erhöht. Zweitens wird eine klare Kalkulationsbasis geschaffen, da jedem IT-Service die erforderlichen personellen und technischen Ressourcen zugeordnet werden können. Auf diese Weise wird nicht nur die Ressourcenplanung erheblich erleichtert, vielmehr lassen sich auch Kostentreiber sowie Ansatzpunkte zur Optimierung identifizieren. Darüber hinaus kann der Servicekatalog als Basis für eine Optimierung bestehender Prozesse herangezogen werden. Drittens werden alle aktiven IT-Services detailliert und nach einem einheitlichen Schema beschrieben. Die Fachabteilungen kommen im Zuge dieser Dokumentation nicht umhin, ihre Anforderungen an die IT genau zu spezifizieren. Derart lassen sich Kommunikations- und Verständnisprobleme zwischen Anwendern und IT vermeiden.

Die Gliederung des Serviceskatalogs sollte mindestens die folgenden Elemente beinhalten:

a) **Name:** Zur schnellen und eindeutigen Identifikation sollte jeder Service einen Namen erhalten.

b) **Ziel**: Jeder Service muss einem klaren Ziel dienen. Dieses ist schriftlich zu fixieren und dient später als wesentliches inhaltliches Abgleichkriterium mit dem Angebot des Cloud-Service-Anbieters.

c) **Zusammenfassende Beschreibung:** Die Beschreibung findet auf einem hohen Abstraktionsniveau statt und muss für den Nutzer leicht verständlich sein. Es muss eine klare Differenzierung zwischen technischen Aspekten und der Geschäftstätigkeit, welche durch den Service unterstützt werden stattfinden (z. B. ist klar zwischen dem IT-System „Entgeldabrechnung“ und dem Service „Personalmanagement“ zu unterscheiden).

d) **Anforderung**: Es sind Qualitätsparameter wie z. B. Reaktions- und Lösungszeiten, Verfügbarkeit, Betriebs-, Support- und Bereitschaftszeiten zu definieren.

e) **Abhängigkeiten**: Einordnung des jeweils beschriebenen Services auf Basis der zuvor erstellten Servicehierarchie. Dies kann zu besseren Übersichtlichkeit auch grafisch geschehen. Gerade die Fachabteilungen erhalten durch dieses Vorgehen einen guten Gesamtüberblick.

f) **Ressourcen**: Jeder Service benötigt Ressourcen unterschiedlichster Art. Zum einen sind dies Human-Ressourcen zum anderen finanzielle, organisatorische, technologische und/oder physische Ressourcen. Diese Ressourcen müssen jeweils den Services zugeordnet werden.

g) **Reifegrade**: Der Service sollte auf Basis eines der gängigen Maturity Models z. B. CMMI (en: Capability Maturity Model Integration) eingestuft werden. Dieses Vorgehen birgt eine Vielzahl von Vorteilen, wie z. B. klar definierte Ziele, weitere vorgegebene konkrete Beschreibungselemente und eine einheitliche Begriffswelt.

h) **Kosten**: Soweit für die einzelnen Services berechenbar, sind die Kosten zu ermitteln. Dies führt zu einem besseren Verständnis der Kostentreiber in einem Unternehmen. Darüber hinaus ist es notwendig ein Verständnis der ungefähren Kosten je Service für die Verhandlungen mit Cloud-Service-Anbietern zu haben bzw. um deren Angebot bewerten zu können.

Tabelle 10 — Verantwortlichkeiten bei der Detaillierung von Services

Nr.	Aufgabe	Geschäftsleitung	Einkauf	Projektleiter	Fachbereich	Cloud-Service-Anbieter	Compliance-Beauftragter/ Betriebsrat	IT
1	Informationsbeschaffung			C	R	A		
2	Servicedefinition	I		C	R	A		
3	Servicehierarchie ermitteln			RA		I		
4	Erstellen Servicekatalog			RA		I		
5	Abnahme Servicekatalog	A		R	I	I		
6	Erstellen Servicematrix	A	I	R		I		

Tabelle 11 — Ergebnisdokumente der Phase „Detaillierung Services“

Dokument ID	Dokument Bezeichnung	Dokument Beschreibung	Dienstschicht	Betriebs-modell
3.3 – H	Servicekatalog	Verzeichnis Services und deren Eigenschaften	IaaS PaaS SaaS	Private Public Hybrid Community
3.3 – I	Serivcematrix	Übersicht aller Services in Matrix-darstellung	IaaS PaaS SaaS	Private Public Hybrid Community

4.3.4 Risikoanalyse der Services

4.3.4.1 Wesentliche Fragen

- Welche Services haben ein besonderes Risikopotential?
- Welche zusätzlichen Risiken ergeben sich für einzelne Services durch die Auslagerung in die Cloud?
- Welche Risiken für einzelne Services werden durch die Auslagerung in die Cloud verringert?
- Wie kann ggf. erhöhten Risiken durch zusätzliche Maßnahmen begegnet werden?

4.3.4.2 Beschreibung allgemein

Durch das Auslagern verschiedener Services begibt sich der Cloud-Sourcing-Geber in ein Abhängigkeitsverhältnis zum Cloud-Service-Anbieter. Der Cloud-Sourcing-Geber sollte sich daher verdeutlichen, welche Risiken mit der Auslagerung von Prozessen verbunden sind. Für jeden ausgelagerten Service sollte deshalb festgehalten werden, welche Folge eine Nicht- oder verzögerte Erbringung bzw. eine unzureichende Erbringung des Dienstes hätte.

Die Risikoanalyse kann grundsätzlich in die folgenden Schritte unterteilt werden:

1) Identifikation von Risiken;

2) Analyse und Bewertung der Risiken;

3) Strategien und Maßnahmen zur Begegnung der Risiken (Risikoabwehr, Risikoreduzierung);

4) Abschätzung des Restrisikos.

Schritte 1 und 2 sind unabhängig vom später ausgewählten Cloud-Service-Anbieter während die Schritte 3 und 4 in Abhängigkeit von der tatsächlich vom Cloud-Service-Anbieter erbrachten Leistung stehen. Die Ergebnisse der Schritte 1 und 2 fließen deshalb in die Anforderungen an den Cloud Service ein.

Risiken beim Cloud-Sourcing an Cloud-Service-Anbieter können in folgende Risikoarten unterschieden werden:

Organisatorische Risiken

— Abhängigkeit vom Anbieter

— Durch proprietäre oder nicht vorhandene Schnittstellen oder Formate und spezielle Anpassungen kann sich eine Abhängigkeit vom Cloud-Service-Anbieter ergeben, die einen Wechsel zu einem anderen Anbieter oder zurück zu einem internen Betrieb erschweren oder gar unmöglich machen kann (gemeinhin wird dieser Sachverhalt als „Vendor-Lock-In“ Effekt bezeichnet).

— Unvorhergesehener Service-Stopp

— Aus verschiedenen Gründen kann es zu einem unvorhergesehenen und vom Cloud-Sourcing-Geber nicht beeinflussbaren Service-Stopp kommen, z. B. durch Insolvenz des Cloud-Service-Anbieters.

— Kontrollverlust

— Da Betrieb und Kontrolle der technischen Ressourcen weitgehend oder vollständig in der Hand des Cloud-Service-Anbieters liegen, kann die Einhaltung von Vorgaben im Detail nicht oder nur schwer kontrolliert werden.

— Fehlendes internes Know-How

— Fehlendes oder unzureichendes Know-How kann dazu führen, dass ungeeignete Anbieter ausgewählt, Fehler bei der Implementierung gemacht oder andere Fehler begangen werden, welche die Sicherheit des ausgelagerten Prozesses negativ beeinflussen.

— Fehlende Flexibilität der Cloud Services

— Fehlende Flexibilität kann dazu führen, dass Lastspitzen nicht aufgefangen werden können, benötigte zusätzliche Leistungen nicht zur Verfügung gestellt werden können oder nicht mehr benötigte Leistungen unnötige Kosten verursachen.

Rechtliche Risiken und Compliance

— Nichteinhaltung rechtlicher Vorgaben

— Die Nichteinhaltung rechtlicher Vorgaben kann zu Strafen, Schadenersatzforderungen Dritter und Reputationsschäden führen, möglicherweise auch zur Nichtigkeit von Teilen des geschlossenen Vertrags oder des Vertrags als Ganzem.

— Anwendbares ausländisches Recht

— Anwendbares ausländisches Recht kann dazu führen, dass geschlossene Vereinbarungen von vorneherein mit rechtlichen Vorgaben am Sitz des Cloud-Sourcing-Gebers kollidieren oder, z. B. bei Änderungen des ausländischen Rechts, dies zu einem späteren Zeitpunkt passiert.

- Nichteinhaltung sonstiger (interner) Vorgaben

- Die Nichteinhaltung sonstiger Vorgaben kann Beeinträchtigungen z. B. bei benachbarten Prozessen hervorrufen, wodurch diese nicht mehr funktionieren oder beispielsweise Zertifizierungen ungültig werden.

- Ungeeignete Verträge

- Ungeeignete Verträge können gravierende Regelungslücken enthalten oder durch Überregulierung dazu führen, dass Prozesse nicht wie gewollt durchführbar sind.

- Nichtdurchsetzbarkeit von Forderungen

- In einigen Fällen besteht keine rechtliche Handhabe gegenüber Cloud-Service-Anbietern im Ausland.

Technische und betriebliche Risiken

- Mangelnde Isolation der Daten

- Isolationsversagen führt dazu, dass Daten eines Cloud-Anwenders in den Zugriffsbereich eines anderen Cloud-Anwenders geraten.

- Kompromittierte Interfaces

- Unzureichend geschützte oder kompromittierte Interfaces zu Cloud Services ermöglichen unbefugten Dritten den Zugriff zu Anwendungen und Daten.

- Unsichere oder unvollständige Datenlöschung

- Nicht vollständig gelöschte Daten erhöhen das Risiko, dass diese Daten in die Hände Unbefugter geraten. Unvollständige Datenlöschung kann auch einen Verstoß gegen rechtliche Vorgaben darstellen.

- Mangelnde Verfügbarkeit der Services

- Unzureichende Netz- oder Service-Verfügbarkeit führt dazu, dass Prozesse nicht wie geplant ablaufen und dadurch zusätzliche Kosten verursachen.

- Feindselige Mitarbeiter

- Cloud-Architekturen erfordern zur Pflege Benutzerrollen mit einer Vielzahl an Rechten. Mit solchen Rollen ausgestattete feindselige Benutzer können unter Umständen Manipulation an Daten vornehmen, diese an unbefugte Dritte weiterleiten oder die Verfügbarkeit der Services stören.

Cloud-Service-Anbieter sollten darlegen, wie sie den identifizierten Risiken begegnen, bzw. welche Werkzeuge sie dem Cloud-Sourcing-Geber zur Verfügung stellen, damit er seinerseits dem Risiko begegnen kann. Dabei werden normalerweise verschiedene Cloud-Service-Anbieter verschiedene Strategien und Werkzeuge zur Begegnung der Risiken zur Verfügung stellen. Ein Vergleich der verschiedenen Strategien und Werkzeuge und die Abschätzung des jeweiligen Restrisikos fließt dann in die Entscheidungsfindung zur Auswahl des Cloud Services ein.

Zur Analyse und Bewertung von Risiken eignet sich allgemein eine Matrix, die Eintrittswahrscheinlichkeit und Auswirkungen des Risikos aufzeigt. Eine genaue Anleitung zu Risikoanalyse und Risikomanagement im IT-Bereich findet sich u. a. in der Norm ISO/IEC 27005.

Tabelle 12 — Verantwortlichkeiten bei der Risikoanalyse der Services

Nr.	Aufgabe	Geschäftsleitung	Einkauf	Projektleiter	Fachbereich	Cloud-Service-Anbieter	Compliance-Beauftragter/ Betriebsrat	IT
1	Identifikation von Risiken	A		R	C	C	C	C
2	Analyse und Bewertung der Risiken	A		R	C	C	C	C
3	Strategien und Maßnahmen zur Begegnung der Risiken (Risikoabwehr, Risikoreduzierung)			A	C	R	C	C
4	Abschätzung des Restrisikos	A		R	C	C	C	C

4.4 Cloud-Service-Anbieterauswahl

4.4.1 Erstellung Anforderungskatalog

4.4.1.1 Wesentliche Fragen

- Wie ist das Vorgehen zum Erstellen eines Anforderungskatalogs?
- Welche Anforderungen sind bei der Erstellung zu berücksichtigen?
- Erfüllt der Cloud Service die grundlegenden Complianceanforderungen?
- Sind die Servicezusagen (SLA) angemessen in Bezug auf die Anforderungen der Nutzer?
- Besteht Transparenz über die Art und Örtlichkeit der Datenverarbeitung und der beteiligten Leistungserbringer?
- Existieren Nachweise zur Umsetzung von Datenschutz- und Sicherheitsmaßnahmen?

4.4.1.2 Beschreibung allgemein

In dieser Phase soll für die identifizierten Cloud-Sourcing-Gegenstände ein Anforderungskatalog zusammengestellt werden, anhand dessen die spätere Cloud-Service-Anbieter-Auswahl strukturiert wird. Die Unterkapitel sollen eine Hilfestellung geben, welche Anforderungen ggf. zu berücksichtigen sind.

Üblicherweise orientieren sich die meisten Firmen bereits an einem oder mehreren IT-Steuerungsmodellen. Sehr verbreitet sind nachfolgende Beispiele:

- ISO 38500 (Corporate Governance of Information Technology),
- ITIL (Information Technology Infrastructure Library™ / IT Service Management),
- CoBIT (A Business Framework for the Governance and Management of Enterprise IT),

welche in der Umsetzung durch generelle Projektmanagementmethoden wie

- ISO 21500 (Leitfaden zum Projektmanagement),
- ICB3 (International Competency Baseline) der GPM,
- Prince2 (Projects in Controlled Environments) des OGC,
- PMBoK (Project Management Body of Knowledge) der PMI

begleitet werden.

Die vorgenannten Modelle enthalten u.a. umfassende Empfehlungen und Checklisten für ein methodisches Vorgehen von IT-Beschaffungsvorhaben.

In Hinblick auf die spätere Auswahl ist es empfehlenswert, die Auswahlkriterien bereits bei der Formulierung des Anforderungskataloges im Blick zu behalten. Üblich ist die Aufteilung in

- funktionale Anforderungen: Funktionen und Leistungen, die benötigt werden
- strategische Anforderungen: z. B. perspektivische Technologie-Auswahl, Berücksichtigung geplanter Entwicklungen, angestrebte Partnerschaften oder Administrationsvereinfachungen
- wirtschaftliche Anforderungen: Anschaffungs-, Nutzungs-, Schulungs-, Administrations, Überführungs-, Rückmigrations- und sonstige Kosten.

Funktional sollte zwischen „Muss-, Soll- und Könnte-Anforderungen“ unterschieden werden (Siehe hierzu Abschnitt 4.4.3).

Um Klarheit über den angebotenen Leistungsumfang zu bekommen, sollten Anbieter bei Befragungen dazu aufgefordert werden, Leistungen so zu kennzeichnen oder darzustellen, dass eindeutig erkennbar wird, ob eine Funktion oder Leistung standardmäßig zur Verfügung steht, eine kostenpflichtige Option darstellt, im Rahmen einer kostenpflichtigen Einstellung erreicht wird oder erst noch zu entwickeln ist.

