Ausgabe 02.15

amendos Newsletter

Internationales Projektmanagement: Die Suche nach einer gemeinsamen Sprache >> Seite 1

Integration von Cloud Services in die IT-Infrastruktur - Teil 2: Risiken >> Seite 3

Aufgaben des IT-Providermanagements >> Seite 6

amendos Seminare 2015 >> Seite 8

Liebe Leserinnen und Leser,

erfolgreiche Kommunikation ist in jedem Projekt eine Herausforderung. Dies gilt umso mehr, wenn es sich um ein multinationales Projektteam handelt, da hier zunächst eine gemeinsame „Projektsprache“ gefunden werden muss. Was dabei zu beachten ist, beleuchten wir in unserem ersten Beitrag.

In unserem letzten Newsletter haben wir mit einer Artikelserie rund um das Thema Cloud begonnen. Im zweiten Teil dieser Serie beschäftigen wir uns mit den Risiken, die Cloud-Computing birgt. Anhand einer beispielhaften Risikoanalyse möchten wir Ihnen zeigen, wie diese Risiken identifiziert und entsprechende Maßnahmen abgeleitet werden können.

Ein gut abgestimmtes Providermanagement ist einer der Grundpfeiler für das erfolgreiche Outsourcing von IT-Services. In unserem letzten Beitrag stellen wir Ihnen daher die entsprechenden dazugehörigen Aufgaben vor.

Wir wünschen viel Spaß beim Lesen!

Jörg Bujotzek
Geschäftsführer
amendos gmbh

amendos gmbh
Frankenstraße 3, 20097 Hamburg
www.amendos.de
Tel. +49 (0) 40 / 248 276 00

Internationales Projektmanagement: Die Suche nach einer gemeinsamen Sprache

Im Zuge der Globalisierung gewinnen internationale Projekte in Unternehmen immer mehr an Bedeutung. Projektteams setzen sich zunehmend aus Mitgliedern verschiedener Kulturkreise zusammen, die über mehrere Zeitzonen und Kontinente verteilt sein können. Dieser Umstand stellt einen Projektleiter und sein Team vor völlig neue Herausforderungen, da für die Projektdurchführung neben Soft Skills und Fach- und Methodenkompetenzen zusätzlich auch interkulturelle Kompetenzen unerlässlich sind. In dem vorliegenden Beitrag soll es um die Findung einer gemeinsamen „Projektsprache“ gehen, die es allen Teammitgliedern ermöglicht, gleichberechtigt an der Kommunikation zu partizipieren.

Eine der ersten Schwierigkeiten, die es zu Beginn eines internationalen Projektes zu bewältigen gilt, ist die Etablierung einer gemeinsamen Kommunikationsgrundlage. Zunächst einmal muss eine gemeinsame Arbeitssprache festgelegt werden. In den meisten internationalen Projekten ist die bevorzugte „Lingua franca“ nach wie vor Englisch. Es kann jedoch nicht selbstverständlich davon ausgegangen werden, dass alle Teammitglieder die Sprache gleichermaßen gut beherrschen, im Gegenteil ist oftmals ein deutliches Sprachgefälle zu beobachten. Eine zu große Sprachdisparität innerhalb eines Teams kann jedoch hinsichtlich des gesamten Projektes gravierende Folgen nach sich ziehen:

- Mangelnde Sprachkenntnisse von einigen Mitgliedern werden verschwiegen oder vertuscht, um sich keine Blöße zu geben und führen zu Verzögerungen oder unzureichenden Ergebnissen, weil Anweisungen / Arbeitspakete nicht verstanden wurden.
- Muttersprachler werden aufgrund ihrer Sprachvorteile teilweise als zu dominant wahrgenommen. Bei Nichtmuttersprachlern mit begrenzten Sprachkenntnissen hingegen besteht die Gefahr, dass falsche Rückschlüsse auf ihre Person gezogen und sie z.B. als fachlich inkompetent eingeschätzt werden. Innerhalb des Teams kann so schnell ein durch Sprache verursachtes Machtgefälle entstehen.
- Dies wiederum zieht häufig nach sich, dass sich bei Nichtmuttersprachlern Unbehagen und Unsicherheit einstellen. Die betroffenen Teammitglieder ziehen sich zurück, das Team verliert seinen Zusammenhalt und ist nur noch eingeschränkt arbeitsfähig.

Genauso wie weniger umfangreiche Sprachkenntnisse zu Schwierigkeiten im Verlauf des Projektes führen können, können überdurchschnittlich gute Sprachkennt-

nisse von Nichtmuttersprachlern ebenfalls Probleme aufwerfen. Hier verhält es sich oftmals so, dass Muttersprachler aufgrund der Sprachkompetenz ihres Gegenübers ein implizites Verständnis der zugrundeliegenden kulturellen Annahmen erwarten, denn jede sprachliche Äußerung fußt immer auf einem bestimmten Kulturverständnis, welches innerhalb eines multinationalen Teams große Interpretationsspielräume eröffnet. Dies kann zu Problemen führen, da Sprecher aus verschiedenen Kulturkreisen oftmals ein und demselben englischen Begriff (z.B. Qualität, Pünktlichkeit, Probleme) eine unterschiedliche Bedeutung und Wertigkeit zuschreiben; Missverständnisse, die sich negativ auf die Zusammenarbeit auswirken, sind häufig die Folge.

