



Leitfaden zur Unterstützung der Einführung von Cloud Computing

Organisationshilfe

*U*nternehmens- und
*I*nformations- *M*anagement
*C*ertification

- **Grundsätzliche Fragen zur Zielbestimmung**
- **Festlegung von Verantwortlichkeiten**
- **Interne Anforderung an ein Cloud Computing-System**
- **Prüfung eines Cloud Computing-Dienstleisters**
- **Abschließende Beurteilung der gewählten Lösung**

*Moltkestraße 19
42115 Wuppertal
Telefon (0202) 3 09 87 39
Telefax (0202) 3 09 87 49
E-Mail certification@uimcert.de
Internet www.uimcert.de*

Der folgende Leitfaden soll Ihnen helfen, den Einsatz von Cloud Computing strukturiert zu planen und dabei wesentliche Aspekte der Sicherheit und Ordnungsmäßigkeit zu berücksichtigen. Er erhebt keinen Anspruch auf Vollständigkeit und sollte durch eigene unternehmenstypische Fragen ergänzt werden.

Grundsätzliche Fragen	
<i>Es muss zunächst festgelegt werden, welche Anwendungen oder Einsatzgebiete mit der Einführung von Cloud Computing abgedeckt werden sollen, ob gleichzeitig neue Anwendungen hinzukommen und bestehende Systeme migriert werden und somit die Ziele erfüllt werden können.</i>	
<p>Erwartungen an das Cloud Computing Welche Erwartungen werden mit der Einführung von Cloud Computing verbunden? (bspw. Effizienz- und Leistungssteigerung, Sicherheit, Kostensenkung, geringere Abhängigkeiten)</p>	
<p>Ziele des Cloud Computings Welche Ziele sollen konkret mit dem Cloud Computing erreicht werden?</p>	
<p>Varianten des Cloud Computings Welche Varianten des CC kommen in Betracht? (Software-as-a-Service, Infrastructure-as-a-Service, Platform-as-a-Service; Private Cloud oder Open Cloud)</p>	
<p>Migration von Systemen in die Cloud (bspw. Office-Anwendungen, Buchhaltung, Personalwirtschaft, Warenwirtschaft, Logistik, allgemeine Datenhaltung, Führungsinformationssysteme, EDIFACT, Groupware, weitere)</p>	
<p>Neueinzuführende Systeme (bspw. Web-Hosting, Fax- oder Voice-over-IP-Dienste, Dokumenten-Management-Systeme (DMS), Chat, VPN-Gateways, Archivierungssysteme, andere)</p>	

<p>Budget Ist das Budget für die Einführung auch so kalkuliert, dass es eine Übergangsphase geben wird, in der Alt- und Neusystem betrieben werden müssen und gegebenenfalls später anfallende variable Kosten gedeckt sind?</p>	
---	--

Verantwortlichkeiten	
<i>Es sollte umfassend geklärt sein, wer bzw. welche Stellen an dem Einführungsprozess beteiligt sind und für welche Aspekte verantwortlich sind.</i>	
Strategische Entscheidungen	
(Vor-)Verhandlung mit den Anbietern	
Implementierung bzw. Migration	
Schulung der Mitarbeiter	
IT-Sicherheit	
Datenschutz-/Ordnungsmäßigkeitssicherung	
Organisation	
Abnahme des Systems	
Weitere	
<i>Auch für den laufenden Betrieb müssen Verantwortungen festgelegt sein.</i>	
Nutzer-Support	
Datensicherungen	
Business Continuity	
Überwachung des CC-Anbieters bzgl. Einhaltung von SLAs und Datenschutz	
Kontakt zum Mitarbeiter (intern)	

Interne Anforderungen an ein Cloud Computing-System <i>Intern muss abgestimmt werden, ob die eigenen Anforderungen an IT-Systeme durch Cloud Computing abgedeckt werden können.</i>	
Leistung Welche Anforderungen werden an die auszulagernden Systeme, bspw. Verarbeitungs- und Übertragungsgeschwindigkeit und an die Latenz/Reaktionszeit gestellt?	
Verfügbarkeit Muss zu bestimmten Zeiten eine Mindestverfügbarkeit gewährleistet sein?	
Vertraulichkeit Werden Daten verarbeitet, die derart vertraulich sind, dass ein erheblicherer Aufwand nötig ist, sie bei Cloud Computing angemessen vor Einsichtnahme Dritter zu schützen?	
Rechnungslegungsvorschriften Aspekte wie das Radierverbot erfordern eine absolute Integrität der Datenverarbeitung. Kann diese bei der entfernten Verarbeitung eingehalten werden?	
Eigene Internetverbindung Ist die eigene Internetanbindung dazu geeignet, die zu erwartenden Datenlasten zu erfüllen?	
Unternehmenspolitik Leiten sich aus der eigenen Unternehmenspolitik Anforderungen ab, die mit CC kollidieren könnten (z.B. Patentschutz, Verträge, etc.)?	
Einhaltung gesetzlicher Ordnungsmäßigkeitsbedingungen Können sämtliche von Ihnen als Unternehmen zu einzuhaltenden Ordnungsmäßigkeitsanforderungen im Hinblick auf: <ul style="list-style-type: none"> • Wiederlesbarmachen, • Archivierung, • Datenschutz • spezielle Gesetze (z. B. Gesundheitswesen) erfüllt werden? 	