4.4.1.3 Compliance-Aspekte

Vor der Nutzung eines Cloud-basierten Services ist zu prüfen, ob eine Nutzung überhaupt zulässig ist. Hierbei sind die jeweiligen nationalen und ggf. internationalen gesetzlichen Rahmenbedingungen zu prüfen. In Deutschland ergeben sich Einschränkungen unter anderem aus folgenden Rechtsbereichen:

- Datenschutzgesetz: Die Weitergabe von personenbezogenen Daten an Dritte wird durch die Datenschutzgesetze stark eingeschränkt und erfordert in der Regel spezifische vertragliche Vereinbarungen mit den Auftragsdatenverarbeitern – im Falle einer Cloud-Nutzung also mit dem entsprechenden Cloud-Service-Anbieter. Die Bereitschaft des Cloud-Service-Anbieters, entsprechende Vertragsklauseln zu vereinbaren, ist im Vorfeld zu prüfen. Pauschale AGB sind hierfür nicht ausreichend. Außerdem steht der Cloud-Sourcing-Geber in der Verpflichtung, regelmäßig die vorgenommenen technisch-organisatorischen Maßnahmen des Auftragsdatenverarbeiters zu prüfen oder prüfen zu lassen. Zertifikate unabhängiger Prüforganisationen sind dabei ein übliches Vorgehen, um den Aufwand für beide Seiten gering zu halten.
- HGB / AO / Steuerrecht: Das ausschließliche Vorhalten steuerrechtlich relevanter Daten im Ausland ist in einigen Ländern wie auch in Deutschland unzulässig. Die Bereitstellung entsprechender Daten im Inland - ggf. in Kopie - muss in diesen Fällen sichergestellt werden. Generell muss vertraglich geklärt werden, dass zu jeder Zeit ein uneingeschränkter Zugang zu den Daten für Prüfungen durch die Steuerbehörden möglich ist.
- Exportrecht: Das Exportrecht regelt nicht nur den Export von Waren, sondern umfasst auch Informationen im Zusammenhang mit entsprechenden Waren. Die Übertragung von Dokumenten und andere Formen von Export-sensiblen Informationen oder Wissen an Cloud-Service-Anbieter, die Speicher oder Verarbeitungskapazitäten im Ausland nutzen, kann deshalb zu entsprechenden Rechtsverstößen führen.
- Kaufmännische Sorgfaltspflichten: Die kaufmännische Sorgfaltspflicht erfordert es, Risiken für das Unternehmen gering zu halten und drohenden Schaden vom Unternehmen abzuwenden. Deshalb ist generell zu prüfen, welchen Wert die in der Cloud verarbeiteten Daten für das Unternehmen haben bzw. ob die mit der Nutzung des Cloud Service verbundenen Risiken (wie z. B. Verlust etc., siehe 4.3.4) in Bezug auf die angebotenen Sicherheitsverfahren akzeptabel und angemessen sind.
- Ableitung von Soll-Vorgaben auf Basis der Compliance-Aspekte in Bezug auf Rechenzentrum-Ort des Cloud-Service-Anbieters (Region), Redundanz des Betriebs und Monitoringmöglichkeiten.
- Die Angemessenheit von Maßnahmen für die Vermeidung oder Reduzierung von Compliance-Verstößen folgt üblicherweise dem Vorgehen einer Risiko-Prüfung, wie sie z. B. in der ISO 31000 umfassend beschreiben wird (siehe 4.3.4).

4.4.1.4 Performance-Aspekte

- Ableitung nicht-funktionaler Anforderungen mit Performance-Bezug.
- Ableitung von Soll-Vorgaben in Bezug auf Performance-Anforderungen in den Dimensionen zugesicherte Round-Trip-Zeit, Netzlatenzen, Datendurchsatz etc.
- In Bezug auf die Servicezusagen (SLA) sollte die Einhaltung der Verfügbarkeiten und der Performance des Cloud-Services durch kontinuierliche Überwachung (Monitoring), Berichtsfunktionen und aktive Benachrichtigungen bei besonderen Vorfällen gewährleistet sein. Diese Berichtsfunktion gilt ab Eingangspunkt des Cloud-Services um eine Abgrenzung zu Performanceverlusten in der vorgelagerten Netzverbindung des Anwenders zum Eingangspunkt zu ermöglichen.

4.4.1.5 Wirtschaftlichkeit (Preis- und Kostenmodell)

- Die Abrechnungsmodelle sollten durchgängig nachvollziehbar sein und die jeweilige Abrechnungseinheit (pro Anwender und Zeit, Übertragungsvolumen, Speichervolumen, Prozessortyp) explizit angeben.
- Jegliche Zusatzkosten, die nicht Bestandteil der Servicekalkulation sind, sollten preislich festgelegt sein, bzw. die zugrunde liegenden Verrechnungseinheiten und die Grundlage der Aufwandsberechnung angegeben werden.
- Bei langfristigen Verträgen sollte ein Tarifwechsel in einen günstigeren Preis bei vergleichbarer Leistung möglich sein, sofern dieser vom Anbieter allgemein angeboten wird.

4.4.1.6 Sicherheit

In Abhängigkeit von der Art der Nutzung eines Cloud-Services ergeben sich unterschiedliche Sicherheitsanforderungen. Diese werden in zahlreichen Studien und Leitfäden von BITKOM, EuroCloud, ENISA, Cloud Security Alliance (CSA) und des Bundesamts für Sicherheit in der Informationstechnik (BSI) erläutert [2], [3], [4], [5], [6], [7], [8].

Zur Einhaltung grundlegender Sicherheitsanforderungen hat der Anbieter einen Nachweis für die Umsetzung eines effizienten Managements der Informationssicherheit (Information Security Management System, ISMS) zu erbringen. Das BSI empfiehlt dabei eine Orientierung an DIN ISO/IEC 27001 und DIN ISO/IEC 27002 oder am BSI-Standard 100-2 zur IT-Grundschutz-Vorgehensweise.

Hierbei werden auch konkrete Anforderungen in den Bereichen

- Patch- und Änderungsmanagement
- Konfigurationsmanagement
- Netzmanagement
- System Management
- Application Management
- Reporting

definiert.

4.4.1.7 Transparenz

Die Vernetzung der Cloud-Service Erbringung ermöglicht im Extremfall die komplette Anonymisierung der an der Leistungserbringung beteiligten Partner, der Datenstandorte und des anzuwendenden Rechts bei eventuellen Auseinandersetzungen. Daher ist es im Vorfeld dringend erforderlich, zu den folgenden Anforderungen eine verbindliche Klärung herbeizuführen, sofern für die Nutzung konkrete Compliance-Vorgaben existieren:

- Bekanntgabe aller an der direkten Leistungserbringung beteiligten Unternehmen
- Standorte der Datenspeicherung (postalische Adresse)

- Nachweis der Erlaubnis zur Bereitstellung des Dienstes, sofern hierzu Lizenzen Dritter zur Anwendung kommen
- Anwendbares Recht bei Auseinandersetzungen
- Nachweis der Subunternehmervereinbarungen zur Auftragsdatenverarbeitung, sofern es um personenbezogene Datenverarbeitung im Sinne des BDSG handelt.

4.4.1.8 Skalierbarkeit

Eine wesentliche Charakteristik von Cloud-Services ist die flexible Skalierung der Inanspruchnahme (sowohl Erweiterung als auch Reduzierung). Für beide Varianten der Anpassung kann es vertragliche Einschränkungen geben, die in Bezug auf die gedachten Nutzungsmöglichkeiten zu prüfen sind. Ergänzend sind die Provisionierungszeiten für Änderungen zu prüfen und sollten idealerweise ohne zusätzliche Administration beim Anbieter ermöglicht werden („self provisioning“).In Bezug auf das Datenvolumen ist es sinnvoll eine Datenbereinigung vor der eigentlichen Anbieterauswahl durchzuführen. Folgende Punkte sind dabei zu berücksichtigen:

- Feststellen, in wie weit eine Bereinigung beim Start die Nutzung günstigerer Angebote ermöglicht
- Für den Fall, dass der Cloud-Service-Anbieter Mengenlimits definiert hat:
  - Feststellen, ob der Cloud Service aufgrund der aktuellen IT-Mengen bzw. unter Berücksichtigung eines vorhersehbaren Volumenwachstums interessant ist.
  - Klärung, ob die Prozesse wirklich dieses Datenvolumen benötigen. Identifikation von Alternativen zur Speicherung und Archivierung der Daten.
  - Vorbereitung und Planung, wie die jetzige Situation verändert werden soll und auf welche Weise die Daten – wenn notwendig – zu bereinigen sind. Projektmäßige Planung der weiteren Schritte.

Generell gilt: ein geringeres Datenvolumen bedeutet, eine weniger aufwendige Migration.

4.4.1.9 Integrations- und Migrationsfähigkeit

Um ein Vendor-Lock-In zu vermeiden, sollte darauf geachtet werden, dass das existierende Cloud-Angebot möglichst gut mit anderen Anwendungen integriert werden kann und die Daten und ggf. auch die Logik selbst gepflegter Anwendungsmodule auf Basis des Angebots wieder exportiert werden können. Um ein Verlassen eines Anbieters möglichst weitreichend abzusichern, sollte vertraglich geregelt werden, welche Daten und ggf. welche Betriebslogiken mit Beendigung des Vertrages durch den Cloud-Service-Anbieter zur Verfügung zu stellen sind. Dies beinhaltet ggf. auch die Formate und Dokumentationen sowie etwaige Unterstützungsleistungen sowie Schadensersatzleistungen bei Nichterfüllung. Außerdem sollten entsprechende Vorsorgen auch für den Insolvenzfall geregelt werden. So kann es zum Beispiel sinnvoll sein, ein regelmäßiges Aushändigen von Zwischensicherungen des eigenen Datenbestandes vertraglich zu vereinbaren.

4.4.1.10 Kontrollmöglichkeiten

Die Möglichkeit zur Überprüfung der vertraglichen Zusicherungen und Einhaltung der im Service Level Agreement (SLA) definierten Leistungen und deren Qualität sollte generell gegeben sein. Sofern es sich um den Zweck der Auftragsdatenverarbeitung im Sinne des BDSG §11 handelt, ist die Gewährung von Kontrollen verpflichtend und sollte direkt im Vertrag zur Auftragsdatenverarbeitung geregelt werden. Die damit verbundenen Aufwände beim Cloud-Service-Anbieter sind konkret in der Preisliste zu benennen.

Individuelle Kontrollen können ggf. durch Nachweis adäquater Audits oder Zertifizierungen hinsichtlich der Kontrollziele vermieden werden.

Tabelle 13 — Verantwortlichkeiten bei der Erstellung eines Servicekatalogs

Nr.	Aufgabe	Geschäftsleitung	Einkauf	Projektleiter	Fachbereich	Cloud-Service-Anbieter	Compliance-Beauftragter/-Betriebsrat	IT
1	**Compliance**							
1.1	Recht	I		A	R			
1.2	Datenschutz	I		A		S	R	
1.3	Vertrag	I	A				R	
2	**Sicherheit**							
2.1	Technische und organisatorische Maßnahmen			A			I	R
2.2	Überwachungsfunktionen (Service Monitoring)			A		S	I	R
3	**Datenübergabe**							
3.1	Archivierung			A	C			R
3.2	Rückübertragung			A	C	S		R
4	**Kontrollfunktionen**							
4.1	Rechenzentrum			A		S		R
4.2	Leistungszusagen			A	R			S
4.3	Datenschutzanforderungen			A		S	R	
5	**Erfüllung der funktionalen Serviceanforderungen**		**A**	**R**	**S**			**S**

4.4.2 Spezifikation des Betriebsmodells

4.4.2.1 Wesentliche Fragen

— Welche Anforderungen sind bei den verschiedenen Betriebsmodellen zu berücksichtigen?

— Wie kann eine Kombination verschiedener Dienstschichten und Betriebsmodelle realisiert werden?

4.4.2.2 Beschreibung allgemein

4.4.2.2.1 Anforderungen für den Eigenbetrieb (Private Cloud)

Der Betrieb der eigenen Cloud-Infrastruktur bedingt eine entsprechende organisatorische Aufstellung und die Schaffung entsprechender Arbeitsgruppen. Als besondere Herausforderungen sind folgende Punkte hervorzuheben:

— Eigene Cloud-Infrastrukturen sind häufig mit der Einführung des sogenannten Fabric Computings gekoppelt. Fabrics kombinieren Server, Netzwerk und Storage in einer abgestimmten Einheit. In den Organisationen sind aber die Bereiche häufig auf verschiedene Abteilungen gespalten, so dass ein der Technologie folgender Betriebsablauf gewährleistet ist. Eine Angleichung der Organisation an die technische Realität ist somit unumgänglich.

— Meist ist die Schaffung einer semantischen Darstellung der Infrastruktur zur Unterstützung der Fehlersuche notwendig. Die eigene Cloud basiert auf einer durchgängigen Virtualisierung von Netzwerk, Storage, Servern sowie ggf. Desktops und Applikationen. Wenn die Zusammenhänge, die sich permanent ändern können, nicht für den Cloud-Service-Anbieter ersichtlich sind, wird die Fehlersuche nahezu unmöglich.

- Der Aufbau eines eigenen Scripting Know-Hows: Auch wenn die am Markt gängigen Lösungen viele Automatisierungsabläufe integriert haben, ist das eigene Wissen für die Abbildung angepasster Prozesse in der Automatisierung unumgänglich.
- Das Ziel der eigenen Cloud-Infrastruktur muss die Abwicklung von Anforderungen ohne den Eingriff von Personen mit Ausnahme von Genehmigungen sein. Der so genannte „Zero-Touch-Ansatz“ – also die Bereitstellung von Funktionalitäten ohne menschliche Eingriffe - sorgt für eine Kalkulierbarkeit von Prozessdauer und Prozesskosten und ist somit ein fester Bestandteil im Servicekatalog.

Unternehmen, die diese technischen Anforderungen nicht erfüllen können, werden sich beim Aufbau und Betrieb einer Private Cloud sehr schwer tun und um die dauerhafte Anmietung von externen Dienstleistern – ob mit oder ohne Betriebsverantwortung – nicht herumkommen.

4.4.2.2.2 Anforderungen für den Fremdbetrieb (Public Clouds)

Die Nutzung der populären Public Cloud Services internationaler Anbieter zur Bereitstellung von Infrastrukturen findet eine zunehmende Verbreitung. Dabei stellt sich die Frage, wer hier in welcher Betriebsverantwortung ist. Denn die meisten Betreiber sorgen sich lediglich um das Starten des Servers und die Integration des Datensicherungs- und –wiederherstellungsprozesses. Der eigentliche Betrieb der Server verbleibt beim Auftraggeber. Dazu gehören Aufgaben wie z. B.:

- Überwachung der Leistungsdaten;
- Überwachung von Fehler-Ereignissen;
- Richtigkeit des Dimensionierung aufgrund der Kapazitätsplanung;
- Einspielen von Security-Patches;
- Sicherstellung der Netzwerkverbindung.

Bei der Nutzung des Fremdbetriebes durch einfach buchbare Infrastrukturen ist die Frage des Betriebes im Sinne der Pflege einer virtuellen Instanz klar zu regeln. Auch in vielen Cloud-Angeboten verbleibt die Verantwortung beim Auftraggeber.

4.4.2.2.3 Anforderungen für Hybrid Clouds

Während viele Diskussionen zum Thema Cloud Computing eine reine Public-Cloud-Lösung zum Inhalt haben, existieren diverse Kombinationsmöglichkeiten von Eigenbetrieb und der Auslagerung einzelner virtueller Maschinen oder Applikationen in die Cloud. Je nach Kriterien entsprechend 3.4.3 „Ableitung eines Kriterienkataloges“ kann die Optimierung der eigenen Infrastruktur zur Abdeckung aller Cloud-Eigenschaften nach 2 „Begriffe“ genauso eine Lösung sein wie die maximale Variante verteilter und mit anderen Unternehmen geteilter Ressourcen. Eine ausschließliche Private oder PublicCloud ist in der Praxis selten. Vielmehr ist die Nutzung individueller Vorteile aller Dienstschicht- und Betriebsmodelle geboten. Beispiele für diese Abwägungen sind:

- Kunden mit stark schwankenden kapazitativen Anforderungen wählen zur Skalierbarkeit die Abdeckung von Spitzen mit Public Cloud-Angeboten als hybride Infrastruktur.
- Hoch sensible Daten bekommen Vorzug in einer On-Premise-Cloud, so dass sie das Haus nicht verlassen.
- Applikationen, die kostengünstiger in der Public Cloud zu betreiben sind, werden mit der Private Cloud gekoppelt.

