IT-Prüfung beim Einsatz von Cloud Computing: eine Analyse und Diskussion des IDW ERS FAIT 5

Bachelorarbeit

zur Erlangung des akademischen Grades „Bachelor of Science (B.Sc.)“ im Studiengang Wirtschaftswissenschaft der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Gronkowski Vorname: Alexander Maximilian

[redacted] [redacted] [redacted] [redacted]

Prüfer: Prof. Dr. M. H. Breitner

Hannover, den 10.08.2015

Inhaltsverzeichnis

1. Einleitung

1.1 Relevanz des Themas

“Cloud computing is often far more secure than traditional computing, because companies like Google and Amazon can attract and retain cyber-security personnel of a higher quality than many governmental agencies.”[1] Dies sind die Worte von Vivek Kundra, dem Federal Chief Information Officer der Vereinigten Staaten von Amerika. Diese Aussage deutet auf kritische Art und Weise an, welches Gefahrenpotenzial in der Nutzung von Cloud Computing liegt.

Der Einsatz von Informationstechnologie unterliegt in Unternehmen derzeit einem Paradigmenwechsel. Der Wandel von der ausschließlich unternehmenseigenen Betreibung von IT hin zu IT-Outsourcing hat längst begonnen. So nutzten in Deutschland im Jahr 2014 bereits 44% der Unternehmen Cloud Computing. Dies ist eine Steigerung von 16 Prozentpunkten seit 2011. Weitere 24% der Unternehmen planen den Einsatz von Cloud Computing. Es lässt sich somit ein solides Wachstum des Cloud Einsatzes für die kommenden Jahre prognostizieren. Die Nutzung der Dienstleistung, Cloud Computing, war lange Zeit nur Großunternehmen und Konzernen vorbehalten. Die aktuelle Entwicklung zeigt, dass auch kleinere Unternehmen verstärkt auf die Cloud setzen. Die folgende Abbildung, in der die Unternehmen hinsichtlich ihrer Mitarbeiteranzahl kategorisiert sind, veranschaulicht diesen Trend.[2]

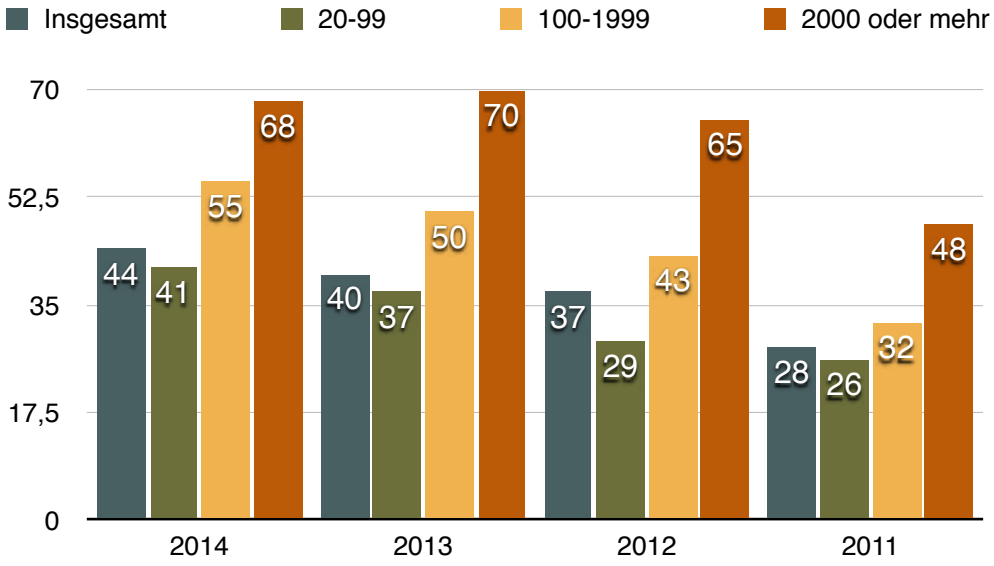

Abbildung 1: Prozentuale Darstellung des Cloud Computing Einsatzes
Quelle: Eigene Darstellung in Anlehnung an KPMG 2015

[1] Kundra (2011)

[2] Vgl. KPMG (2015), S. 5-9

Cloud Computing stellt also eine Dienstleistung dar, die den Umgang und die Nutzung von IT in Unternehmen grundlegend verändern soll. Es ist der nächste Schritt zu einem, auf Nachfrage basierenden Service. Dieser bietet Unternehmen auf der einen Seite die Möglichkeit, sich lückenlos auf das jeweilige Kerngeschäft zu konzentrieren und somit gegenüber der Konkurrenz einen Wettbewerbsvorteil zu bilden. Auf der anderen Seite gibt es jedoch auch mannigfaltige Gefahrenpotentiale bei der Nutzung von Cloud Computing. Um den Gefahren und Risiken entgegen zu wirken, wird im Rahmen einer Abschlussprüfung beim auslagernden, prüfungspflichtigen Unternehmen die IT-Prüfung durchgeführt. Diese soll sicherzustellen, dass das IT-gestützte Rechnungslegungssystem die vorgeschriebene Ordnungsmäßigkeit erfüllt und somit die Verlässlichkeit der in Buchführung, im Jahresabschluss und im Lagebericht enthaltenen Daten gewährleistet wird. Das Institut der Wirtschaftsprüfer legt in seinen Verlautbarungen die Berufsauffassung dar, wie die Abschlussprüfung beim Einsatz von Cloud Computing vorzunehmen ist.[3] [4]