Was also können der Projektleiter und das Projektteam tun, um Englisch als gemeinsame Projektsprache zu etablieren, die allen die gleiche Partizipation erlaubt?

Eine der wichtigsten Voraussetzungen für eine gleichberechtigte Kommunikation im Projektverlauf ist, die einzelnen Teammitglieder schon vor Beginn des Projektes sprachlich in der „Lingua franca“ so vorzubereiten, dass zu Projektbeginn ein allzu großes Sprachgefälle ausgeschlossen wird – ganz wird es sich in der Praxis sicherlich nie vermeiden lassen.

Zu Beginn des Projektes sollte der Projektleiter auf jeden Fall eine Diskussion zur Klärung von zentralen Begriffen initiieren, damit alle Teammitglieder ein einheitliches Verständnis entwickeln. So lässt sich der oben angesprochene Interpretationsspielraum weitestgehend minimieren. Weiterhin ist es Aufgabe des Projektleiters, dafür Sorge zu tragen, dass bestimmte Kommunikationsregeln aufgestellt und im Projektverlauf auch eingehalten werden. Diese könnten z.B. folgendermaßen lauten:

Sprecher sollten in ihren Beiträgen...

- ausreichend Pausen machen,
- kurze Sätze, denen man gut folgen kann, bilden,
- eine einfache Sprache verwenden und schwierige Ausdrücke ggf. umschreiben,
- keinen Slang benutzen und
- auf idiomatische Ausdrücke verzichten.

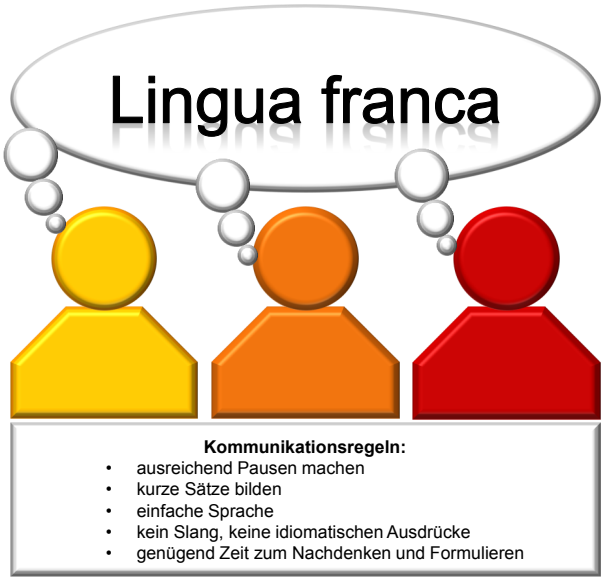


Abbildung 1: Kommunikationsregeln

- Außerdem muss Nichtmuttersprachlern ausreichend Zeit gewährt werden, um in Ruhe nachdenken und ihre Beiträge formulieren zu können.

Der Projektleiter sollte darauf achten, dass Teammitglieder mit sehr guten Sprachkenntnissen die Kommunikation nicht dominieren, sondern allen Teilnehmern die gleiche Redezeit zur Verfügung steht. Weiterhin wäre es wünschenswert, wenn er schwächere Sprecher ermutigt und unterstützt, sich an den Diskussionen zu beteiligen, denn so wird ein Austausch unter allen Teammitgliedern sichergestellt.

Neben dem Projektleiter kommt Muttersprachlern in einem multinationalen Projektteam hinsichtlich der Kommunikation eine besondere Rolle zu. Zum einen kann es hin und wieder notwendig werden, sie in ihrer Sprachdominanz etwas zu bremsen und an die Einhaltung der verabredeten Kommunikationsregeln zu erinnern. Zum anderen können Muttersprachler die Rolle eines „Verständnisvermittlers“ einnehmen: indem sie Äußerungen von Nichtmuttersprachlern aufnehmen und nochmals paraphrasieren, helfen sie, sicherzustellen, dass das gesamte Team alles korrekt verstanden hat. Dieses Vorgehen hilft, Nichtmuttersprachler zu unterstützen und verhindert, dass sich einige Sprecher aus Unsicherheit oder Scham aus der Kommunikation zurückziehen.