Eine detaillierte Analyse nach Anforderungen wie Agilität, Sicherheit, Budget-Situation ist von Fall-zu-Fall zu klären. Nach dieser Klärung kann eine optimale Lösung implementiert und genutzt werden, die nicht auf konsequenter Verlagerung beruht, sondern sich den Geschäftsbedürfnissen anpasst.

4.4.2.2.4 Anforderungen für Community Clouds

Um die Aufwände zur Kopplung zu fremden Systemen zu vermeiden und die Sicherheit zu erhöhen, ist die Community Cloud mehr als ein Kompromiss: Interessengemeinschaften wie Konzerne, Arbeitsgemeinschaften, Branchenverbände oder Standorte bilden eine Community Cloud mit dem Vorteil der Geschlossenheit und entsprechender Sicherheit unter gleichzeitiger Verwendung der Methoden einer Public Cloud in Bezug auf Self-Service und Verrechnung. Durch die natürliche Vertrauensposition sind die Anforderungen und somit auch die budgetären Belastungen bei weitem nicht so hoch, wie zu unbekannten und teilweise weltweit aktiven Cloud-Service-Anbietern.

Die größte Hürde für den Betriebsverantwortlichen der Community Cloud ist die Allokation von Finanzmitteln; in der Regel geben die potentiellen Mandanten vor Fertigstellung der Lösung keine Absichtserklärung über die Nutzung ab. Somit sind das Geschäftsmodell und die Cloud-Eigenschaften wie Betriebsmodelle mit den potentiellen Nutzern abzustimmen.

4.4.2.2.5 Kombination von Dienstschicht und Betriebsmodell

Die Kombination verschiedener Dienstschichten und Betriebsmodelle kann sinnvoll sein, um gestellte Anforderungen optimal zu erfüllen. Eine Kopplung der eigenen Infrastruktur (Private) mit der entfernten (Hybrid oder Public) bedingt die Umsetzung folgender Aufgabenpakete:

- Implementierung einer Brückenfunktion (so genanntes Bridging) zur Herbeiführung einer sicheren Cloud-Cloud-Kopplung mit entsprechenden Zugriffslisten und zur transparenten Darstellung für den Anwender
- Implementierung eines Identity- und Access-Management zur durchgehenden Authentisierung und Autorisierung (siehe 3.6.1)
- Nutzung von Hersteller-unabhängigen Formaten zur Erhöhung von Portabilitäten; beispielsweise für die Virtualisierungsschicht kann ein Austauschformat die Verschiebung zwischen der Private und der Public Cloud ermöglichen bzw. vereinfachen.

Das Ergebnis eines solchen Ansatzes kann eine private PaaS-Infrastruktur mit einer öffentlichen SaaS-Lösung sein oder eine private Produktivumgebung in Kombination mit einer öffentlichen Entwicklungs- und Testumgebung.

Tabelle 14 — Verantwortlichkeiten bei der Spezifikation des Betriebsmodells

Nr.	Aufgabe	Geschäftsleitung	Einkauf	Projektleiter	Fachbereich	Cloud-Service-Anbieter	Compliance-Beauftragter/ Betriebsrat	IT
1	Ableitung des Kapazitätsbedarfs			A	S	S		R/A
2	Planung des Zugriffs auf die Cloud-Infrastruktur			A	S	S	R	R
3	Identifizierung der für die Cloud relevanten Workloads			A	R		S	R
4	Abstimmung der Automatisierungsschnittstellen der verschiedenen Betriebsmodelle			A	C			R
5	Implementierung der Hypervisor-neutralen Technologien			A			C	R/A

4.4.3 Ableitung eines Kriterienkatalogs

4.4.3.1 Wesentliche Fragen

- Welche Kriterien sind bei der Auswahl zu berücksichtigen?
- Welche Prioritätsstufen sind den Kriterien zuzuordnen?
- Welche Verbindlichkeitsstufen sind für Kriterien zu definieren?
- Welche Realisierbarkeitseinstufungen sind für Kriterien zu definieren?
- Welche Finanzierbarkeitseinstufungen sind für Kriterien zu definieren?

4.4.3.2 Beschreibung allgemein

4.4.3.2.1 Vorgehensweise

Basierend auf 4.4.1 „Erstellung Anforderungskatalog“ und 4.4.2 „Spezifikation des Betriebsmodells“ ist ein Kriterienkatalog abzuleiten. Dieser Kriterienkatalog wird für die Auswahl des Cloud-Service-Anbieters benötigt – das Ergebnis stellt als Teil einer Bewertungsmatrix die wesentliche Entscheidungsgrundlage dar. Im Folgenden wird eine Methode zur Erstellung des Kriterienkatalogs beschrieben. Die Methode eignet sich in besonderer Weise für die Auswahl von Cloud-Service-Anbietern, unabhängig von gewählter Dienstschicht und Betriebsmodell. Es wird die Möglichkeit geboten sowohl funktionale als auch nicht-funktionale, textbasierte oder modellbasierte sowie präzise oder ungenaue Anforderungen zu berücksichtigen. Das Vorgehen gliedert sich in insgesamt drei Phasen:

5) Bewertung der Anforderungen;
6) Strukturierung des Kriterienkatalogs;
7) Ableitung einzelner Kriterien.

4.4.3.2.2 Bewertung der Anforderungen

Die Basis für die Bewertung der Anforderungen bildet sachlogisch der Anforderungskatalog. Ziel der Überführung in einen Kriterienkatalog ist die Reflexion der Anforderungen, auch aus der Sichtweise des späteren Cloud-Service-Anbieters, als auch die Qualitätssicherung der zuvor definierten Anforderungen. Die nachfolgend dargelegten Kategorien sind lediglich als Vorschlag zu verstehen, eine Anpassung auf die KMU spezifischen Bedürfnisse ist möglich und sinnvoll. Zu diesem Zweck sind in einem ersten Schritt unterschiedliche **Prioritätsstufen** zu definieren.

Tabelle 15 — Mögliche Ausprägungen der Kategorie „Prioritätsstufe“

Prioritätsstufe	Beschreibung
Muss	Die Anforderung muss vom Cloud-Service-Anbieter erfüllt werden, um ein Auslagern des Services möglich zu machen.
Soll	Die Anforderung sollte wenn möglich (finanzierbar, realisierbar) vom Cloud-Service-Anbieter erfüllt werden. Für die Umsetzung gilt jedoch das Gebot der Wirtschaftlichkeit.
Könnte	Eine solche Anforderung beschreibt einen Zusatznutzen, der beispielsweise die Akzeptanz der Benutzer erhöht. Die Anforderung sollte vom Cloud-Service-Anbieter erfüllt werden, sofern dies kostengünstig oder kostenneutral erfolgen kann.
Unnötig	In keinem Fall sollte für die Umsetzung einer solchen Anforderung Kosten entstehen oder unverhältnismäßig viel Zeit in die Begutachtung investiert werden.

4.4.3.2.3 Präzision

Im zweiten Schritt ist die **Präzision,** mit der Anforderungen beschrieben werden müssen, zu definieren.

Tabelle 16 — Mögliche Ausprägungen der Kategorie „Präzision“

Präzisionsstufen	Beschreibung
Sehr präzise	Eine vollständige Beschreibung ohne Interpretationsspielraum ist notwendig. Insbesondere bedeutet dies eine exakte Beschreibung des Cloud-Service-Anbieter Services Verhaltens (SLA) unter allen Umständen (z. B. Ausfallzeiten, Antwortzeiten, etc.). Der hohe Grad an Präzision lässt sich insbesondere durch die Verbindung von Modellen (z. B. EPKs, Ereignisgesteuerte Prozessketten), strukturierten Texten und mathematischen Ausdrücken (z. B. OCL, en: Object Constraint Language) erreichen.
Weitgehend präzise	Es findet keine vollständige Beschreibung aller Fehler- oder Ausnahmefälle statt. Trotzdem ist die Gesamtsituation sowie Verhaltensweise beidseitig gut zu verstehen und nachvollziehbar.
Unpräzise	Die Anforderung ist unklar, besitzt offene Punkte oder einen hohen Interpretationsspielraum, z. B. „Der Cloud-Service-Anbieter muss schnell antworten“, etc. Eine solche Beschreibung kann in einigen Fällen bei der Beschreibung von Anforderungen aufgrund eines zu hohen Aufwands oder unvollständiger Informationen vorkommen.

4.4.3.2.4 Verbindlichkeit

Die dritte zu beschreibende Kategorie ist die Verbindlichkeit. Sie legt das Verhältnis zwischen Realisierung einer Anforderung zu ihrer Beschreibung fest. Diese Kategorie ist als eine Ergänzung zu der zuvor beschriebenen Präzision zu verstehen, so ist es z. B. denkbar, dass eine Anforderung zwar äußerst präzise beschrieben werden muss, ein Abweichen jedoch denkbar und eventuell im Projektverlauf auch sinnvoll sein kann.

Tabelle 17 — Mögliche Ausprägungen der Kategorie „Verbindlichkeit“

Verbindlichkeitsstufen	Beschreibung
Exakt	Die definierte Anforderung muss exakt vom Cloud-Service-Anbieter umgesetzt werden. Eine Anforderung die exakt erfüllt sein muss, erfordert eine sehr genaue Beschreibung und bereits zum Zeitpunkt der Definition umfassendes Wissen über den Sachverhalt.
Gleichartig	Der Cloud-Service-Anbieter muss in einer gleichartigen Service Leistung die Anforderung erfüllen. Eine Realisierung der Anforderung, welche gleichartig ist, ist insbesondere dann sinnvoll, wenn noch nicht alle Eigenschaften des Services klar definiert sind.

4.4.3.3 Realisierbarkeit

Die vierte zu beschreibende Kategorie ist die **Realisierbarkeit.**

Tabelle 18 — Mögliche Ausprägungen der Kategorie „Realisierbarkeit“

Realisierbarkeitsstufen	Beschreibung
Realisierbar	Die betrachtete Anforderung ist in einer ersten Bewertung sowohl theoretisch wie auch praktisch umsetzbar.
Unrealisierbar	Die Anforderung ist entweder auf Seiten des Outsourcenden oder des Cloud-Service-Anbieters nicht umsetzbar.
Unklar	Es ist nicht klar, in wie weit die Anforderung umsetzbar ist. Dies kann ins besondere der Fall sein, sofern die Anbieter noch nicht vollständig erhoben und deren Angebote untersucht wurden.

4.4.3.4 Finanzierbarkeit

Die letzte zu beschreibende Kategorie stellt die **Finanzierbarkeit** der Anforderung dar. Im Rahmen der Finanzierbarkeit ist eine Umsetzung vor dem Hintergrund des Projektbudgets zu beurteilen: ist die Umsetzung der Anforderung unverhältnismäßig teuer oder überschreitet das Projektbudget, ist diese nicht umsetzbar. Hier gilt es die Abhängigkeit einzelner Anforderungen zu beachten. In wie weit einzelne Anforderungen finanzierbar sind, hängt häufig von einer Kombination von Anforderungen ab. Diese gilt es zu berücksichtigen.

Tabelle 19 — Mögliche Ausprägungen der Kategorie „Finanzierbarkeit“

Finanzierbarkeitsstufen	Beschreibung
Finanzierbar	Die Anforderung ist im Rahmen des Projektbudgets finanzierbar.
Unfinanzierbar	Die Anforderung übertrifft das Projektbudget oder ist unverhältnismäßig teuer zum entstehenden Nutzen. Häufig ist dies der Fall bei überzogenen nicht-funktionalen Anforderungen, wie z. B. sehr geringen Antwortzeiten, sehr hoher Ausfallsicherheit, etc.
Unklar	Zum Zeitpunkt der Erstellung des Kriterienkatalogs ist noch unklar, welche Kosten durch die Erfüllung der Anforderung entstehen. Diese sollten nach der Angebotsphase nachgepflegt werden.

4.4.3.5 Anwendung der Kategorien auf die Anforderungen

Den Anforderungen wird für jede der zuvor definierten Kategorien eine Ausprägung zugeordnet und tabellarisch dargestellt. Auf Basis der gesammelten Informationen werden Risiken kurz, stichpunktartig beschrieben und eine Empfehlung zum weiteren Verfahren gegeben. Handelt es sich z. B. um eine „Muss“ Anforderung, die unpräzise formuliert ist, besteht das Risiko unvollständig erfüllter Anforderungen vom Cloud-Service-Anbieter. Dies gilt es zu verhindern. Aus diesem Grund sind möglichst exakte Formulierungen ratsam.

Tabelle 20 — Beispielstruktur eines Anforderungskatalogs

Anforderung	Priorität	Genauigkeit	Verbindlichkeit	Realisierbarkeit	Finanzierbarkeit	Risiko	Empfehlung
Beispiel 1						Dokument wird unnötig aufgebläht.	Entfernen
Beispiel 2						Wichtige Bestandteile werden falsch verstanden.	Überarbeiten und präzisieren
Beispiel 3						Die Anforderung übersteigt das Projektbudget.	Anforderung neu definieren oder streichen

4.4.3.6 Ableitung einzelner Kriterien

Nach der Bewertung und Strukturierung der Anforderungen müssen aus diesen einzelne Kriterien abgleitet, in die Struktur des Kriterienkatalogs einsortiert und gewichtet werden. Der Verantwortliche sollte folgende Punkte berücksichtigen:

- Anforderungen die finanzierbar, realisierbar und entweder als „Muss“ „Soll“ oder „Könnte“ Anforderungen eingestuft wurden, sollten durch den Cloud-Service-Anbieter abgedeckt werden.

- Es ist zu beachten, dass zwischen Anforderungen und Kriterien eine theoretische n:m Beziehung bestehen kann, d. h. eine Anforderung kann durch eines bis mehrere Kriterien abgedeckt werden oder auch eine oder mehrere Anforderungen können durch ein Kriterium abgedeckt werden. Es ist jedoch anzustreben, dass eine Anforderung durch ein Kriterium abgedeckt ist.

- Bei der Gewichtung der Kriterien muss die Anzahl der Anforderungen und deren Bewertung berücksichtigt werden. „Muss“ Anforderungen sollten grundsätzlich eine hohe Gewichtung erhalten.

- Für die Nachvollziehbarkeit der Gewichtung sollte immer auch eine Begründung gegeben werden, um eventuell spätere Anpassungen oder die Begutachtung durch Dritte zu erleichtern.

4.4.3.7 Strukturierung des Kriterienkatalogs

Der Kriterienkatalog kann in der nachfolgend beschriebenen Struktur verfasst werden. Prinzipiell ist diese jedoch frei wählbar, daher handelt es sich bei der hier vorgestellten lediglich um einen Gliederungsvorschlag.

Tabelle 21 — Beispielstruktur eines Kriterienkatalogs

Kriterienhauptgruppe	Kriteriengruppe	Kriterium	Gewichtung	Begründung

Tabelle 22 — Verantwortlichkeiten bei der Ableitung eines Kriterienkatalogs

Nr.	Task	Geschäftsleitung	Einkauf	Projektleiter	Fachbereich	Cloud-Service-Anbieter	Compliance-Beauftragter/ Betriebsrat	IT
1	Definition weiterer Bewertungskategorien			A	R		I	C
2	Zuordnung der Anforderungen zu Kategorien			A	R		I	C
3	Gewichtung durchführen	A		R	R		I	
4	Bewertung und Ergebnis festlegen	A	I	R			I	

Tabelle 23 — Ergebnisdokumente der Phase „Ableitung eines Kriterienkatalogs“

Dokument ID	Dokument Bezeichnung	Dokument Beschreibung	Dienstschicht	Betriebsmodell
3.4 – A	Bewertungsgrundlage und Kriterienkatalogstruktur	Verzeichnis aller Kriterien, deren Eigenschaften und möglichen Ausprägungen	IaaS PaaS SaaS	Private Public Hybrid Community

4.4.4 Erstellung einer Bewertungsmatrix

4.4.4.1 Wesentliche Fragen

— Erfolgt eine sachgerechte Einordnung der Anforderungen zur Prozessabhängigkeit des Cloud Services?

