UIMCert-Checkliste Cloud Computing

1. Management der IT-Sicherheit	a) Hat sich das Management hinlänglich mit der Thematik Cloud Computing befasst und dessen Einsatz vorab genehmigt? b) Kennt das Management die Risiken, insbes. die IT-Sicherheitsrisiken, die mit dem Cloud Computing verbunden sind und wurden diese in einer Risikoanalyse niedergelegt? c) Wird betrachtet, dass der Cloud Computing-Betrieb noch immer im Rahmen der Verantwortung des Managements liegt, sodass daraus entsprechende Konsequenzen abgeleitet werden (z. B. Haftungsprobleme des Managements)? d) Existieren Organisationsanweisungen, die sich speziell mit der Nutzung des Cloud Computings beschäftigen?
2. Qualität des Risikomanagements	a) Wurden grundsätzlich Risiken, die durch das Cloud Computing entstehen können, erkannt, bewertet und durch Maßnahmen aufgefangen? b) Wurden die in der Cloud verarbeiteten Daten hinsichtlich ihrer Kritikalität für Unternehmen und Stakeholder klassifiziert? c) Wurden neben den Aspekten einer höheren Flexibilität (Skalierbarkeit) und ggf. geringerer Energiekosten (Green IT) auch etwaige Kosten durch fahrlässigen Umgang mit schützenswerten Daten oder schwacher Verfügbarkeit einkalkuliert? d) Ist das Risikomanagement dahingehend durchgeführt worden, dass das Cloud Computing ein zentraler Angriffspunkt für die gesamte Betriebssicherheit darstellt?
3. Vorhandensein von Business Continuity-Konzepten	Liegt ein umfassendes Business Continuity-Konzept vor, das insbesondere betrachtet, dass a) es bei (massenhaften) Ausfällen bei Anbietern von Cloud Computing zu massiv verzögerten Reaktionszeiten kommen kann? b) ein Wiederanlauf nur sehr eingeschränkt durch eigenes Eingreifen erwirkt werden kann? c) Anbieter, insb. in der Online-Branche, unvorhersehbar plötzlich insolvent oder übernommen werden oder ihre Geschäftsstrategie ändern, sodass kurzfristig auf alternative Lösungen zurückgegriffen werden können muss?

4. Qualität der technischen Lösungen	a) Wie erfolgt die Abnahme im Hinblick darauf, dass Systeme ggf. nicht ganzheitlich betrachtet werden können (Intransparenz)? b) Inwiefern sind vertrauliche Daten und die Datenübertragung durch Verschlüsselung oder ähnliche Maßnahmen geschützt? c) Da ggf. die zu nutzenden physischen Systeme weit entfernt sind: wie ist die integere und zeitsynchrone Datenübertragung gewährleistet? d) Ist sichergestellt, dass eine Migration vollständig, verlustfrei und ordnungsgemäß sowohl von den Alt-Systemen zur Cloud als auch im Bedarfsfalle umgekehrt erfolgen kann (Lock-in-Effekt)?
5. Vorhandensein von klaren vertraglichen Lösungen in Form von SLAs	a) Sind bezüglich des Cloud Computing Sicherheitsmaßnahmen, Leistungsbeschreibungen und Form der Lieferung vertraglich in SLAs fixiert? b) Werden das Angebot und die Einhaltung der SLAs systematisch überwacht? c) Betreibt der Anbieter ein sicheres Rechenzentrum (Zutritt, höhere Gewalt etc.)?
6. Klare Konzepte zur Speicherungsarchivierung, Auslagerung und Löschung	a) Ist die Speicherinfrastruktur des Anbieters so beschaffen, dass Inkonsistenzen (bspw. durch Mehrfachvermietung) vermieden werden und sowohl Verfügbarkeit als auch Datensicherheit jederzeit gewährleistet sind? b) Umfasst das Angebot prüfsichere Methoden zur Datensicherung und Archivierung, auf deren Ausgestaltung der Kunde selbst Einfluss nehmen kann? c) Ist sichergestellt, dass bei Löschung von Daten diese auch tatsächlich erfolgt, somit keine Daten auf den physischen Host-Systemen mehr vorhanden sind?

7. Qualitativ hochwertiges Datenschutzkonzept	Existiert ein Datenschutzkonzept, das im Hinblick auf die Einführung von Cloud Computing berücksichtigt, dass a) es sich um eine Form der Auftragsdatenverarbeitung handelt, die gemäß der einschlägigen Datenschutzgesetze gestaltet werden muss (§§ 9, 11 BDSG)? b) nicht immer ausgeschlossen werden kann, dass – je nach Form des Cloud Computing - Daten möglicherweise in *unsicheren Drittstaaten* verarbeitet werden (§§ 4d, 28 BDSG)? c) sich Cloud Computing sich auch grundsätzlich als Mittel zur Telearbeit realisieren lässt und daher besonderen Anforderungen unterliegen kann?
8. Dokumentierte Lösungen in Bezug auf die Einhaltung von Ordnungsmäßigkeitsanforderungen in Bezug auf Steuer-, Handels- und Datenschutzrecht	a) Werden Daten/Belege revisions- und manipulationssicher – d. h. ordnungsgemäß entsprechen der Forderungen der aktuellen Gesetzgebung - abgelegt? b) Ist vertraglich geregelt, wie die Vertraulichkeit gewährleistet wird? c) Wie wird verhindert, dass unbefugte Dritte Zugriff jedweder Art auf die Cloud Computing-Systeme haben?
9. Vorhandensein von qualifizierten Mitarbeitern	a) Ist trotz der Auslagerung des Betriebs von Cloud Computing gewährleistet, dass auf ausreichende (auch interne) IT-Kompetenzen zurückgegriffen werden kann, die erforderlich sind, um die Prozesse zu disponieren, zu organisieren, zu administrieren und das IT-Management des Anbieters zu prüfen? b) Sind die Endanwender in den Bereichen Selbsthilfe, Maßnahmen zur IT-Sicherheit und auch möglicher spezifischer Risiken geschult? c) Greift eine umfassende Personalentwicklung, die sicherstellt, dass Kompetenzen für Systeme, die einem entwicklungsbedingt hohen Wandel unterliegen und auch die Datenschutz-Sensibilisierung angemessen vorhanden sind/vermittelt werden?

10. Erworbene Zertifikate auf den Sektoren IT-Management, IT-Sicherheit und Datenschutz	a) Ist ein ISMS etabliert worden, zu dessen Scope explizit auch die externe Datenverarbeitung in Clouds gehört? b) Wurde die IT einschließlich des Cloud Computings von Dritten auditiert oder gar nach einer einschlägigen Norm wie der ISO/IEC 27001-02 zertifiziert, sodass der sichere Betrieb belegt ist? c) Wurde die Verarbeitung personenbezogener Daten von Sachverständigen bewertet und ggf. die Ordnungsmäßigkeit mit einem Gütesiegel bestätigt. Die Auswirkungen auf die Innen- und Außenwirkungen dürfen nicht vernachlässigt werden.