Fazit

Eine der grundlegenden Voraussetzungen für den Erfolg eines Projektes mit einem multinationalen Team ist neben der Festlegung einer gemeinsamen Projektsprache die Ausgestaltung der gemeinsamen Kommunikation im Team. Hierzu sollte einerseits das Verständnis zentraler Begriffe diskutiert und in Übereinstimmung gebracht werden. Andererseits ist es unerlässlich, verbindliche Kommunikationsregeln aufzustellen, und deren Einhaltung durchzusetzen. Sowohl dem Projektleiter als auch Muttersprachlern kommen in multinationalen Teams hinsichtlich der Kommunikation Schlüsselrollen zu. Während ersterer vornehmlich eine gleichberechtigte Kommunikation zwischen allen Teammitgliedern sicherstellen muss, fungieren letztere gleichsam als „Verständnisvermittler“.

Petra Bleshoy

Integration von Cloud Services in die IT-Infrastruktur - Teil 2: Risiken

Laut Cloud-Monitor 2014, einer von KPMG in Auftrag gegebenen repräsentativen Studie zum Thema Cloud Computing, zieht jedes zweite Unternehmen Konsequenzen aus der NSA-Affäre. Im Vordergrund stehen dabei vor allem erhöhte Sicherheitsanforderungen an den jeweiligen ITK-Dienstleister um sich vor Spionageversuchen und Hackerangriffen zu schützen. Doch welche Risiken gibt es im Bereich der Public Cloud überhaupt? Wie bewertet man sie und welche Maßnahmen können ergriffen werden, um diese zu minimieren. Diese Fragen werden im folgenden zweiten Teil unser Cloud-Computing Serie beleuchtet.

Die Risiken hinsichtlich einer Public Cloud kann man in drei große Bereiche einteilen: **rechtliche, organisatorische** und **technische Risiken**. Weiterhin ergeben sich durch die rasante Entwicklung des Cloud-Marktes immer wieder **unvorhergesehene Risiken** und Probleme. Im Rahmen von Cloud-Projekten ist es daher unbedingt notwendig, eine Risikoanalyse vorzunehmen. Diese erfolgt üblicherweise in den drei Phasen Risikoidentifizierung, Risikobewertung und Risikomanagement. Wie eine solche Risikoanalyse aussehen kann, zeigt die Tabelle auf der nächsten Seite.

Risikoidentifizierung (siehe Spalte 1, 2 und 3)
Zunächst identifiziert man, soweit möglich, alle Risiken die im Zusammenhang mit der Cloud auftreten können. Zur besseren Übersicht sollten diese dann im Folgenden den einzelnen, oben genannten Kategorien zugeordnet werden. Hierbei kann es durchaus vorkommen, dass bestimmte Risiken in mehrere Kategorien fallen. Anschließend sind die Risiken und ihre Konsequenzen für das Unternehmen genauer zu beschreiben. Dieser Schritt ist unbedingt notwendig, um später unter anderem das Schadenspotential zu bewerten (vgl. Spalte 4, 5 und 6).

Risikobewertung (siehe Spalte 4, 5 und 6)
Sind alle Risiken erfasst und beschrieben, wird die Risikobewertung durchgeführt. Hierbei können verschiedene Kriterien in die Bewertung einfließen. Am häufigsten werden jedoch die Folgenden verwendet: Wahrscheinlichkeit des Eintreffens sowie das Schadenspotential. Die Bewertung an sich ist dann je nach Unternehmen und Art der Daten, welche in der Cloud gespeichert werden, höchst unterschiedlich. Befinden sich in der Cloud zum Beispiel Daten, die Produktionsdetails enthalten, ist das Schadenspotential erheblich höher als bei nicht-sensitiven Daten, etwa die Fuhrparkverwaltung eines Unternehmens, welches Logistik nicht als Teil des Kerngeschäfts betreibt, zum Beispiel eine Steuerberatungsgesellschaft.

Risikomanagement (siehe Spalte 7)
Basierend auf dieser Bewertung muss dann erfasst werden, welche korrektiven und Präventionsmaßnahmen erforderlich sind und mit welcher Dringlichkeit diese umgesetzt werden müssen. Auch diese Maßnahmen können je nach Art der Daten bzw. des Unternehmens höchst unterschiedlich ausfallen. Soll etwa eine gesamte Anwendungssuite, wie zum Beispiel Office, in die Cloud verlagert werden, muss größter Wert auf eine sichere Verschlüsselung gelegt werden, da unternehmenskritische Daten sonst in falsche Hände geraten könnten. Anders sieht es bei Anwendungen aus, die nicht zum Kerngeschäft eines Unternehmens gehören, wie z.B. das o. g. Tool für die Fuhrparkverwaltung einer Steuerberatungsgesellschaft. Auch hier sollten die Daten selbstverständlich verschlüsselt werden, ihr Bekanntwerden hätte jedoch keine unternehmenskritischen Auswirkungen, da es sich nicht um sensitive Daten handelt.