— Sind die Compliance Anforderungen der zu verarbeitenden Daten definiert?

— Sind die monetären Risiken bei einem Systemausfall des Cloud Services kalkuliert?

— Existieren Notfallpläne mit dokumentierten Verfahrensbeschreibungen für alle betroffenen Bereiche bei Leistungseinschränkung oder -ausfall?

4.4.4.2 Beschreibung allgemein

Anhand der vorgenannten Überlegung ist zu empfehlen, für die Entscheidungsfindung eine Score Card zu erstellen, die den jeweiligen Kriterien entsprechend eine Qualifizierung des Services und des Anbieters im Auswahlprozess ermöglicht.

Hierbei sind zwei Auswahlbereiche zu berücksichtigen:

- Identifikation von IT-Services, die generell als Cloud Service verwendet werden können. Hier werden die Kriterien an unternehmensinternen Vorgaben definiert (siehe 4.3.3, insbesondere „Definition des Servicekatalogs“).

- Identifikation von Anbietern, die einen möglichen Cloud Service bereitstellen. Hier werden die Kriterien an den konkreten Cloud Service definiert (siehe 4.4.5).

Im Ergebnis kann ein solches Scoring in verschiedene Auswertebetrachtungen überführt werden. Im folgenden Beispiel werden drei mögliche Use Cases für den Einsatz von Cloud-Infrastrukturservices aufgeführt:

i) Test und Entwicklungssysteme

Das Unternehmen plant für die Ausstattung der Entwicklung und Qualitätssicherung an den verschiedenen Standorten die Nutzung von virtuellen Servern. Generell ist dabei die Anforderung an das Datenschutzniveau gering, da keine personenbezogenen Daten verarbeitet werden. Es besteht aber eine gewisse Prozessabhängigkeit, da bei Ausfall oder Nichtverfügbarkeit diese Tätigkeit nicht ausgeführt werden kann. Aufgrund der geringen Mitarbeiterzahl und der Möglichkeit, Alternativtätigkeiten auszuführen, ist die Kritikalität dennoch im mittleren Bereich zu sehen. Die Einrichtung einer solchen Infrastruktur ist mäßig komplex, da einige Schnittstellen zwischen den Systemen eingerichtet und gewartet werden müssen und auch die Verbindung zu den lokalen IT-Systemen herbeigeführt werden muss.

j) E-Mail Archivierung

Die Archivierung von E-Mail unterliegt erhöhten Compliance-Anforderungen. Zum einen gibt es regulatorische Anforderungen (Aufbewahrungspflicht) und durch den Personenbezug auch eine Einhaltungsverpflichtung der Datenschutzbestimmungen.

Die technische Integration ist wenig komplex, sofern es sich um die Ablage von Archivdateien (idealerweise verschlüsselt) handelt. Hierbei ist anzumerken, dass es auch E-Mail Archivierungsservices als SaaS Angebot gibt, die zu einer anderen Bewertung führen können.

k) PPS (Produktions- und Planungssystem) im Eigenbetrieb auf Cloud Servern

Die Einrichtung eines gesamten PPS Systems mit eigener Software auf gemieteten virtuellen Servern ist dagegen bezüglich der Komplexität der Integration, der Prozessabhängigkeit, der Verfügbarkeit und den Datenschutzanforderungen als hoch anzusetzen und unterliegt den Anforderungen kritischer Infrastrukturen mit besondere Absicherung der Servicequalität. Je nach Einschätzung der möglichen Risiken kann es auch zu einer nur teilweisen Einbindung externer Services bzw. einer generellen hybriden Architektur führen.

Je nach Ausprägung und individueller Gewichtung der einzelnen Bewertungskriterien kann die Einordnung anhand der kumulierten Werte grafisch visualisiert werden (Bild 5).

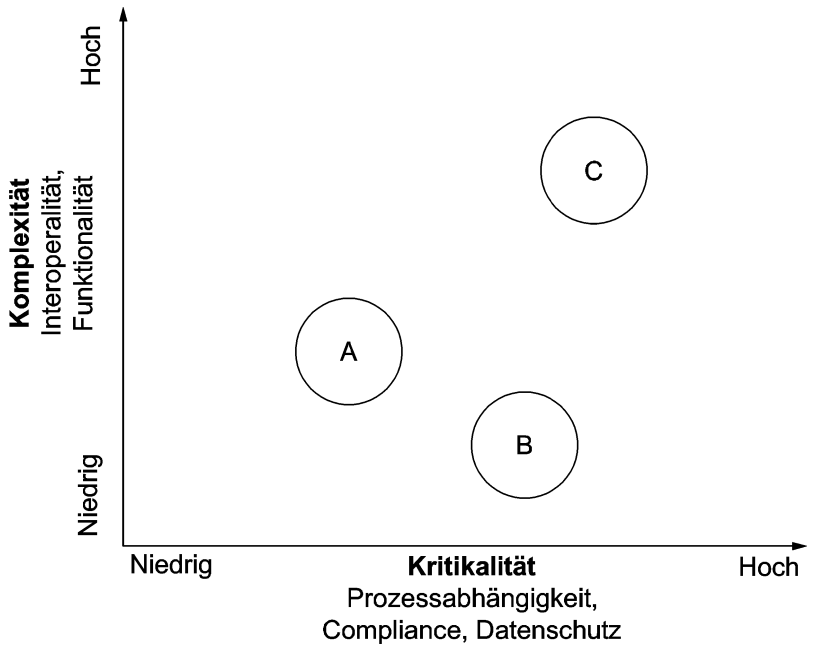

Bild 5 — Einordnung eines Gesamtscorings

Die jeweilige Einordnung von standardisierten Cloud Services ist also immer eine Betrachtung von Basiskriterien (wie zum Beispiel aus Zertifikaten) und der anwenderbezogenen Einordnung unter Berücksichtigung der jeweiligen Nutzung und den Umfeldbedingungen. Da diese immer individuell zu bewerten sind, ist eine generelle Methodik auf den jeweiligen Anwendungszweck anzupassen. Eine Reduktion auf reine Sicherheitsanalysen und technische Anforderungen ist dabei nicht ausreichend. Im Vergleich zur den nach innen gerichteten Auswahlentscheidungen nach 4.3.1 und 4.3.2 - erfolgt an dieser Stelle eine anbietergerichtete Bewertung der zuvor als relevant eingestuften Kriterien [9].

4.4.5 Erhebung und Auswahl eines Cloud-Service-Anbieter

4.4.5.1 Wesentliche Fragen

- Sind potenziell relevante Cloud-Sourcing-Nehmer identifiziert?
- Welche potenziellen Cloud-Sourcing-Nehmer sollen die Ausschreibung erhalten?
- Wie soll die Ausschreibung aufgebaut sein?
- Wie wird das Auswahlverfahren bis zum Vertragsabschluss organisiert?

4.4.5.2 Beschreibung allgemein

Auf Basis der Ergebnisse der vorherigen Phasen sind geeignete Cloud-Service-Anbieter zu identifizieren. Bei der **Erhebung geeigneter Cloud-Service-Anbieter** geht es zunächst um eine erste Marktanalyse und noch nicht um die konkrete Auswahl eines Cloud-Service-Anbieters. Neben der (internen) Marktanalyse können in dieser Phase Informationsanfragen (RFI) an potenzielle Cloud-Service-Anbieter versendet werden, um erste Informationen für eine Eignung als Geschäftspartner zu erhalten.

In dieser Phase liegen bereits erhebliche Informationen über interne Prozesse, Kostenstrukturen und potenzielle Cloud-Service-Anbieter vor. Die maßgeblichen Entscheidungsträger (in der Regel die Geschäftsführung) sollten an dieser Stelle eine **Entscheidung für oder gegen eine Fortführung des Cloud-Sourcing-Vorhabens** fällen. Es handelt sich hierbei noch nicht um eine Entscheidung für einen konkreten Cloud-Service-Anbieter oder eine tatsächliche Umsetzung, sondern vielmehr um eine Freigabe für nächste Projektschritte und eine folgende Detailplanung.

Zu unterscheiden ist, ob es sich um eine am Markt stark standardisierte oder um eine individuell konfigurierte Leistung handelt. Bei standardisierten Leistungen ist das folgende Verfahren dahingehend zu vereinfachen, dass die Anbieter in der Regel eine Standardleistung anbieten und diese nicht spezifisch auf die Anforderungen des Kunden anpassen. So benötigen diese auch ggf. keine umfangreichen Ausschreibungsunterlagen, sondern der Ausschreibende muss die Produktspezifikationen des Anbieters gegen seine Anforderungen spiegeln.

In der **Detailplanung** sind die geplanten Schritte im weiteren Vergabeverfahren zu planen. Dabei sollten neben den Bearbeitungszeiten der Anbieter auch die Zeiten für Auswertung aller Angebote und Entscheidungsverfahren beim Ausschreibenden angemessen berücksichtigt werden.

Auf Basis dieser Marktübersicht sollte entschieden werden, welche potenziellen Anbieter die **Ausschreibungsunterlagen** (RFP) erhalten. Die Ausschreibungsunterlagen sollten auf dem Servicekatalog und dem Kriterienkatalog basieren und Informationen zur Planung des Vergabeverfahrens enthalten (vgl. auch DIN SPEC 1041, 3.4.1).

Die erhaltenen **Angebote** können nach Gesichtspunkten der zuvor erarbeiteten Kriterien **analysiert** werden.

Nach der Analyse kann zunächst eine **engere Auswahl von Anbietern** auf Basis des Ergebnisses der zuvor durchgeführten Angebotsanalyse erstellt werden. Als Ergebnis sollten mindestens ein, im Normalfall jedoch mehrere, Anbieter ausgewählt werden, mit denen Vertragsverhandlungen geführt werden.

Je nach Komplexität und Kritikalität des Ausschreibungsgegenstands kann es sinnvoll und erforderlich sein, eine **Due Diligence** (de: gründliche Prüfung) durchzuführen (vgl. zur Auswahl auch DIN SPEC 1041, 3.4.2). Bei Standardprodukten wird dies in der Regel nicht möglich sein.

Tabelle 24 — Verantwortlichkeiten bei der Erhebung und Auswahl eines Cloud-Service-Anbieters

Nr.	Aufgabe	Geschäftsleitung	Einkauf	Projektleiter	Fachbereich	Cloud-Service-Anbieter	Compliance-Beauftragter/ Betriebsrat	IT
1	Erhebung von möglichen Cloud-Service-Anbietern							
1.1	Durchführung einer Marktanalyse	I	A	R	C	C	I	
1.2	Ggf. Durchführung RFI-Verfahren	I	A	R	C	C	I	
1.3	Entscheidung zur Ausschreibung	A/R	C	C	C	I	I	I
2	Ausschreibungsverfahren							
2.1	Vorbereitung der Ausschreibungsunterlagen	I	A	R	C		C	I
2.2	Auswahl der potenziellen Anbieter	C	A	R	C		C	I
2.3	Versand der Ausschreibungsunterlagen	I	R	C	I		I	I
2.4	Erstellung der Angebote					A/R		
3	Vorbereitung der Auswahlentscheidung							
3.1	Analyse der erhaltenen Angebote	I	A	C	C		C	I
3.2	Ggf. Durchführung Due Diligence	I	A	R	C	C	C	I
3.3	Auswahlempfehlung	I	A	R	C	I	C	I
4	Vertragsabschluss mit Cloud-Service-Anbietern[1]							
4.1	Erarbeitung der Vertragsstruktur	I	A	R	C	I	C	I
4.2	Verhandlung der Vertragsinhalte	R	A	R	R	R	C	I
4.3	Abschluss des Vertrags	A	R	C	C	R	C	C

[1] Diese Aufgaben sind Teil des nachfolgenden Kapitels, wurden jedoch der Übersicht halber an dieser Stelle mit aufgenommen.

Tabelle 25 — Ergebnisdokumente der Phase „Erhebung und Auswahl eines Cloud-Service-Anbieters“

ID	Dokument Bezeichnung	Dokument Beschreibung	Dienstart	Dienst modus
3.4 – B	Bewertungsmatrix	Quantitative Bewertung der erhaltenen Angebote auf Basis des Kriterienkatalogs	Alle	Alle
3.4 – C	Bericht zur Auswahl der Dienstleister	Begründung der Auswahlempfehlung auf Basis der Bewertungsmatrix und ggf. weiterer Gesichtspunkte	Alle	Alle

4.4.6 Vertragsabschluss mit dem Cloud-Service-Anbieter

4.4.6.1 Wesentliche Fragen

- Wie soll der Vertrag strukturiert werden?
- Welche Cloud-spezifischen Inhalte sollte der Vertrag regeln?

4.4.6.2 Beschreibung allgemein

In der **Vertragsverhandlung** wird das Vertragswerk zwischen Cloud-Sourcing-Geber und Cloud-Service-Anbieter erarbeitet. Bei standardisierten Cloudprodukten werden die Anbieter in der Regel auf standardisierten Verträgen bestehen.

Vorbereitend kann eine Absichtserklärung (LOI) abgeschlossen werden. Auf Grund der Komplexität eines Cloud-Sourcingvorhabens wird das Vertragswerk in der Regel aus mehreren Dokumenten bestehen (vgl. DIN SPEC 1041, 3.4.3):

- Rahmenvertrag mit allgemeinen Regelungen;
- Organisatorische Regelungen;
- Serviceregelungen (Service Level Agreement, SLA).

Die folgenden Punkte sollten durch einen Vertrag mit einem Cloud-Service-Anbieter mindestens geregelt werden:

Tabelle 26 — Zu berücksichtigende Themen bei einem Vertragsabschluss

Thema	Fragestellung
Konkretes Leistungsangebot (SLA)	Im Vertrag sollte das Leistungsangebot des Anbieters genau festgelegt werden. Zu diesen Service-Level-Agreements gehören unter anderem die Verfügbarkeit der Services, die zulässige Ausfallrate, die Reaktionszeiten bei Störungen oder die Wiederanlaufzeit der Systeme nach einem Ausfall.
Sicherheits- und Datenschutzaspekte	Das BSI (Bundesamt für Sicherheit in der Informationstechnik) empfiehlt, neben den konkreten Leistungen auch sicherheitsrelevante Aspekte und Datenschutzvereinbarungen in den SLAs festzulegen. Um nachhaltige Datensicherheit zu gewährleisten, sollte sichergestellt sein, dass der Service-Anbieter sein Sicherheitskonzept entsprechend der technischen Entwicklung kontinuierlich anpasst.
Gewährleistung, Haftung und Vertragsstrafen bei Nichterfüllung	Haftung und Gewährleistung sollten klar geregelt sein. Die Vertragspartner können zusätzlich Pönalen für den Fall vereinbaren, dass der Anbieter die vereinbarten SLAs nicht erfüllt.
Beauftragung von Subunternehmen	Die Vertragspartner sollten festlegen, ob und in welcher Form der Anbieter Subunternehmen mit bestimmten Leistungen beauftragen kann. Grundsätzlich darf ein CloudAnbieter dabei nur solche Unternehmen beauftragen, die mindestens das gleiche Schutzniveau sicherstellen wie der Auftragnehmer selbst. Auch sollten keine Wettbewerber des Kunden vom Auftragnehmer unterbeauftragt werden.
Kontrollrecht des Auftraggebers	Der Auftraggeber sollte sich vertraglich das Recht zusichern lassen, dass er die Datenverarbeitung des CloudAnbieters einschließlich der Schutzmaßnahmen regelmäßig kontrollieren darf. Die mögliche Ausgestaltung ist auch stark vom CloudService abhängig (im Bereich PublicCloud sind meist kaum Kontrollrechte für den Auftraggeber gegeben).
Vertragslaufzeit und Rückgabe der Daten	In einem Cloud-Vertrag muss nicht nur die Laufzeit zwingend geregelt werden, sondern auch die Modalitäten bei der Rückgabe oder Löschung der Daten. Dazu gehören zum Beispiel der Übertragungsweg oder das Dateiformat.
Exit-Strategie	Auch eine frühzeitige Rückgabe der Daten - zum Beispiel im Falle der Insolvenz eines Anbieters oder bei einem Anbieterwechsel - muss klar geregelt sein. Eine solche Exit-Strategie sollte den Auftraggeber im Zweifelsfall auch berechtigen, die Daten von Subunternehmen zurückzufordern.
Nutzungsrechte	Es sind die Fragen zu klären ob kritische Nutzungseinschränkungen aufgrund der Art der Lizenzeinräumung existieren und in wie weit die Lizenzen auch für Tochterunternehmen gelten.
Anwendbares Recht	Verträge nach ausländischem Recht schränken die Gültigkeit in Deutschland üblicher Rechtsnormen (z. B. von AGB, und Gewährleistungen) unter Umständen ein. Außerdem kann die Geltendmachung von Ansprüchen im Ausland schwierig und aufwändig, in Teilen unmöglich werden.