Prüfung des Cloud Computing-Dienstleisters <i>Das vorgesehene Angebot sollte vom Anbieter derart transparent gestaltet sein, dass es Ihnen möglich ist, folgende Fragen sicher zu beantworten.</i>	
<p>allgemeine Eignung des Anbieters Hat der potentielle Anbieter bereits Erfolge bei aussagekräftigen Referenzkunden gehabt?</p> <p>Hat der Anbieter generell ein gutes Renommee?</p> <p>Versteht er die Branche und bietet entsprechende Dienstleistungen und Support an?</p>	
<p>Unterstützung bei der Einführung Bietet der Anbieter umfassende Leistungen an, die bei der Einführung behilflich sind (z.B. Beratung, Tutorials, Schulungen, Ausführen der Implementierung)?</p>	
<p>SLAs, AGB und Verträge Wurden die Dienstleistungsverträge durch eine sachkundige interne oder externe Stelle umfassend geprüft?</p> <p>Ist sichergestellt, dass die zugesagten Leistungen tatsächlich erbracht werden müssen und nicht willkürlich ausgeschlossen werden können?</p>	
<p>Wechsel des Anbieters Ist vertraglich sichergestellt, dass ein Wechsel des Anbieters in angemessener Frist möglich ist?</p>	
<p>Gerichtsstand Ist der Gerichtsstand im Einsatzland bzw. zumindest innerhalb der EU?</p>	
<p>Versicherungen und Eigenkapital Ist der Anbieter ausreichend versichert, sodass ggf. Schadensersatzforderungen entsprochen werden können?</p> <p>Verfügt er über genügend Eigenkapital und Rücklagen, um langfristig die Leistung bieten zu können?</p>	

<p>Support Bietet der Anbieter eine kompetente (ggf. kostenlose) Unterstützung? Ist der Helpdesk auch auf große Beanspruchung ausgelegt?</p>	
<p>Standort der Server Ist definiert, wo die Cloud Computing Hosts untergebracht sind? Wird die Datenverarbeitung dynamisch auf Systeme verteilt, die ggf. im Ausland stehen? Sind die Rechenzentren gegen Einbruch, technisches Versagen und höhere Gewalt geschützt; ist die Organisation ordnungsgemäß?</p>	
<p>Eigentum der verarbeiteten Daten Hat der Anbieter ggf. vertraglich ein Anrecht auf die verarbeiteten Daten gestellt? Werden die Daten seitens des Anbieters für eigene Zwecke ausgewertet (Data Mining)?</p>	
<p>Verschlüsselungsverfahren Kann eine sichere Verschlüsselung der Datenhaltung und -übertragung aktiviert werden?</p>	
<p>Vertraulichkeit Ist vertraglich sichergestellt, dass die Vertraulichkeit hinreichend gewahrt bleibt und Mitarbeiter des Anbieters zur Wahrung der Verschwiegenheit verpflichtet sind?</p>	
<p>Verfügbarkeit Sichert der Anbieter vertraglich eine definierte Verfügbarkeit zu? Werden Vertragsstrafen bei Unterschreitung fällig?</p>	
<p>Datensicherung Sind Backup-Verfahren möglich, auf deren Ausgestaltung der Auftraggeber Einfluss nehmen kann? Werden die Sicherungen andernorts, mindestens in einem anderen Brandabschnitt, gelagert?</p>	

<p>Löschen von Daten Können Daten physisch gelöscht werden? Ist sichergestellt, dass keine Schattenkopien verbleiben?</p>	
<p>Kompatibilität der Daten Sind die Daten so beschaffen, dass sie auch jenseits des Anbieters (d.h. intern oder bei Dritten) vollumfänglich genutzt werden können?</p>	
<p>Steuerung von Updates Ist gewährleistet, dass dem Nutzer die Autonomie bleibt, selbsttätig Updates an den Systemen vorzunehmen oder zu verweigern?</p>	
<p>Möglicher Ausstieg Garantiert der Anbieter im Bedarfsfalle Möglichkeiten zu einem vollständigen und verlustfreien Ausstieg aus dem Cloud Computing und gibt er Unterstützung dazu?</p>	
<p>Beleg für die Qualität Bestätigen Gutachten, Gütesiegel oder Zertifikate nach einschlägigen Normen und Gesetzen die Ordnungsmäßigkeit und Qualität des Anbieters?</p>	

Abschließende Beurteilung der gewählten Lösung	
<i>Vor der Entscheidungsfindung, sollten für die folgenden Punkte konkrete Antworten vorliegen.</i>	
<p>Zielrealisierung Ist die gewählte Lösung geeignet, die gesetzten Ziele zu erfüllen?</p> <p>Worin bestehen gegebenenfalls Mängel?</p>	
<p>Risiken Können die mit dem Cloud Computing verbundenen Risiken getragen oder abgewälzt werden; kann ihnen angemessen begegnet werden?</p>	
<p>Business Continuity Sind die Verfahren für die Wiederaufnahme des Geschäftsbetriebs denen, die bisher angewandt werden, zumindest gleichwertig?</p>	
<p>Qualifizierte Mitarbeiter Ist trotz der Einführung von Cloud Computing noch sichergestellt, dass auf genügend IT-Kompetenz im Haus zurückgegriffen werden kann, um das Cloud Computing kompetent zu überwachen?</p>	
<p>Dokumentation der Lösung Liegt ein Fachkonzept bzw. Pflichtenheft vor, das die Umstellung auf Cloud Computing und den folgenden Betrieb umfassend dokumentiert?</p>	