Eine erste Risikoanalyse sollte man schon in der initialen Projektphase, also während der Spezifikation der Cloud-Serviceanforderungen und vor der Auswahl eines Providers, erstellen. So können eventuelle Maßnahmen bei der Auswahl und der Vertragsgestaltung gleich berücksichtigt werden. Regelmäßige Updates der Risikobewertung sowie Aktualisierungen der Maßnahmen sollten dann bei sich verändernden Rahmenbedingungen – im Unternehmen, im Unternehmensumfeld und hinsichtlich der genutzten Services – sowie bei etwaigen neuen Anforderungen des eigenen Unternehmens erfolgen.

Fazit
Generell gilt: Da sich der Cloud-Markt ständig weiterentwickelt, ist es wichtig, eine einmal durchgeführte Risikoanalyse kontinuierlich zu aktualisieren und die identifizierten Risiken regelmäßig neu zu bewerten. Nur so kann man bisher nicht antizipierten Problemen rechtzeitig begegnen. In dem darauffolgenden Schritt – dem Risikomanagement – werden entsprechende Maßnahmen, die es ermöglichen, die festgestellten Risiken auszuschließen oder zu minimieren, festgelegt. Bei den Maßnahmen ist zu beachten, dass diese auch bei vollumfänglicher Umsetzung keinen 100-prozentigen Schutz bieten können. Es werden immer Risiken vorhanden sein, deren Eintritt man nicht ausschließen kann, deren Wahrscheinlichkeit und Ausmaß aber durch das Festlegen von Prozessabläufen und anderen Vorkehrungsmaßnahmen reduziert werden können.