Tabelle 26 (*fortgesetzt*)

Thema	Fragestellung
Umfang des gewährleisteten Datenschutzes	Bei der Verarbeitung personenbezogener Daten sind regelmäßig Auftragsdatenverarbeitungsverträge erforderlich. Sind der Datenschutz und ggf. ausreichende Auftragsdatenverarbeitungsverträge geregelt? Sind die damit verbundenen erforderlichen Kontrollrechte des Auftraggebers geregelt? Nicht zuletzt ist eine Risikoabschätzung zu treffen, ob die konkreten Gegebenheiten für das erforderliche Schutzniveau ausreichen (z. B. Schutz vor Spionage etc.). Auch die Verarbeitungssicherheit (Pflicht und Nachweis regelmäßiger Backups) sollten geregelt sein?
Speicherort der Daten	Der Daten- und Informationstransfer ins Ausland kann sowohl aus Datenschutzgründen als auch aus dem Exportrecht heraus unzulässig sein. Bei einer Datenhaltung im Ausland sind die grundsätzliche Zulässigkeit und die vertraglichen Zusicherungen des Auftragnehmers genau zu prüfen.
Dateneigentum und -Rückgabe	Ist sichergestellt, dass die Rechte an den Daten und Ergebnissen der Verarbeitung auch beim Auftraggeber/Nutzer verbleiben und eine Nutzung durch Dritte ausgeschlossen ist? Ist auch eine zwischenzeitliche Herausgabe aller Daten sichergestellt? Ist sichergestellt, dass ausreichend Datenlogik und Dokumentation zur Weiterverarbeitung zur Verfügung steht? Sind die Kosten für eine Rücktransferierung geregelt?
Verschlüsselung	In welchem Umfang werden Daten verschlüsselt und wer ist Inhaber des privaten Schlüssels? Die Anwendung bestimmter Verfahren ist nicht stets in allen Ländern zulässig.
Zertifikate	Liegen für den Cloudanbieter entsprechende Zertifikate vor (z. B. SAS 70 bzw. ISAE 3402)?
Archivierung	In welchem Umfang leistet der Anbieter die Archivierung der jeweils zum Einsatz kommenden Software, um zu einem späteren Zeitpunkt innerhalb der GoB (Grundsätze ordnungsmäßiger Buchführung) ggf. archivierte Daten zu lesen? Darüber hinaus sind folgende Fragen zu stellen: — Wie muss ein sinnvolles Backup-Konzept aussehen auch im Hinblick auf ein Vertragsende? — Sind die Übertragungswege und die Speicher hinreichend gesichert und verschlüsselt? — Werden die Daten in separaten Speicherbereichen gelagert und wie werden die Speicher gelöscht bei Verschiebungen innerhalb der Cloud?
Change Management	Da sich über die Vertragslaufzeit Änderungen der Rahmenbedingungen ergeben werden, ist ein besonderes Augenmerk auf die Möglichkeit der Anpassungen und Veränderungen (Change Management) zu richten: — Sind zukünftige Anpassungen bei beispielsweise gesetzlichen Änderungen möglich? — Wie wirken sich größere Änderungen im Bereich Datenvolumen oder Systeme auf den Vertrag aus?

Zusätzlich sollte der Vertrag auch die allgemeinen Anforderungen des Unternehmens an Lieferantenverträge erfüllen und ggf. rechtlich überprüft werden [10].

Tabelle 27 — Verantwortlichkeiten beim Vertragsabschluss

Nr.	Aufgabe	Geschäftsleitung	Einkauf	Projektleiter	Fachbereich	Cloud-Service-Anbieter	Compliance-Beauftragter/ Betriebsrat	IT
1	Ausarbeiten des Vertragswerks		R	A	R		I	C
2	Prüfen und unterzeichnen des Vertrags	RA						

Tabelle 28 — Ergebnisdokument der Phase „Vertragsabschluss mit dem Cloud-Service-Anbieter“

ID	Dokument Bezeichnung	Dokument Beschreibung	Dienst-art	Dienst-modus
3.4 – D	Cloud-Sourcingvertrag	Vertragswerk, in der Regel aus mehreren Vertragsbestandteilen wie Rahmenvertrag, organisatorischen Regelungen und den spezifischen Serviceregelungen (SLA)	Alle	Alle

4.5 Implementierung

4.5.1 Wesentliche Fragen

Mit der Planung für eine Cloud-Implementierung beginnt die Detaillierung einzelner Fragestellungen. Trotz der sorgfältigen Vorbereitung mit Hilfe der hier vorliegenden DIN SPEC besteht immer auch das latente Risiko, dass im Vorfeld einzelne (Teil-)Themen unzureichend eingeschätzt wurden und spätestens vor Start der Implementierung einer Korrektur bedürfen. Die Anwendung dieser DIN SPEC minimiert diese Risiko jedoch. Zu den Themen gehören vor allem:

- Welche Anforderungen von Seiten der IT-Sicherheit sind zu berücksichtigen?
- Welche Komplexität von technischen und Prozess-Schnittstellen ist zu beachten?
- Wie hoch ist der Anpassungsbedarf der technischen Infrastruktur?
- Wie hoch ist der Grad der Standardisierung im Bereich IT und der Betriebsprozesse?
- Welche Kosten verursacht die Transformation?
- Welche übergeordneten IT-Ziele und -Prioritäten sollen mit Cloud Computing adressiert werden?
- Welche Organisationseinheiten nutzen Cloud Services?
- Welche Cloud Services sollen bereitgestellt werden?

Tabelle 29 — Verantwortlichkeiten bei der Implementierung

Nr.	Aufgabe	IT-Leitung	IT-Entwicklung	IT-Betrieb	Projektleiter	Fachbereich	Betriebsrat	IT-Sicherheits-verantwortlicher	Cloud-Service-Anbieter
1	**Anpassung von Schnittstellen, fachliche Prozesse**								
1.1	Liste der betroffenen Prozesse erstellen	A	S	R/C		S		S	
1.2	Erstellen des Soll-Prozessmodel	A	S	R/C		S		S	S
1.3	Auslistung alles betroffenen Schnittstellen	A	S	R/C		S		S	S
2	**Vorbereitungsphase**								
2.1	Projektziele definieren und die Projektkommunikation festlegen	A		S	R	S			C
2.2	Projektorganisation festlegen	A		S	R	S			
	Dokumentationsstruktur und die Ablage-struktur definieren und abstimmen			A/S	R	S			
2.3	Projektplan erstellen und Projekt-Risiko-management etablieren			S	A/R	S			C
3	**Design Sollkonzept**								
3.1	Dokumentation der organisatorische Auswirkungen und Verantwortlichkeiten				A/R	S			
3.2	Anpassung der Prozesse				A/R	S			
3.3	Erhebung von Mengengerüsten und Bereinigung von Daten	A		S	R	S			C
3.4	Design der notwendigen Schnittstellen und Dateiformate, sowie der Datenmengen	A	S	S	R	S			C
4	**Vorbereitung der Migration**								
4.1	Kriterien für die Wahl der Migrationsart treffen	A			R				C
4.2	Auswahl der Migrationsart festlegen	A			R				C
5	**Planung der Migration**								
5.1	Beschreibung des Ausgangszustandes (Konfigurationen, Mengen, Einstellungen)			A	R/C	S			
5.2	Beschreibung des Zielzustandes	A		S	R/C				S
5.3	Planung der Migration in Einzelschritte			S	R/C	S			S
5.4	Festlegung der Migrationstests			S	R/C	S			S
6	**Durchführung der Migration**								
6.1	Umsetzung der Migrationsplanung	A			R				C

Tabelle 29 (*fortgesetzt*)

Nr.	Aufgabe	IT-Leitung	IT-Entwicklung	IT-Betrieb	Projektleiter	Fachbereich	Betriebsrat	IT-Sicherheits-verantwortlicher	Cloud-Service-Anbieter
6.2	Durchführung von regelmäßigen Statussitzungen	A/S			R				C
6.2	Planung „point of decision“	A/S		S	R				C
7	**Nachbereitung der Migration**								
7.1	Einrichten der „task force“ zur Behebung von Schwierigkeiten in den ersten Tagen	A		S	R				C
7.2	Abschließende Sicherung aller Daten			R					
7.3	Rückbau der Alt-Systeme durchführen	A		S	R				
8	**Vorbereitung der Inbetriebnahme**								
8.1	Überprüfung der Performance, Verfügbarkeit und Support			S	A	S			R
8.2	Verbesserung des Services (wenn notwendig)	I		S	A	S			R
9	**Betriebsübergabe und Projektabschluss**								
9.1	Erstellen des Betriebshandbuches mit allen relevanten Prozeduren und Abläufen				A				R
9.2	Projektabschluss und Projektabnahme durchführen	A		R	S	S			C

4.5.2 Anpassung von Schnittstellen, Fachliche-Prozesse

Nachdem die auszulagernden Prozesse bzw. Services definiert wurden, müssen die Prozessteile, die im Unternehmen verbleiben, neu gestaltet und angepasst werden.

Die vom Cloud-Sourcing betroffenen Prozesse müssen genau bezüglich Tätigkeiten und operativen Verantwortlichkeiten zwischen Cloud-Sourcing-Geber und Cloud-Service-Anbieter abgegrenzt und die jeweiligen Mitwirkungspflichten definiert werden. Der Prozessteil, der im Unternehmen verbleibt, muss dabei „redesigned“ werden und ein Soll-Prozessmodell ist zu erstellen. Der auszulagernde Prozessteil liegt bezüglich des Designs in Verantwortung des Cloud-Service-Anbieters und ist zunächst somit von untergeordnetem Interesse. Das Soll-Prozessmodell enthält insofern nur den Prozessteil des Cloud-Sourcing-Gebers. Alle Prozessaktivitäten, die als Schnittstelle (Prozess, Systeme) zum Service Anbieter dienen, sollten bei der Prozessmodellierung besonders hervorgehoben werden.

Die Besonderheit von Cloud Computing Projekten ist, dass an vielen Stellen bewährte Mittel und Methoden zur Herstellung des IT-Betriebs nicht mehr ausreichen und/oder, dass Auswirkungen von Änderungen sich nicht auf einen isolierten Bereich beschränken. Die damit einhergehende Unsicherheit über den Erfolg eines Cloud Projektes sollte nicht abschrecken, sondern einer konkreten Untersuchung der eingesetzten Techniken und Prozesse weichen, um veränderte Bedingungen zu erkennen und bewerten zu können. Zusätzlich kommt hinzu, dass neben einem veränderten Betriebskonzept die Zusammenarbeit mit einem Cloud-Service-Anbieter auch bedeutet, den IT-Betrieb auf Standardprozesse und einen hohen Grad an Automatisierung anzupassen.

In unten stehender Tabelle sind beispielhaft Fragestellungen zu wichtigen Schnittstellen-Themen aufgeführt, die im Rahmen der Implementierung eines Cloud Computing Projektes auftreten und zu einer Neubewertung selbstverständlich gewordener IT-Praktiken führen können. Die konsequente Auseinandersetzung mit solchen oder ähnlichen Fragestellungen im Vorfeld der Implementierung sollte den Erfolg eines Cloud Projekts sichern und zu den erwünschten Lösungen führen.

Tabelle 30 — Bei der Implementierung zu berücksichtigende Aspekte

Schnittstellenthema	Fragestellung
Anforderungen an die IT-Sicherheit	— Sind die Sicherheitsstandards /-konfigurationen des Cloud-Service-Anbieters kompatibel mit den unternehmenseigenen? — Müssen Firewall-Einstellungen angepasst werden, um einen Datentransfer zwischen Unternehmen und Cloud-Service-Anbieter zu erlauben und entspricht dies dann noch den internen Sicherheitsrichtlinien? — Ist die Netzwerkverbindung zum Cloud Anbieter auch für sensitive Daten sicher?
Komplexität von technischen und Prozess-Schnittstellen	— Sind Software- oder Hardwareaktualisierungen notwendig, um in ein Cloud-Konzept migrieren zu können? — Müssen Prozesse neu gestaltet werden? — Sind Zugriffsberechtigungen auf technische Systeme, Betriebswerkzeuge oder Daten ausreichend segmentiert und standardisiert, um Dritten die Steuerung und Betrieb einzelner Teile zu ermöglichen? — Sind die bisherigen Authentifizierungsprozesse und die Zugriffskontrolle von Personen und IT-Prozessen ausreichend? — Mit welchen grundsätzlichen Veränderungen muss ein Benutzer rechnen (z. B. andere Ansprechpartner, mehr „Self-Service“)?
Anpassungsbedarf der technischen Infrastruktur	— Ist die Bandbreite des Wide Area Netzwerks ausreichend, um einen performanten Benutzerzugriff zu erlauben? — Entstehen Zusatzkosten durch die Anbindung des Cloud Anbieters an das unternehmenseigene Netzwerk? — Ist die Bandbreite des Netzwerks ausreichend für den erforderlichen Datenaustausch zwischen verbundenen Anwendungen, die an verschiedenen Standorten betrieben werden?
Grad der Standardisierung der IT und der Betriebsprozesse	— Ist der Leistungsschnitt des IT-Betriebs im Unternehmen marktkonform und können somit Teile desselben fremdbetrieben werden? — Welche Informationen werden an der Schnittstelle zum Cloud Anbieter erwartet? Sind diese mit den bisher genutzten Informationen kompatibel oder finden Veränderungen statt? Liegen erwünschte Daten überhaupt vor? — Welche Reports und Kennzahlen sind notwendig, um die Qualität des Cloud-Betriebs zu bewerten? — Wie werden die Cloud Dienste abgerechnet? Kann die Abrechnung überprüft werden und ist die Art der Abrechnung kompatibel mit dem unternehmenseigenen Abrechnungsmodell?
Kosten der Transformation	— Sind Kosten für HW (en: Hardware) oder SW (en: Software) Aktualisierungen geplant? — Sind Kosten für Schulung von Mitarbeitern berücksichtigt? — Wären Investitionskosten in IT-Technologie auch auf andere Cloud Anbieter übertragbar?

4.5.3 Vorbereitungsphase

In der ersten Projektphase werden die Standards für die Zusammenarbeit im Projekt festgelegt. Grundsätzlich unterscheiden sich die Anforderungen vorerst nicht wesentlich von denen anderer (nicht Cloud) Projekte. Es werden:

- Projektziele abgeleitet und die Projektkommunikation initial festgelegt;
- die Projektorganisation aufgestellt;
- Projektdokumentation und –ablage bestimmt;
- ein Projektplan erstellt und ein Projekt-Risikomanagement etabliert.

Im Gegensatz zu anderen Projekten, welche den zuvor aufgelisteten Bereichen zwar auch jeweils eine unterschiedliche Gewichtung zuweisen, erhalten in einem Cloudprojekt diese jedoch eine grundlegend andere Gewichtung.

Die Ableitung der Projektziele sollte deutlich machen, warum ein Cloud Projekt gestartet wurde und welche Vorteile das Ergebnis bietet. Dies ist die erste Gelegenheit, nicht nur das Projekt vorzustellen, sondern auch verschiedene Interessengruppen auf mögliche Veränderungen vorzubereiten. In anderen Projekten sind die Adressaten meistens eindeutiger festgelegt als bei Cloud Projekten. In den ersten Cloud Projekten ist die Wahrscheinlichkeit sehr hoch, dass Änderungen an der existierenden IT-Struktur stattfinden (z. B. veränderte Authentifizierung). Entsprechende flankierende Infrastrukturänderungen können daher im Vorfeld einer Cloud-Migration notwendig sein.

Die Aufstellung der Projektorganisation, der Projektplan sowie das Risikomanagement sind nicht nur von Zeitplanung und Ressourcen im eigenen Unternehmen abhängig, sondern werden auch von den Vorgaben des Cloud-Service-Anbieters und den Standards der eingekauften Cloud Services, dem Team des Cloud-Service-Anbieters und den identifizierten Risiken der zukünftigen Cloud Nutzung bestimmt. Es sollte erwartet werden, dass die Projektorganisation prinzipiell breiter aufgestellt ist als in anderen Projekten, da der Cloud-Service-Anbieter mit einbezogen werden muss (sofern er nicht selber das Projekt leitet). In Public Cloud Projekten ist meist das Gegenteil der Fall, da der Service-Anbieter davon ausgeht, dass die Projektarbeit vollständig auf Seiten des Auftraggebers geleistet wird. Eine persönliche Interaktion zwischen dem Service-Anbieter und dem Auftraggeber erfolgt in Public Cloud Projekten meist nicht. Die Ausrichtung der Projektplanung an Vorgaben und Standards des Cloud Anbieters, sowie möglichen vertraglichen Regelungen und Terminen, muss verstärkt Ressourcen im Projekt berücksichtigen, die nur kurze Zeit gezielte Beiträge zum Projekt leisten, aber nicht grundsätzlich am Projekt beteiligt sind (z. B. bei Änderungen an Netzwerk-Konfigurationen, Software-Aktualisierungen). Neben der bereits zuvor angeführten individuellen Komplexität eines Cloud Projektes ist hier eine gute und konstante Kommunikation der Projektziele und des Projektfortschritts ein Schlüssel zum Erfolg.

Das Risikomanagement des Projektes steht insofern im Fokus, als dass Sicherheit der IT und moderne IT-Technologien grundsätzlich hohes Interesse bei der Geschäftsführung eines Unternehmens auslösen.

Grundsätzlich wird die Projektplanung eines Cloud Projektes auf festgeschriebene Bestandteile aus dem Vertrag oder den beauftragten Services bezogen. Die Freiheitsgrade für die Gestaltung sind insofern eingeschränkt. Ebenso muss die Beteiligung des Anbieterprojektteams am Projekt bewertet werden. Der Fokus liegt auf der Implementierung standardisierter Services mit vorab definierten Betriebsmechanismen.

4.5.4 Design Sollkonzept

4.5.4.1 Organisatorische Auswirkungen und Verantwortlichkeit im Unternehmen

Durch die Einführung von Cloud Services können sich in einem Unternehmen Änderungen auf verschiedenen Ebenen der Organisation ergeben. Diese Auswirkungen müssen frühzeitig adressiert werden, sodass das Unternehmen zum Zeitpunkt der Auswahl eines Cloud Services entsprechend vorbereitet ist (siehe 4.5.2).

Durch die Einführung von Cloud Services können sich die angestammten Rollen und Verantwortlichkeiten zwischen Fachbereichen und IT verändern. Es ist u. a. möglich, dass der Cloud Service aus der organisatorischen Entscheidungsgewalt der IT-Organisation in Richtung von Schlüsselanwendern (Key User) aus den Fachbereichen verlagert wird. Hier sind klar die Entscheidungshoheit und auch die nachfolgende Verantwortlichkeit für eine organisatorische Betreuung des Cloud Service im Unternehmen zu klären.

4.5.4.2 Business Value

Cloud Services stellen primär standardisierte Services dar. Daher bedeutet ihre Einführung oft eine Anpassung von bestehenden Abläufen und teilweise eine Einschränkung im Vergleich zu bestehenden Services im Sinne der bereichsspezifischen Bedürfnisse. Aus diesem Aspekt ist die Business Value Betrachtung auf der reinen Kostenebene zumeist zu kurz gegriffen. Die Aufbereitung und Kommunikation des Mehrwerts (schnelle und vereinfachte Einführung neuer Technologien, Flexibilität der Lizenzierung, Anbindung mobiler Mitarbeiter, etc) für die unterschiedlichen betroffenen Gruppen auf Basis ihrer Bedürfnisse ist somit neben einer „ehrlichen“ Kostenbetrachtung notwendig.

4.5.4.3 Anpassung der Prozesse

Anhand der Ergebnisse des Assessments sollten jene Prozesse identifiziert worden sein, die beim Umstieg auf den Cloud Service geändert werden müssen. Bei der Anpassung der Prozesse sollte auf folgende Punkte Rücksicht genommen werden:

- Wie häufig wird der Prozess je Zeiteinheit ausgeführt?
- Ergeben sich durch die Nutzung des Cloud Services Änderungen in der Häufigkeit?
- Wird der Prozess dadurch wichtiger oder verliert er an Relevanz?
- Gibt es geänderte Ansprechpartner und Verantwortliche, von denen einige auch außerhalb des Unternehmens sitzen?
- Existieren Schnittstellen und „Single Points of Contact“ innerhalb des Unternehmens, über die möglicherweise die Kommunikation zu bündeln ist?
- Entstehen geänderte Voraussetzungen zur Nutzung eines Services (z. B. Kenntnis der Kundennummer, geänderte Identifikationsprozeduren)?
- Gibt es andere, in der Regel längere Antwortzeiten als bisher? Dies kann auch dazu führen, dass Prozesse geteilt werden müssen.

Die Bereinigung der Prozesse kann mit Hilfe einer Prozessmodellierungsmethode durchgeführt werden.

4.5.4.4 Erhebung von Mengengerüsten und Bereinigung von Daten

Die IT ist in vielen Unternehmen historisch gewachsen. Dies bedeutet in den meisten Fällen, dass die Anforderungen sehr auf die Wünsche und Besonderheiten der User angepasst wurden. Insbesondere trifft dies auf die für IT-Services genutzten Mengen zu.

Beispiele sind:

- genutzter Speicherplatz auf Fileservern;
- Speicherverbrauch für persönliche Dateien;
- Größen von E-Mail-Postfächern;
- Upload- und Download-Volumen.

Beim Umstieg auf Cloud Services ergibt sich eine gute Gelegenheit, die gewachsenen Datenmengen zu bereinigen, d. h. es werden nur tatsächlich für den laufenden operativen Betrieb benötigte Informationen migriert. Die bereits bestehenden Daten können in geeigneter Form archiviert werden.

Durch diese Bereinigung kann man die Nutzung des Cloud Services mit einem geringeren Ausgangdatenvolumen beginnen und so die initialen Kosten reduzieren (z. B. Nutzung günstigerer Cloud Service-Pakete). In Ausnahmefällen kann es auch sein, dass der Cloud-Service-Anbieter Limits bezüglich der Nutzung von Ressourcen, wie z. B. Speicherplatz definiert. Auch in diesen Fällen müssen vorab Datenbereinigungen stattfinden. Folgende Schritte sollten bei der Erhebung der IT-Mengen/Mengengerüste erfolgen:

- Identifikation der Datenvolumina für das Mengengerüst in Form einer Liste;
- Einteilung, welche Datenvolumina vom Umstieg auf Cloud Services betroffen sind; im Weiteren sollen nur die betroffenen Datenvolumina behandelt werden;
- Erhebung des tatsächlichen Verbrauchs des letzten Jahres / der letzten Perioden;
- Erhebung des Volumenwachstums pro zu definierender Zeiteinheit (z. B. Jahr oder Quartal).

4.5.4.5 Abhängigkeit vom Schnittstellenumfang

In aller Regel erlaubt eine echte SaaS-Applikation keinen direkten Zugriff auf die Datenbanken, welche der Applikation zugrunde liegen. Der Anbieter gewährt Zugriff auf die Daten in der Applikation ausschließlich über Schnittstellen mit Soap-Web-Services, REST, CSV-Dateien etc. Somit gilt, dass alles, was nicht durch diese Schnittstellen passt, nicht exportiert oder importiert werden kann – zumindest nicht mit Standardmitteln.

- Kandidaten hierfür sind je nach System Dateianhänge, Zeitstempel für Erzeugung und Aktualisierung von Datensätzen, Reports, Sichtbarkeitsregeln, Zugriffsrechte, Custom-Metadaten etc.
- Strikte Vorgaben beim Datenformat, feste Vorgaben für die Formatierung von Datenfeldern – korrektes E-Mail Format für E-Mail-Adressen, vordefinierte Pick-Lists, Einmaligkeit von Feldeinträgen bei Schlüsseln, Beschränkungen der Zeichenanzahl etc. – werden von den Anbietern bzw. in der Konfiguration bewusst vorgegeben, um die Datenqualität im laufenden Betrieb hochzuhalten.

Cloud-Applikationen sind nahezu immer strikter als traditionelle Lösungen, da für sie wie oben erwähnt Schnittstellen bewusst definiert sowie implementiert werden müssen und Speicherplatz wie auch Datenstrukturen für einen kosteneffizienten Betrieb beim Anbieter möglichst schlank gestaltet werden. Eine Herausforderung stellen die strikten Vorgaben dar, aus einem anderen System stammenden Daten, welche im Ausgangsformat nicht diesen Vorgaben entsprechen, zu importieren.

4.5.5 Vorbereitung der Migration

Die Migration in die Cloud ist für die meisten Unternehmen nicht dem „Tagesgeschäft“ zugehörig. Eine gute Vorbereitung und eine adäquate Wahl der Migrationsmethode sind ebenso relevant wie eine erhöhte Aufmerksamkeit während der Migration. Manche der nachfolgenden Schritte können bereits sehr früh – parallel zu den strategischen Überlegungen und der Auswahl des Cloud-Service-Anbieters – begonnen werden.

Grundsätzlich stehen je nach Unternehmensgröße und Service folgende unterschiedlichen Migrationsarten zur Verfügung:

- **Big Bang** (Umstieg in einem Schritt): In einer Big-Bang-Migration wird der gesamte Service für alle Benutzer zum gleichen Zeitpunkt umgestellt. Eine Umstellung dieser Art verlangt gute Planung und normalerweise eine bis zwei Testmigrationen. Insbesondere sind Migrationsaktivitäten mit langer Laufzeit kritisch für eine Big-Bang-Migration (z. B. Kopieren der gesamten Dateien etc.). Der besondere Vorteil dieser Migrationsvariante liegt im Entfallen eines etwaigen Doppelbetriebes. Die Big-Bang-Migration wird dort angewendet, wo ein Doppelbetrieb kostenintensiv und organisatorisch schwer durchzuführen ist.

- **Schrittweise Migration**: Die phasenweise Migration erfolgt in mehreren Schritten. Bei den einzelnen Schritten werden bestimmte Gruppen von Benutzern (funktionale oder organisatorische Gruppen) migriert. Durch die Größe dieser Schritte kann die Komplexität gut gesteuert werden. Während der Gesamtmigration ist ein Doppelbetrieb der Services aufrechtzuerhalten. Die Schritte werden in der gleichen Form durchgeführt, d. h. die Migrationsmannschaft gewinnt mit jedem Schritt mehr Erfahrung und die Qualität der Migration steigt daher.

- **Optionaler Pilotbetrieb**: Der Pilotbetrieb kann sowohl vor einer Big-Bang-Migration als auch vor einer schrittweisen Migration verwendet werden. In dieser Phase wird der Service für eine ausgewählte Gruppe von Usern bereitgestellt. Anhand der Erfahrungen dieser Pilot-User werden Erkenntnisse für die Migration erarbeitet. Die gewonnenen Erkenntnisse fließen in die Dokumentation sowie auch in den technischen Migrationsablauf ein.

Die Wahl der Migrationsmethode sollte so früh wie möglich erfolgen. Bei der Wahl sollten sich die Verantwortlichen sowohl vom Cloud-Service-Anbieter als auch von internen und externen Experten beraten lassen. Für jeden Cloud Service existiert Expertenwissen über die zu präferierende Methode.

Ist die Migrationsart festgelegt, so ist die Entscheidung über einen optionalen Pilotbetrieb zu treffen. Der Pilotbetrieb sollte in einer Art und Weise gestaltet sein, dass die Benutzer den Cloud Service anstelle des alten Services nutzen. Eine Nutzung parallel zum bisherigen Service hat sich als nicht besonders erkenntnisgewinnend herausgestellt.

4.5.6 Planung der Migration

In einer Migration wird ein System von einem Ausgangszustand erfolgreich in einen Zielzustand versetzt. Die Migration umfasst alle Schritte, die notwendig sind, um diese Transformation zu ermöglichen.

Wichtige Voraussetzungen sind die Kenntnis über den Ausgangszustand und den Zielzustand sowie eine geeignete Beschreibungsform. Informationen über den Ausgangszustand sind in der Regel aus den folgenden Quellen zu erhalten:

- Der internen IT-Abteilung;
- Spezialisten als Migrationsbegleiter;
- Mithilfe eines Fragenkataloges, den der Cloud-Service-Anbieter zur Verfügung stellt.

Wichtig ist, dass alle relevanten Fakten, Konfigurationen, Einstellungen, Mengen etc. berücksichtigt werden. Die Erfahrung zeigt, dass der Ausgangszustand auch bei guter Dokumentation nur in den seltensten Fällen ausreichend detailliert erfasst ist.

Eine Beschreibung des Zielzustandes ist u. a. aus folgenden Quellen zu erhalten:

- der internen IT-Abteilung in Zusammenarbeit mit den Spezialisten des Cloud-Service-Anbieters;
- Spezialisten als Migrationsbegleiter;
- Cloud-Service-Anbieter aufgrund seiner Erfahrung, in diesem Fall muss jedoch ein Quercheck mit dem Planungsteam auf Vollständigkeit und Verständlichkeit erfolgen.

Sind der Zielzustand und die Ausgangslage ausreichend beschrieben, so ist der darauf folgende Schritt die Planung der Migration. Dabei sind zu berücksichtigen:

- Alle technischen und organisatorischen Schritte vor der Migration. Ziel sollte sein, alle Vorbedingungen für den Start der Migration zu erarbeiten.
- Alle Schritte während der Migration. Hier ist empfohlen, mehrere Meilensteine an markanten oder kritischen Punkten der Migration zu identifizieren. Diese Schritte enden in der Regel in einer „GO“-Entscheidung.
- Alle Schritte, die nach einer „GO“-Entscheidung notwendig sind bis zur Aufnahme des Regelbetriebes.
- Alle Schritte, die nach einer „NO-GO“-Entscheidung notwendig sind, um den ursprünglichen Zustand wiederherzustellen.

Diese Planung kann in mehreren Workshops erfolgen, in denen neben „Best Practices“ der Beteiligten auch der Plan iterativ verfeinert wird. Nach den Workshops sollte der Gesamtplan immer an alle Teilnehmer kommuniziert werden.

Hat der Plan eine finale Version erreicht, sollte über die Migrationstests entschieden werden. Fragestellungen sind:

- Wie umfangreich wird getestet (Anzahl der Systeme; Umfang der Daten)?
- Wird ein voller Migrationszyklus getestet (inklusive Probebetrieb)?
- Anhand welcher Kriterien wird eine „GO“-Entscheidung gefällt?
- Wird der „NO-GO“-Fall (Rückstieg) geprobt?