Michael Pfitzmann

Risiko-Identifizierung			Risikobewertung			Risikomanagement
Kategorie	Risiko	Beschreibung	Wahrschein-lichkeit (W)	Schadens-potential (SP)	Risikowert (W*SP)	Maßnahmen
Rechtlich	Datenschutz und rechtliche Vorgaben sowie Compliance	Nichteinhaltung von Datenschutzgesetzen, wodurch Daten möglicherweise Wirtschaftsspionage ausgesetzt sind (Speicherung in Ländern mit weniger strengen Zugriffsregeln aufgrund fehlender Regelungen im Cloudvertrag).				Abklärung der rechtlichen Rahmenbedinungen und deren Einbeziehung in die Verhandlungen mit dem Cloud-Provider. Zwingende SLAs mit dem Cloud-Provider vereinbaren, die eine Datenhaltung und -verarbeitung in anderen Ländern (mit denen es keine entsprechenden Abkommen wie Safe Harbour gibt) ausschließen.
	Beschlagnahmung von Hardware im Fall von Ermittlungen gegen den Cloud-Provider oder andere gehostete Unternehmen	Mögliche Beschlagnahmung von Hardware des Public Cloud-Providers, auf welcher sich Daten vom Unternehmen befinden können, über die man dann keine Kontrolle mehr hat.				Verschlüsselung der beim Cloud-Provider abgelegten Daten, um unkontrollierten Zugriff durch Behörden zu verhindern. Backups der Daten auch außerhalb der Cloud-Infrastruktur aufbewahren.
Organisatorisch	Verlust an Transparenz sowie Steuerungs- und Kontrollmöglichkeit	Übertragung einer Vielzahl von Aufgaben mit Relevanz für IT-Sicherheit und Datenschutz an den Public Cloud-Provider. Die Verantwortung dafür verbleibt jedoch im Unternehmen.				Prüfen, inwieweit der Cloud Anbieter so etwas in seinen Vereinbarungen schon anforderungsgerecht enthalten bzw. betrachtet hat. Klar definierte SLAs.
	Abhängigkeit vom Provider (Lock-in)	Providerspezifische, proprietäre Applikationen macht den Cloud-Vorteil der Flexibilität teilweise wieder zunichte, da ein Providerwechsel sehr aufwendig wäre.				Ausgewählter Provider sollte möglichst viele providerübergreifende Standards anbieten.
	Insolvenz des Providers	Unklarheit was mit den Rechenzentren bzw. den Daten passiert, sollte ein Public Cloud-Provider insolvent werden -> Verlust der Kontrolle über die Daten.				Festlegung von entsprechend eintretenden, auszuführenden Prozessen in den Verträgen mit dem Cloud-Provider.
	Vom Provider beauftragte Subunternehmer	Der Provider kann verschiedene Subunternehmer mit bestimmten Leistungen beauftragen. In einer Public Cloud bleibt diese zusätzliche Komplexität dem Nutzer unter Umständen verborgen. Daten können sich dann auf Computing-Ressourcen eines unbekannten Subunternehmers irgendwo in der Welt befinden.				Vertragliche Regelungen, die solche Situationen ausschließen, inklusive Vertragsstrafen bei Erkennung von Misachtung dieser Richtlinien.
Technisch / Organisatorisch	Mandantenfähigkeit in virtualisierten Umgebungen	Durch ungenaue Trennung der einzelnen Mandanten auf Seiten des Public Cloud-Providers können unter Umständen Unbefugte auf die jeweiligen unternehmensinternen Daten zugreifen.				Zertifkate oder Vergleichbares, mit denen der Cloud Provider die sichere Mandantenfähigkeit nachweisen kann. Festlegung von Vetragsstrafen, sollte dieser Fall trotzdem eintreten (SLAs). Sichere Authentisierungsstrategie.
	Mangelnde Rollentrennung von Administrationsbereichen, Gefahr durch Innentäter/Insider sowie mögliche Erpressungen	Ungenügende Rollentrennung von Administrationsbereichen auf Seiten des Public Cloud-Providers, insbesondere bei SaaS Anbietern (z.B.: Datenbank Administrator ist gleichzeitig Administrator der Anwendung). Dadurch entsteht zum Beispiel die Gefahr von Erpressungen mit Firmendaten.				Festlegung von Vertragsstrafen, sollte dieser Fall eintreten, sowie Sicherstellung von Tracking Maßnahmen seitens des Cloud-Providers um diese Fälle schnellstmöglich aufzuklären.
Technisch	Unsichere Schnittstellen bei Datenübertragungen	Unverschlüsselte Schnittstellen auf Seiten des Public Cloud-Providers, dadurch Gefahr durch Industriespionage etc.				Verschlüsselung als notwendige Voraussetzung vertraglich festlegen
	Identitätsdiebstahl	Angriffe von Kriminellen die sich gegenüber dem Cloud-Provider als Mitarbeiter des Kunden ausgeben -> Gefahr durch Industriespionage.				Mehrfache Authentifizierungsmechanismen festlegen und nutzen.
	Backup	Komplexität von Backups in der Cloud sowie die allgemeine Gefahr eines Angriffs auf die Backup Daten -> Gefahr von Datenverlust.				Erstellung und regelmäßige Überprüfung eines Backup-Szenarios. Sichere Zugangsrichtlinien und Benutzerauthentisierung sowie Key Management (bei verschlüsselten Backups).
	Internetverbindung	Schlechte Verfügbarkeit von Cloud-Diensten durch mangelnde, oder fehlende Internetverbindung, wodurch Einschränkungen für die Mitarbeiter entstehen.				Prüfen ob sich LTE oder ähnliches nutzen lässt, sollte zum Beispiel schnelles DSL nicht vorhanden sein.
	Man in the Middle Attacken	Hacker-Angriffe um die Daten während Datentransfers vom Kunden zum Public Cloud-Provider zu stehlen.				Verschlüsselung als notwendige Voraussetzung vertraglich festlegen.
	DDoS Attacken	Gezieltes Blockieren von Public Cloud-Providern um den gehosteten Unternehmen zu schaden.				Cloud Provider muss entsprechend starke Abwehrmaßnahmen bereitstellen (allerdings kann ab einer gewissen Größe des Angriffs auch der beste Schutz nichts mehr ausrichten).
	Verlust von Identitäten, Passwörtern und PIN-Codes	Gefahr von Datenlecks auf Seiten des Public Cloud-Providers mit gravierenden Konsequenzen für das nutzende Unternehmen.				Festlegung von Vertragsstrafen, sollte dieser Fall eintreten. Ansonsten kann ein Unternehmen bei einem solchen Ereignis nichts anderes ausrichten.
	Unzureichende Löschung von Daten	Mangelnde Sicherstellung der Löschung von Daten, entweder festgelegt durch die Datenart an sich oder nach Beendigung eines Vertragsverhältnisses -> Gefahr durch Industriespionage.				Festlegung von Prozessen und Abläufen bei Ende des Vertragsveräl tnisses. Testen einer Löschung.
Technisch / Organisatorisch / Rechtlich	Künftige bzw. unvorhergesehene Bedrohungen	Bedingt durch die technische Entwicklung sind in Zukunft Bedrohungen möglich, die heutzutage noch nicht zu antizipieren sind (neue Trojaner, neue Möglichkeiten zur Entschlüsselung bzw. zum Abhören oder Abfangen von Datenübertragungen). Ebenfalls möglich sind sich ändernde rechtliche Rahmenbedingungen durch neue Gesetze etwa in Deutschland, der EU, den USA oder China etc.				Kontinuierliche Risikoanalyse und ggf. Anpassung bzw. Festlegung von entsprechenden Maßnahmen.

Tabelle 1: Beispiel einer Risikoanalyse

amendos Spezial PM – Soft Skills

Im Sinne eines ganzheitlichen Projektmanagement-Ansatzes spielt nicht nur die fachliche Kompetenz bei der Erfüllung eines Projektauftrages eine wichtige Rolle, sondern dem Bereich der Soft Skills ist ebenfalls ausreichend Raum zu gewähren.

In dieser Ausgabe von **amendos Spezial** dreht sich daher alles um

„Projektmanagement – Soft Skills“:

- Soft Skills im IT-Projektmanagement
- Teambildung und Überwindung von Widerständen
- Ressourcenkonflikte
- Turnaround Management

amendos Spezial IT Service Management

Ein zielgerichtetes, effizientes IT Service Management ist heutzutage unerlässlich da IT Service Provider – sowohl interne als auch externe – ihre IT-Dienstleistungen nicht mehr nur an der IT-Sicht, sondern auch an der Business-Sicht ausrichten müssen.