Endergebnis sind ein Migrationsplan und ein Plan für den Ablauf der Test- und Echtmigrationen.

4.5.7 Durchführung der Migration

Jede Migration ist individuell. Daher lassen sich an dieser Stelle nur allgemeine Grundsätze zur Durchführung der Migration geben.

Die wichtigsten Punkte für Migrationen zu Cloud-Service-Anbietern sind:

- Einbau von Pufferzeiten in den Migrationsplan und Nutzung dieses Puffers in der Migrationsphase.
- Im Zuge des Risikomanagements ist ein Fallback-Plan zu definieren, der im Falle einer fehlgeschlagenen Migration greift.
- In der Planung neigen Experten dazu, zu optimistische Durchlaufzeiten anzugeben. Einzelne zeitliche Verlängerungen sollten mit eingeplant werden.
- Planung eines „Point-of-Decision“ für das Treffen der „GO“-/“NO-GO“-Entscheidung und konsequente Entscheidung zu diesem Zeitpunkt (etwaige zeitliche Puffer sollten daher vor diesem Punkt liegen).
- Nutzen der Erfahrungen des Cloud-Service-Anbieters, sowie der Erfahrungen der internen IT.

Einplanung eines „kleinen Chaos“ für den ersten Betriebstag, trotz aller Vorbereitung und Kommunikation: Insbesondere ein verstärktes Support-Team und eine schnelle Eingreiftruppe haben sich für den ersten Tag danach bewährt. Da es sich um IT-Services handelt, ist in den ersten Stunden nach der Migration ein Handout mit den wichtigsten Informationen eine wertvolle Unterstützung für die Endbenutzer.

4.5.8 Nachbereitung der Migration

Nach der erfolgreichen Migration werden kleinere Probleme zum Nachbessern verbleiben. Für diese Probleme ist die Einrichtung von Frequently Asked Questions (FAQs) eine große Hilfe für die Benutzer. In der Nachbereitung ist ein wesentlicher Aspekt der Rückbau der Alt-Infrastruktur.

Nachdem die Migration bei vielen Projekten ausreichend geübt ist, wird der Rückbau der Alt-Infrastruktur in vielen Fällen ohne vorherige Probe durchgeführt. Neben Seiteneffekten der Abschaltung von Services oder Hardware ist hierbei ein wichtiges Risiko der eventuelle Verlust von Daten. Sind diese Risiken jedoch bekannt, so kann der Rückbau in kleinen Schritten und risikovermeidend geplant, getestet und durchgeführt werden. Die letzte Sicherung der Daten (vor der Migration) ist zu archivieren und in Abhängigkeit der gesetzlichen Aufbewahrungsfrist auf einem entsprechenden Medium zu archivieren. Darüber hinaus ist ggf. sicherzustellen, dass ein System für die Einsichtnahme in die Daten vorzuhalten ist.

4.5.9 Vorbereitung der Inbetriebnahme

Vor der endgültigen Inbetriebnahme der Cloud-Services sollten die folgenden Themen einer besonderen Prüfung unterzogen werden, bzw. sollten Beachtung finden:

- Support,
- Performance;
- Verfügbarkeit;
- Verbesserung.

l) Support

Der Einsatz von Cloud Services bedeutet vorrangig eine Änderung des Serviceprozesses. Diesbezüglich ist zu definieren, wer Serviceanforderungen erfasst, und wie diese kommuniziert sowie möglicherweise eskaliert werden. Die unterschiedlichen Möglichkeiten des Supports wurden bereits in der Auswahl des Cloud Services und des Cloud-Service-Anbieters geklärt und sind den Anwendern zu kommunizieren.

m) Performance

Potenzielle Engpässe sollten einerseits durch den Cloud-Service-Anbieter proaktiv kommuniziert und bei Bedarf durch unternehmensinterne Performance-Messungen kontrolliert werden. Durch die definierten Servicelevel-Vereinbarungen ist in diesem Punkt der Serviceverantwortliche gefordert, die Einhaltung der Performance und Verfügbarkeitsgarantien zu verifizieren sowie mögliche weitere Ressourcen zu skalieren.

n) Verfügbarkeit

Der Serviceanbieter wird im kontinuierlichen Zyklus Patches und Updates einspielen. Die entsprechenden Informationen müssen vom Cloud-Service-Anbieter zur Verfügung gestellt werden und sind vom Cloud-Sourcing-Geber mit dessen Updatezyklen zu synchronisieren.

o) Verbesserung des Services

Für Cloud Services, die unternehmenskritische Prozesse abdecken, kann es sinnvoll sein, bereits bei der Auswahl eines Cloud-Service-Anbieters die Anforderung und das Kriterium zu definieren, bei welchem eine regelmäßige Evaluierung des Services stattfinden soll. Diese Evaluierung und deren Ergebnisse können je nach Anforderung im Sinne eines Reportings (Service Level-Reporting, durch den Cloud-Service-Anbieter durchgeführte Audits, durchgeführte Verbesserungen) erfolgen oder – soweit der Cloud-Service-Anbieter diese Möglichkeit ebenfalls vorsieht – im Rahmen eines Feedbackgesprächs stattfinden. Die Möglichkeit einer persönlichen Betreuung wird eher der Ausnahmefall sein, sollte aber bei unternehmenskritischen Services als Möglichkeit in Betracht gezogen werden. Im Gespräch selbst liegt das Hauptaugenmerk auf der zukünftigen Verbesserung des Betriebes und Vermeidung der aufgetretenen Fehler und weniger in der Feststellung der Schuldfrage.

4.5.10 Betriebsübergabe und Projektabschluss

Das Projekt wird abgeschlossen und eine detaillierte „Betriebsplanung“ für die produktive Phase erstellt. Das Produktivsystem wird eingespielt, geprüft und es erfolgt nun die Freigabe des Systems.

Für die Betriebsplanung ist ein Betriebshandbuch (Operational Manual) mit den folgenden Kapiteln sinnvoll (Auszug):

1) System-Liste (Run Inventory)

Liste mit allen Batch Jobs, bestehend aus Namen der Batch-Jobs, Aufgabe des Jobs, System auf dem die Jobs laufen.

Liste mit allen transaktionsbasierenden Software Komponenten, die beim Hochfahren bzw. Runterfahren eines Systems nacheinander gestartet bzw. gestoppt werden müssen.

2) Ablaufkalender (Run Sequence)

   Ein Kalender aus dem hervor geht, in welcher Reihenfolge und zu welchem Zeitpunkt ein bestimmtes Softwaresystem oder ein Batch Job läuft. Folgende Inhalte sollten hierbei aufgeführt werden:

   a) Wochentag der Ausführung (oder Monat),

   b) Uhrzeit der Ausführung (wenn notwendig);

   c) Erwartete Laufzeit;

   d) Abhängigkeiten zu anderen Jobs.

3) Diagnoseprozeduren
   Beschreibung der Diagnose- und Fehlererkennung des Systems.

4) Fehlermeldungen
   Liste mit allen Error Codes und Meldungen.

5) Kontaktliste
   Ansprechpartner für die einzelnen Anwendungen mit allen notwendigen Kontaktdaten.

6) Restart/Recovery Prozeduren
   Prozeduren die bei einem Restart oder bei der Wiederherstellung notwendig sind.

7) Backup Prozeduren
   Beschreibung der Prozeduren für das Backup.

8) Eskalationsprozeduren
   Beschreibung der Verfahren, die bei einer Eskalation anzuwenden sind.

Das Betriebshandbuch wird zum Betriebsstart vom Projektteam an den Verantwortlichen im Bereich „Operations“ übergeben und von diesem freigegeben.

4.5.11 Abschluss-Workshop

Das Gegenstück zum Kick-off-Workshop ist der Abschluss-Workshop. In dessen Rahmen blickt das Projektteam auf das Projekt zurück und gibt gegenseitig Feedback. Das gewonnene Wissen wird abschließend dokumentiert, die Übergabe der Projektergebnisse an die Betriebsorganisation und der Abschlussbericht werden vorbereitet. In der Folge wird das Projektteam entlastet, sichert die Daten und Dokumente und baut die entstandene Infrastruktur zurück.

Inhaltlich sollte ein Projektabschluss-Workshop den eigentlichen Projektabschluss vorbereiten. Dieser Workshop hat zum Ziel, alle Aufgaben der Beteiligten bis Projektende zu definieren.

Ein wesentlicher Teil ist der Abschluss der Projektdokumentation. Hier sollte vor allem geklärt werden, wie und wo die Projektdokumentation abgelegt wird und wer zukünftig Zugriff darauf erhalten soll.

Gleichzeitig ist ein zukünftiger Ansprechpartner für Sachverhalte das Projekt betreffend festzulegen. Ggf. sind hierfür auch entsprechende Ressourcen vorzusehen. Außerdem muss geklärt werden, wer die ggf. noch ausstehenden Restarbeiten mit wessen Unterstützung bis wann ausführt.

Ein weiterer wichtiger Punkt ist das gegenseitige Feedback: es kann sowohl positive wie auch negative Aspekte umfassen. Ziel ist es nach dem Projekt „reinen Tisch“ zu machen und Erfahrungen für künftige Projekte zu sichern („Lessons Learned“).

4.6 Betrieb

4.6.1 Wesentliche Fragen

- Wie lässt sich ein effizienter Betrieb von Cloud-Lösungen gewährleisten?
- Wie erfolgt die Berücksichtigung des Cloud-Charakteristikums Selbstbedienung im Betrieb?
- Wie ist ein sicherer und zuverlässiger Betrieb von Cloud-Lösungen möglich?
- Wie kann Netzwerkabhängigkeit im Betrieb reduziert werden?

— Wie erfolgt die Berücksichtigung der Cloud-Charakteristika Elastizität im Betrieb?

— Welche Aspekte sind im Betrieb auf Grund des Anspruchs nutzungsabhängiger Verrechnung zu berücksichtigen?

Tabelle 31 — Verantwortlichkeiten während des Betriebs

Nr.	Aufgabe	IT-Leitung	IT-Entwicklung	IT-Betrieb	Projektleiter	Fachbereich	ITi-Scherheits-verantwortlicher	Cloud-Service-Anbieter
1	**Bereitstellung**	A	S	R	(R)	I	I	R
1.1	Initiale Bereitstellung	A	S	R	(R)	I	I	R
1.2	Laufende Bereitstellung.	A		R		I	I	R
1.3	Außerbetriebnahme	A	S	R	(R)	I	I	R
2	**Sicherstellung Schnelligkeit**	A	S	R	(R)	C	I	R/S
2.1	Sicherstellung infrastruktureller Voraussetzungen	A	S	R	(R)	C	I	R
2.2	Konzeption schlanker Prozesse und kurzer Weisungswege	A	S	R	(R)	C	I	S
2.3	Programmierte Administration	A	S	R	(R)	C	I	S
3	**Selbstbedienung**	**A**	**R**	**C/S**	**(R)**	**R/I**	**I**	**S**
3.1	Realisierung SB-Infrastruktur	A	R	C	(R)	C	C	S
3.2	Nutzer-Administrationsanforderungen	I				R/A	I	
3.3	Berechtigungsanforderungen	I				R/A	I	
3.4	Nutzer-Administration-Freigabe	I		R		I	I	R/I
3.5	Berechtigungsanforderungen Freigabe	I		R		I	I	R/I
4	**Betriebssicherung**	**I**	**S**	**R**	(R)	**I**	**A**	**R**
4.1	Sicherstellung von Voraussetzungen für Betriebssicherung	A	S	R	(R)	I	A	R/C
4.2	Realisierung von Fail-Over	A	S	R	(R)		R	R
4.3	Realisierung von Verschlüsselung	A	S	R	(R)		R	R
4.4	Reduktion von Netzwerkabhängigkeit	A	S	R	(R)		R	R
5	**Elastischer Betrieb**	**I/A**		**C/R**		**R**		**C/R**
5.1	Bedarfsmeldungen zu Kapazitäten	I		C		R		C
5.2	Anpassung der Kapazitäten	A		R		I		R
6	**Monitoring**	**A**		**R**	(R)	**C**	**C**	**R**
6.1	Sicherstellung der Monitoring-Voraussetzungen	A		R	(R)	C	C	R
6.2	Implementierung des Monitoringssystems	A		R	(R)	C	C	R
6.3	Durchführung des Monitorings	A		R		I	I	R
7	**Qualitätsmanagement**	**A**	**S**	**R**		**C**	**C**	**S**
8	**Changemanagement**	**A**	**S**	**R**		**S**	**C**	**R**

Tabelle 32 — Ergebnisdokumente der Phase „Betrieb“

Dokument ID	Dokument Bezeichnung	Dokument Beschreibung	Dienstschicht	Betriebsmodell
3.5 – A	Betriebshandbuch	Stellt in Bezug auf den Betrieb der Cloud-Lösung notwendige Tätigkeiten inklusive Verantwortlichkeiten dar. Dokumentiert die wesentlichen logischen und ggf. physischen Systeme.	Alle	Jedes
3.5 – B	Notfallhandbuch	Stellt Maßnahmen bei Störung oder Ausfall der Cloud-Lösung inklusive Verantwortlichkeiten dar.	Alle	Jedes
3.5 – C	Selbstbedienungshandbuch	Stellt die Infrastruktur zur Selbstbedienung dar und dokumentiert die vereinbarten Freigabewege und Verantwortlichkeiten.	Alle	Jedes

4.6.2 Beschreibung allgemein

Für den Betrieb von Cloud-Lösungen gelten zunächst dieselben Anforderungen, wie für den allgemeinen IT-Betrieb. Es wird das Ziel verfolgt, eine existierende Lösung sicher, effizient und zuverlässig zu betreiben. Zu diesem Zweck wird eine routinierte Arbeitsorganisation, Infrastruktur und ein auf dieser Basis integrativ betriebenes Werkzeugsystem entwickelt, das zur Zielerreichung notwendige Tätigkeiten, möglichst effektiv durchzuführen hilft.

Aus den spezifischen Charakteristika des Cloud Computings ergeben sich spezielle Anforderungen für den IT-Betrieb. Die physischen IT-Systeme selbst sind weniger zu berücksichtigen, da Cloud-Lösungen entweder komplett durch Dritte betrieben werden, oder aber zumindest von der eigentlichen Hardware abstrahierende Virtualisierungslösungen eingesetzt werden.

Im Fall von Private-Cloud-Lösungen ist deren Betrieb allerdings dem traditionellen IT-Betrieb verteilter Anwendungssysteme sehr ähnlich. Das Private-Cloud-Betriebsmodell erfordert neben den im Folgenden für alle Betriebsmodi geltenden Überlegungen, die Berücksichtigung administrativer Maßnahmen, die geeignet sind mit hoch-volatilen und –virtualisierten verteilten Infrastruktursystemen umzugehen – die Behandlung dieser Sachverhalte bleibt entsprechender Fachliteratur vorbehalten.

4.6.3 Effizienter Betrieb und Selbstbedienungsbetrieb

Mit dem Cloud Computing geht der Anspruch von Schnelligkeit im Betrieb einher. Diese Forderung nach Schnelligkeit wird zum einen an die initiale Bereitstellung, den laufenden Administrationsbetrieb aber auch die Außerbetriebnahme der Lösungen gestellt.

Wesentliches Hindernis einer schnellen Administration ist die Notwendigkeit manueller Tätigkeiten. Manuelle Tätigkeiten sind daher soweit wie möglich durch programmierte Administration zu ersetzen. Im Rahmen der programmierten Administration werden sämtliche manuelle Tätigkeiten, die für die Inbetriebnahme von Cloud-Lösungen, die flankierenden administrativen Tätigkeiten im Bereich Nutzer-Administration und Berechtigungsverwaltung, aber auch die Tätigkeiten, die bei einer Abschaltung eingesetzter Cloud-Lösungen notwendig sind, durch parametrisierbare Programmaufrufe ersetzt.