In dieser Ausgabe von **amendos Spezial** dreht sich daher alles um

„IT Service Management“:

- Erstellung von kundenorientierten IT-Services
- servicefokussiertes IT-Controlling und Wirtschaftlichkeitsprüfung
- Service Portfolio Management

Aufgaben des IT-Providermanagements

Zunehmend wird in Unternehmen erkannt, dass das Outsourcing von IT-Services ohne Etablierung eines angemessenen Providermanagements nicht erfolgreich sein kann. Diese Tatsache ist unabhängig davon, wie gut der Vertrag mit dem Provider ausgearbeitet wurde. Das Providermanagement des Auftraggebers stellt sicher, dass der Provider die mit ihm vereinbarte Leistung auch in angemessener Qualität erbringt. Im Folgenden soll aufgezeigt werden, welche Aufgaben im Rahmen des Providermanagements wahrzunehmen sind, um die Beziehung mit dem Provider langfristig erfolgreich zu gestalten.

Die Aufgaben des Providermanagements sind vielfältig: Neben der Notwendigkeit der Überwachung der Providerleistungen sind auch übergreifende Prozesse zwischen Provider und Abnehmer zu koordinieren und bei Bedarf Abstimmungen der Zusammenarbeit sicherzustellen. Änderungen der Rahmenbedingungen und Anforderungen im beauftragenden Unternehmen machen zudem eine regelmäßige Justierung der Zusammenarbeit mit dem Provider unabdingbar. Des Weiteren kann ein Prozess zur kontinuierlichen Verbesserung der Zusammenarbeit sicherstellen, dass die Erreichung der Outsourcing-Ziele stetig zunimmt.

Im Einzelnen lassen sich die Aufgaben des Providermanagements den vier Aufgabenbereichen „Governance“, „Betrieb“, „Änderungen“ und „stete Verbesserung“ zuordnen. Die Kernprozesse dieser Aufgabenbereiche sind in Tabelle 1 dargestellt.

Aufgabenbereich	Kernprozesse
Governance	Outsourcing Business Planning
	Relationship Management
	Risikomanagement
Betrieb	Performance Management
	Operations Management
	Knowledge Management
	Eskalation
	Finance Management
	Compliance Management
Änderungen	Projekt Portfolio Management
	Claim Management
	Change Management
	Projekt Management
	Transition Support in der Vertrags-Endphase
Stete Verbesserung	Reifegradprüfung
	Kontinuierlicher Verbesserungsprozess
	Weiterbildung
	Marktbeobachtung

Tabelle 1: Aufgabenbereiche und Kernprozesse des Providermanagements

Im Folgenden werden die im Rahmen der Kernprozesse entstehenden Aufgaben näher erläutert.

1. Governance

Outsourcing Business Planning

Im Rahmen des Outsourcing Business Planning wird periodisch (üblicherweise einmal pro Jahr) ein Update des Outsourcing Business Plans mit den vier Sektoren Strategie, Operations, Finanzen und Management vorgenommen. Im Sektor Strategie werden folgende Aspekte für die Neuausrichtung der Providerbeziehung berücksichtigt:

- Änderungen in der eigenen Unternehmensausrichtung sowie bei den Unternehmenszielen,
- Ergebnisse des Reviews der Gesamtperformance-Entwicklung der Providerleistung,
- neue Services des Providers die einen identifizierten Zusatznutzen für die eigene Organisation darstellen.

Im Sektor Operations werden die Initiativen aus der Strategie operationalisiert.

Im Sektor Finanzen erfolgt das Update des Outsourcing Business Case aufgrund der in Oprations geplanten Veränderungen.

Im Sektor Management erfolgt ein Review von Stärken und Schwächen des laufenden Management Prozesses unter Einbeziehung der geplanten Neuerungen.

Relationship Management

Im Relationship Management erfolgt periodisch eine Bewertung des Providers mit dem Ziel, den Zustand der Providerbeziehung zu überwachen. Grundlage hierfür ist üblicherweise ein periodischer Health Check letzterer, der unter anderem die Faktoren finanzielle Performance, Fachexpertise, Agilität, Flexibilität, Qualität und Compliance einbezieht. Diese Providerbewertung bildet dann wiederum die Basis für den Sektor Strategie im Outsourcing Business Planning (siehe oben).

Zudem finden in regelmäßigen Intervallen Vertragsreviews statt, in denen unter anderem die Bedeutung des Vertrags für die Zukunft bewertet wird und erforderliche Vertragsänderungen identifiziert werden. Bei Bedarf werden auch die Kündigungs- und Verlängerungsoption geprüft und bewertet.

Weitere Aktivitätsbereiche dieses Kernprozesses sind die Ableitung von Maßnahmen zur Verbesserung der Zusammenarbeit sowie die Pflege der Beziehung zum Provider.

2. Betrieb

Performance Management

Die periodische (i.d.R. monatliche) Messung der Performance des Providers erfolgt auf Basis des im Vertrag vereinbarten, KPI-

basierten Reportings des Providers. Zu prüfen ist hierbei, ob die Serviceerbringung vertragskonform erfolgt.

Die gemessene Providerleistung kann zudem mit der separat zu ermittelnden Zufriedenheit und Erwartungshaltung interner Stakeholder (insbesondere der internen IT-Kunden) verglichen werden. Hierauf aufsetzend ist ein Management der Erwartungen interner Stakeholder empfehlenswert.

Operations Management
Hierunter fallen vor allem folgende Aufgaben:

- Durchführung regelmäßiger operativer Meetings zur Steuerung des Tagesgeschäfts (Basis hierfür sind üblicherweise die Providerreports aus dem Performance Management),
- Durchführung von Audits (regelmäßig bzw. ad hoc) zur Identifikation von Schwachstellen (u.a. hinsichtlich der Einhaltung von Vorgaben bezüglich Sicherheit, Compliance etc.),
- regelmäßige Überwachung des im Vertrag vereinbarten Configuration Managements, d.h. Sicherstellung, dass der IT-Bestand gemäß den vereinbarten Konventionen und Prozeduren gepflegt wird,
- periodische Überprüfung von Umfang und Aktualität der vereinbarten Dokumentation.

Knowledge Management
In diesem Kernprozess wird sichergestellt, dass das Wissensmanagement im vertraglich vereinbarten Rahmen, mit vereinbarten Tools und nach vereinbarten Regeln erfolgt.

Eskalation
Im Rahmen dieses Prozesses ist sicherzustellen, dass eine konsequente Eskalation gemäß vereinbarter Regeln und Prozeduren erfolgt. Aufgrund der gesammelten Erfahrungen ist das Eskalationsverfahren bei Bedarf zudem weiterzuentwickeln.

Finance Management
Hierunter fallen insbesondere folgende Aufgaben:

- Rechnungsprüfung und -begleichung,
- interne Leistungsverrechnung,
- periodische Budgetüberwachung / Forecasting,
- Provider-bezogenes Finanzreporting (Kennzahlen, Trends etc.),
- ggf. Asset Management (IT-Hardware, Softwarelizenzen).

Compliance Management
Das Compliance Management umfasst die Prüfung von Änderungen bestehender Compliance Regeln und deren Auswirkungen auf die Providerleistung sowie die Auslösung ggf. durchzuführender Changes.

3. Änderungen

Projekt Portfolio Management
Im Rahmen des Projekt Portfolio Managements erfolgt die Annahme, Bewertung und Freigabe von Projektanfragen, die Providerleistungen betreffen bzw. erweitern sowie das grobe Tracking des Fortschritts aller freigegebenen Projekte.

Claim Management
Das Claim Management umfasst Prüfung von (Nach-) Forderungen des Providers bzw. des Auftraggebers hinsichtlich der Deckung durch einen bestehenden Vertrag (in scope oder out-of-scope) und Klärung des Umgangs mit der Gegenseite.

Change Management
Das Change Management umfasst die Prüfung von Change Requests, Freigabe sowie Steuerung der Planung und Umsetzung von Changes. Hierbei sind Changes mit und ohne Vertragsänderungsbedarf zu unterscheiden (Identifikation: siehe Claim Management).

Projekt Management
Im Kontext von Providermanagement liegt hier der Fokus insbesondere auf der kundenseitigen Projektleitung und Teammitgliedsstellung für Projekte mit Providerbeteiligung.

Transition-Support in der Vertrags-Endphase
In diesem Kernprozess ist sicherzustellen, dass der Provider vertragsgemäß die Transition zu einem neuen Provider unterstützt und seine Aufgaben im Rahmen der Transition übernimmt. Zudem ist ein kontinuierlicher Betrieb bis zur Übergabe an den neuen Provider sicherzustellen.

4. Stete Verbesserung

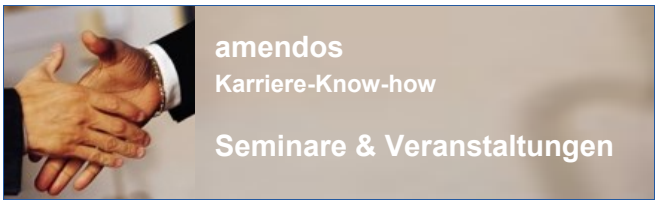
Reifegradprüfung
Die Reifegradprüfung umfasst die periodische Überprüfung des aktuellen Reifegrads der Outsourcing Prozesse (z.B. CMMI basierend). Im Anschluss sind jeweils Entwicklungsziele bezüglich des Reifegrads festzulegen und Maßnahmen zur Erhöhung des Reifegrads gemäß Zielvorgabe abzuleiten.