Die Realisierung entsprechender Programme ist keine typische Administrationsaufgabe. Damit diese notwendigen Programme dennoch entwickelt werden können, empfiehlt es sich den Administratoren – zumindest in der Einführungsphase einer Lösung - Softwareentwickler mit Erfahrung im Bereich Infrastruktur- und Administrationsautomatisierung zur Seite zu stellen. Sollte es innerhalb einer Organisation keine entsprechenden Softwareentwickler geben, so ist es sinnvoll sich entsprechende externe Services einzukaufen.

Damit administrative Programme effizient entwickelt werden können, ist es weiterhin notwendig, dass eingesetzte Cloud-Lösungen über Programmierschnittstellen verfügen, die deren einfache Integration in das administrative Werkzeugsystem ermöglichen.

Im optimalen Fall werden organisatorisch bedingte Anforderungen an die Systemadministration, wie beispielsweise die Notwendigkeit neue Nutzer oder Berechtigungen anzulegen, durch die Nutzer der Fachbereiche selbst ausgelöst. Die Administration übernimmt dann lediglich noch eine überwachende und freigebende Aufgabe gegenüber den durch die organisationsinternen Nutzer der Cloud-Lösung selbst angestoßenen administrativen Programmausführungen. So ist es zur Berechtigungsverwaltung beispielsweise sinnvoll, dem Vorgesetzten eines Fachbereichs eine Möglichkeit zu geben, dass er seinen Mitarbeitern organisationsobjektbezogene Berechtigungen erteilt. Die an den Organisationsobjekten orientierte fachliche Berechtigungsvergabe erzeugt dann einen Arbeitsvorrat potentieller Programmaufrufe, die von der Administration lediglich zur Ausführung freigegeben werden müssen. Dem sogenannten „Zero-Touch-Cloud"-Gedanken vollends folgend, kann auf eine administrative Freigabe gar absolut verzichtet werden, in diesem Fall erfolgt die administrative Freigabe automatisch durch Freigabe eines vorgesetzten Fachbereichsleiters.

Die integrative Berücksichtigung durch die Nutzer des Systems selbst angebahnter administrativer Tätigkeit wird dem Cloud-Charakteristikum der Selbstbedienung gerecht. Die fachlichen Nutzer von Cloud-Lösungen sollten beispielsweise selbst in der Lage sein, benötigte Benutzer anzulegen, zu ändern und zu löschen - oder zumindest die Anbahnung und Vorbereitung dieser administrativen Vorgänge in einer Weise durchführen können, dass mit ihr eine Reduktion der Arbeitsbelastung der Administration der Systeme einhergeht. Dies führt auch zu deutlich beschleunigten Prozessen.

Häufig bringen Cloud-Lösungen bereits eigene Funktionalität für die fachliche Berechtigungsvergabe mit sich. Die Existenz solcher Funktionalität reduziert oft allerdings nicht die Notwendigkeit der Entwicklung administrativer Programme. Cloud-Lösungen können oft lediglich effizient betrieben werden, wenn sie mit anderen Anwendungssystemen, die bereits in einer Unternehmung existieren, eng verknüpft werden. Da fachliche Berechtigungsvergaben in einer Cloud-Lösung somit unter Umständen die Notwendigkeit flankierender Berechtigungsvergaben in anderen eingesetzten Systemen mit sich bringen - deren Umsetzung die Administration bei Notwendigkeit manueller Tätigkeit qualitativ oder quantitativ überfordern könnte - ist gründlich zu prüfen ob administrative Programme zu entwickeln sind.

Grundsätzlich ist – bevor evtl. die Entscheidung für die Entwicklung administrativer Programme getroffen wird – zu klären, ob nicht bereits Standardsoftware für entsprechende Aufgaben am Markt erhältlich ist und diese ggf. eine wirtschaftlichere Problemlösung darstellt.

Für den Fall der Problematik verteilter und stark volatiler Berechtigungen in verteilten Anwendungssystemen existieren z. B. Identity Management Lösungen (IDM-Lösungen), die – allerdings auch lediglich durch Anpassungsentwicklung – in der Lage sind administrative Tätigkeiten zu beschleunigen.

4.6.4 Sicherer und zuverlässiger Betrieb, Vermeidung von Netzwerkabhängigkeit

Wenn der Betrieb von Cloud-Lösungen nicht in Form einer Private Cloud durch die Organisation selbst erfolgt, besteht für die Administration eine eingeschränkte Möglichkeit die Sicherheit des Infrastrukturbetriebs zu garantieren. Prinzipiell sollten immer gesicherte Verbindungen (HTTPS, FTPS …) für den Datentransport verwendet werden. Wenn technisch möglich, sollten Daten, die bei Cloud-Dienstleistern gespeichert werden oder über entsprechende Dienstleister mit Dritten ausgetauscht werden, anhand asymmetrischer Verfahren verschlüsselt und signiert werden. So kann die Wahrscheinlichkeit erhöht werden, dass sich keine unberechtigten Dritten auf den Systemen des Cloud-Dienstleisters Zugang zu den Unternehmensdaten verschaffen.

Ein zuverlässiger Betrieb kann gewährleistet werden, sofern vom Dienstleister zur Verfügung gestellte Fehlertoleranzmechanismen von der Administration konfiguriert und im Fehlerfall bedient werden. Auch hier ist aber darauf zu achten, dass nach Möglichkeit die Notwendigkeit manueller Eingriffe im Fehlerfall vermieden wird und vielmehr automatisierte Kompensationsmechanismen ausgelöst werden, wenn dies notwendig ist.

Da unter Umständen im Falle eines Netzwerkausfalls für den Geschäftsbetrieb wesentliche Funktionalität, die über Cloud-Lösungen bereitgestellt wird, nicht mehr verfügbar ist, stellt sich die Frage, wie dieser Netzwerkabhängigkeit entgegengewirkt werden kann. Hier bestehen grundsätzlich zwei Handlungsvarianten: Zum einen die Möglichkeit, eine Notfalllösung für den Netzbetrieb vorzuhalten und Datenleitungen redundant auszulegen zum anderen Dienstleistungskomponenten in Anspruch zu nehmen, die es ermöglichen, eigentlich cloudbasierte Funktionalität in dem eigenem lokalen Netzwerk vorzuhalten, damit für den Fall eines WAN-Ausfalls (en: Wide Area Network) dennoch die Funktionalität der Cloud-Lösung über ein Notfallsystem im lokalen Netzwerk – wenngleich evtl. in eingeschränktem Umfang – verfügbar ist.

4.6.5 Elastischer Betrieb

Dem Charakteristikum der Elastizität von Cloud-Lösungen muss die Administration Rechnung tragen, indem nicht mehr benötigte Kapazitäten und Funktionalitäten von Cloud-Lösungen schnell wieder freigegeben werden können und neu benötigte oder erweitert benötigte Kapazitäten und Funktionalitäten zeitnah verwendet werden können.

Es bleibt somit festzuhalten, dass unter Betriebsgesichtspunkten die Möglichkeiten eines elastischen Betriebs mit den weiter oben erläuterten Möglichkeiten eines schnellen administrativen Betriebs einhergehen, und lediglich durch Automatisierung der administrativen Tätigkeit zu erreichen sind.

Der Grundstein für einen elastischen Betrieb muss bereits in früheren Phasen bei der Serviceauswahl gelegt werden. Bietet ein Vertrag z. B. keine Möglichkeiten, positive Elastizität zu nutzen, da Mindestkontingente verabredet worden sind, die weit über den Mindestbedarfen des Cloud-Sourcing-Gebers liegen, so kann Elastizität zwar technisch sichergestellt werden, nicht aber de-facto in Anspruch genommen werden.

4.6.6 Monitoring und Berücksichtigung der Nutzungsabhängigkeit

Im Rahmen des Monitorings wird überprüft, ob Cloud-Dienste fehlerfrei ablaufen, welche Änderungen an den Konfigurationen erfolgen und ggf. auch welche Nutzung erfolgt.

Das Monitoring eingesetzter Cloud-Lösungen sollte so detailliert erfolgen, dass eine interne Verrechnung der Cloud-Lösung-Kosten auf Kostenstellen oder zumindest Abteilungsebene möglich ist.

Es bestehen verschiedene Ansatzpunkte für ein entsprechendes Monitoring. Stellt der Cloud-Dienstleister nicht bereits Auswertungen zu diesem Zweck zu Verfügung, so sind vom Cloud-Sourcing-Geber entsprechende Programme zu entwickeln. Die Programme sollten Protokolldateien auswerten, die Zugriffe der Nutzer auf die Cloud-Lösung dokumentieren. Hierbei kann es sich um Protokolldateien von Client- oder Server-Anwendungen eines Cloud Anbieters oder um Proxy-Server-Protokolle des Cloud-Sourcing-Gebers handeln, die die Netzzugriffe der Nutzer auf einen Cloud-Dienst dokumentieren. Das Monitoring liefert Daten, die die Überprüfung der Einhaltung der zugesicherten SLAs ermöglichen. Es liefert darüber hinaus Informationen für eine Lokalisierung von Fehlerursachen. Insbesondere in Bezug auf die Fähigkeit eines Monitorings zur Identifikation von Fehlerquellen ist eine notwendige Voraussetzung, dass das Monitoring alle Komponenten des Anwendungssystems einzeln überwacht. So entsteht die Möglichkeit einer Ende-zu-Ende Betrachtung, die für eine problemlösende Ursachenanalyse notwendig ist.

Die im Rahmen entsprechender Protokollierung anfallenden Datenmengen und notwendige flankierende administrative Tätigkeiten können erheblich sein. Daten sollten daher immer so früh wie möglich auf ein benötigtes Aggregationslevel konsolidiert werden. Bei dieser Konsolidierung ist auch darauf zu achten, dass Daten nicht auf einzelne Personen zurückzuführen sind, da ansonsten mitbestimmungspflichtige Bereiche entstehen.

Vor Inbetriebnahme entsprechender Protokolllösungen sollten dennoch auf jeden Fall Gespräche mit den Institutionen der Arbeitnehmervertretung erfolgen, damit nicht der falsche Eindruck einer Leistungskontrolle entsteht. Die Arbeitgebervertretung muss gegenüber der Arbeitnehmervertretung klarstellen, dass es sich lediglich um eine Datenerhebung zum Zweck der internen Verrechnung der Cloud-Lösung-Kosten handelt.

Die hier skizzierte Monitoring-Problematik ist bereits in früheren Phasen bei Aufbau des Kriterienkatalogs und der Produktauswahl zu berücksichtigen. Insbesondere sollte darauf geachtet werden, dass das Monitoring detailliert genug erfolgt, um eine Ursachenanalyse im Fehlerfall zu gewährleisten, aber gleichzeitig aggregiert genug, um mitbestimmungspflichtige Bereiche zu vermeiden.

4.6.7 Qualitätsmanagement

Wie auch bei allen anderen IT-Systemen, sollte bei Cloud-Lösungen die Endanwenderzufriedenheit in regelmäßigen Abständen ermittelt werden. Neben der Anwenderzufriedenheit sind auch die Kosten der Systeme in Bezug auf Alternativen zu überprüfen (Benchmarking) und das Problemaufkommen im Zeitverlauf („Incidents“ im Sinne von Störungen) zu beobachten.

Bei sich verschlechternden Trends sind Maßnahmen zu ermitteln, abzustimmen und durchzuführen.

Da insbesondere die Endanwender-Zufriedenheit stark von der Endanwender-Befähigung abhängig ist, sollten Schulungen und Endanwender-Beobachtungen mit dem Ziel der Verhaltensoptimierung durchgeführt werden.

Eine enorme Qualitätsverbesserung können Key-User-Konzepte, in denen Support durch besonders befähigte User geleistet wird, oder auch der Rückgriff auf externe Helpdesks bewirken.

4.6.8 Change Management

Im Rahmen des Change Managements sind alle Veränderungen an vorhandenen, sowie das Hinzufügen oder Außerbetriebnehmen von Cloud-Lösungen zu kontrollieren und begleiten. Das Ziel des Change Managements ist eine effiziente Veränderung und die Minimierung mit der Veränderung ggf. einhergehender Risiken und Störungen.

Das Change Management sollte sich mit außerordentlichen Changes befassen. Die Anlage oder Änderung eines Nutzers gehört nicht zu den relevanten Änderungen, wohl aber die Anbindung einer Cloud-Lösung an ein innerhalb der Organisation betriebenes Buchhaltungssystem.

Änderungsanträge sollten – wie in gängigen IT-Rahmenwerken beschrieben – zumindest den Grund für eine Änderung, eine Beschreibung der Änderung, einen Ziel-Änderungstermin, eine Priorisierung und eine mit der Änderung einhergehende Risikoklassifizierung enthalten.

Stellt die Menge der Änderungen die Administration vor Ressourcenprobleme, so ist in Anbetracht der Änderungspriorisierung eine Planung unter Berücksichtigung der Engpässe durchzuführen, die hilft, die durch die zeitliche Verzögerung resultierenden Probleme zu minimieren.

Im Sinne des oben kurz beschriebenen Qualitätsmanagements sind abgeschlossene Änderungsvorgänge hinsichtlich ihrer Durchführung und Ergebnisse zu bewerten und ggf. verbessernde Maßnahmen in Bezug auf den Änderungsprozess zu planen und zu realisieren.

Das Change Management begleiten häufig hohe Anforderungen der Berichterstattung. So sind Änderungen qualitativ und quantitativ für die Unternehmensführung zu dokumentieren und in Präsentationen aufzubereiten. Um unnötige manuelle Übertragung von Daten im Rahmen dieser Berichtserstattung zu vermeiden, sollte das Change Management durch eine Datenbank unterstützt werden, die in der Lage ist, Reports voll- oder zumindest teilautomatisiert zu erzeugen.

Insbesondere wenn hohe Risiken mit einer Änderung einhergehen, sollte darauf geachtet werden, dass zumindest ein Vier-Augen-Prinzip implementiert wird, das vermeidet, dass zu riskante Änderungen ohne Autorisierung in Angriff genommen werden. Entsprechende Freigaben sind schriftlich oder IT-basiert durch digitale oder echte Signaturen zu dokumentieren.

Literaturhinweise

[1] *Henneberger, M., Strebel, J., Garzotto, F.: Ein Entscheidungsmodell für den Einsatz von Cloud Computing in Unternehmen. HMD Praxis der Wirtschaftsinformatik. 275, 76–84 (2010).*

[2] *BITKOM Leitfaden „Cloud Computing – Evolution in der Technik, Revolution im Business“, Oktober 2009.*

[3] *BITKOM Leitfaden „Cloud Computing – Was Entscheider wissen müssen“, 20.12.2010.*

[4] *EuroCloud Leitfaden „Recht, Datenschutz & Compliance“, 02.12.2011.*

[5] *Catteddu, D. and Hogben, G., editors. „Cloud Computing Benefits, Risks and Recommendations for Information Security“, The European Network and Information Security Agency (ENISA), 2009.*

[6] *Brunette, G. and Mogull, R., editors. „Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.“, Cloud Security Alliance, 2009.*

[7] *Cloud Security Alliance (2010): „Cloud Controls Matrix V1.1“*

[8] *BSI Eckpunktepapier Sicherheitsempfehlungen für Cloud-Computing-Anbieter – Mindestanforderungen in der Informationssicherheit; Stand Februar 2012*

[9] *Jonas Repschläger: Cloud Computing Framework zur Anbieterauswahl der TU Berlin – Lehrstuhl für Informations- und Kommunikationsmanagement. (http://www.ikm.tu-berlin.de/fileadmin/fg16/Forschungsprojekte/Cloud_Computing_Anbieterauswahl_Framework_v1-1.pdf)*

[10] http://www.eurocloud.de/2012/11/23/leitfaden-cloud-vertrage-effizient-gestalten