Kontinuierlicher Verbesserungsprozess
Im Rahmen des kontinuierlichen Verbesserungsprozesses fallen insbesondere folgende Aufgaben an:

- strukturierte Identifikation von Verbesserungsmaßnahmen,
- Festlegung von Verbesserungszielen,
- Planung und Umsetzung der Verbesserungsmaßnahmen,
- Messung der Zielerreichung und Behebung von Defiziten.

Weiterbildung
Dieser Kernprozess umfasst die regelmäßige Planung eines Weiterbildungsprogramms sowie die Durchführung geplanter und ad-hoc erforderlicher Trainingsmaßnahmen.

Marktbeobachtung
Im Rahmen der kontinuierlichen Marktbeobachtung sind Entwicklungen am Markt, die Relevanz für die Weiterentwicklung



Seminare 2015

Projektmanagement

Intensiv Seminar Projektmanagement
Hamburg, 17.11. – 19.11.2015

Project Management Offices im IT-Umfeld
Hamburg, 25.06. – 26.06.2015

Soft Skills für Projektleiter/innen
Hamburg, 17.08. – 18.08.2015

Kommunikationskompetenz in Projektkrisen
Hamburg, 19.08. – 20.08.2015

IT-Projekte erfolgreich aus der Krise führen
Hamburg, 27.08. – 28.082015

IT SM

Einführung in die Prozessoptimierung
Hamburg, 05.10. – 06.10.2015

Prozessdokumentation gestalten
Hamburg, 07.10.2015

IT-Providermanagement
Hamburg, 06.11.2015

Erstellung von IT-Servicekatalogen
Hamburg, 04.12.2015

Outsourcing

IT-Ausschreibung mit Finanzierungsoptionen
Hamburg, 16.09. – 17.09.2015

Ausschreibung von IT-Dienstleistungen
Hamburg, 18.09.2015

Outsourcing von Workplace Services
Hamburg, 05.11.2015

IT-Outsourcing
Hamburg, 09.11. – 10.11.2015

ITK

Cloud Computing Overview
Stuttgart, 23.10.2015

Seminare: Info & Anmeldung
www.amendos.de/seminare
Tel (040) 248 276-00, info@amendos.de

der eigenen IT-Services haben, zu identifizieren. Erkannte relevante Markttrends sind in den kontinuierlichen Verbesserungsprozess einzubringen.

Fazit

Die dargestellten Aufgaben sind in Auswahl und Ausprägung grundsätzlich auf die vereinbarte Providerleistung auszurichten: ein Outsourcing aller IT-Leistungen an einen Provider bedarf einer anderen Ausgestaltung des Providermanagements als ein weniger komplexer und kritischer outgesourcter Managed Service.

Für alle Aufgaben sind entsprechende Vereinbarungen im Rahmen des Providervertrags Voraussetzung, d.h. der Vertrag ist wesentliche Grundlage für Aufbau und Ausgestaltung des Providermanagements.

Seminar

Seminar „IT-Providermanagement“

In diesem Seminar erhalten Sie…

- einen Überblick über das Aufgabengebiet des IT-Providermanagements,
- einen Einblick in die Möglichkeiten der Einbindung des IT-Providermanagements in die eigene Organisation,
- Tipps zur effizienten Ausgestaltung der Providersteuerung.

Termin: 06.11.2015 in Hamburg

Anmeldung: Tel (040) 248 276 00, info@amendos.de

Nach – der Providerleistung angemessener – Ableitung von Aufgaben im Providermanagement sind diese jeweils einer Instanz in der Auftraggeber-Organisation zuzuordnen. Viele der dargestellten Aufgaben lassen sich schon vor dem Outsourcing vorhandenen Fachabteilungen zuordnen, da diese jeweils die Kernkompetenz in diesem Aufgabenbereich besitzen. Dies sind u.a. häufig Aufgabenteile des Vertragsmanagements, des Finanzmanagements und des Projekt Portfolio Managements. Die Gesamtkoordination des Providermanagements sollte in einer Verantwortung liegen: diese Instanz hat dann das Zusammenspiel von beteiligten internen Einheiten und dem Provider sicherzustellen und weiterzuentwickeln.

Jörg Bujotzek

Impressum

amendos gmbh I Frankenstraße 3 I 20097 Hamburg
Tel (040) 248 276 00 I Fax (040) 248 276 01 I www.amendos.de I info@amendos.de I Geschäftsführer: Dipl. Oec. Jörg Bujotzek
Handelsregister: AG Hamburg HRB 105648 I Umsatzsteueridentifikationsnummer: DE 814989917

Erscheinungsweise 4 / jährlich I Bezug: kostenfrei als PDF I Copyright: amendos gmbh
Herausgeber und inhaltlich verantwortlich gemäß § 55 Abs. 2 RStV: Dipl. Oec. Jörg Bujotzek