Im Rahmen der Wirtschaftsprüfung, insbesondere der IT-Prüfung, existieren eine Vielzahl von Standards. Das Institut der Wirtschaftsprüfer (IDW) gilt in Deutschland als wichtiger Standardsetter. Das IDW ist ein eingetragener Verein, welcher das Interesse seiner rund 13.000 Mitglieder wahrt und deren Berufsausübung durch fachlichen Rat und berufsständische Standards unterstützt. Die Mitglieder setzen sich aus ca. 12000 Wirtschaftsprüfern, was fast 83% aller Wirtschaftsprüfer in Deutschland ausmacht, und etwa 1000 Prüfungsgesellschaften zusammen. Die Erstellung von Verlautbarungen, welche sich auf die verschiedenen Bereiche der Jahresabschlussprüfung beziehen, ist die primäre Funktion des IDW. Gerade unter der neuen Herausforderung „Cloud Computing“ sind Standards zum Thema IT-Sicherheit und IT-Outsourcing von besonderer Bedeutung. Der IDW hat hierzu einen Entwurf entwickelt, den IDW ERS FAIT 5. Dieser Standard bezieht sich auf die Themenblöcke IT-Outsourcing und Cloud Computing. Der FAIT 5 definiert vorwiegend Anforderungen an die IT und an die damit verbundene Umsetzung durch die gesetzlichen Vertreter der Unternehmen beim IT-Outsourcing bzw. Cloud Computing. Ein „verwandter“ Standard des FAIT 5 ist der IDW RS FAIT 1. Der FAIT 1 gilt als offizielle Verlautbarung und definiert die Anforderungen für den klassischen Einsatz von IT im Unternehmen.[5]

Das Ziel dieser Arbeit ist die Beantwortung der Forschungsfragen, um so die IT-Prüfung beim Einsatz von Cloud Computing näher zu durchleuchten und somit eine

[3] Vgl. Wood (2012), S. 1-2

[4] Vgl. IDW RS FAIT 1 (2002), S. 4

[5] Vgl. IDW (o.J.)

Aussage über die Rolle und Bedeutung des IDW ERS FAIT 5 zu bilden. Es handelt sich um die folgenden Fragen:

Forschungsfrage
1. Welche Verlautbarungen des IDW sind für die Abschlussprüfung beim Einsatz von IT und bei der Auslagerung rechnungslegungsrelevanter Dienstleistungen, insbesondere Cloud Computing, relevant?
2. Welche Anforderungen ergeben sich aus den Verlautbarungen, FAIT 1 und FAIT 5, an die IT und an die damit verbundene Umsetzung durch die gesetzlichen Vertreter und was sind die größten Unterschiede in den Anforderungen?
3. Kann die Hypothese bestätigt werden, dass beim Einsatz von Cloud Computing absolute Sicherheit für das auslagernde Unternehmen vorliegt, wenn die aus dem IDW FAIT 5 definierten Anforderungen eingehalten werden?

Abbildung 2: Übersicht der Forschungsfragen
Quelle: Eigene Darstellung

Die drei, aufeinander aufbauenden Forschungsfragen werden in dieser Arbeit in chronologischer Reihenfolge bearbeitet und beantwortet.

1.2 Stand der Forschung

Für die Forschungsfragen ist es relevant herauszubilden, inwieweit speziell der IDW ERS FAIT 5 bereits in vorherigen Arbeiten zum Thema gemacht worden ist. Die Recherche stützt sich dabei auf die Suchmaschine „Google Scholar“. Die folgende Tabelle zeigt, zu welchen Ergebnissen die Verwendung der jeweiligen Suchbegriffe geführt hat:

Suchbegriffe	Ergebnisse	Davon ist durchsucht worden	Tatsächlicher Bezug auf den FAIT 5
IDW ERS FAIT 5	21	alles	1
„FAIT 5“	149	alles	2
Auslagerung Dienstleistungen Cloud Computing Prüfung FAIT 5	5	alles	3

Tabelle 1: Übersicht Stand der Forschung
Quelle: Eigene Darstellung

Als Filter wurde eingestellt, dass Scholar nur Ergebnisse anzeigt, die nicht älter als 2014 sind. Ältere Ergebnisse besitzen keine Relevanz, da der Entwurf des FAIT 5 erst am 04.11.2014 veröffentlich worden ist.[6] Die am 22.07.2015 ordnungsgemäß durchgeführte Literaturrecherche, hat gezeigt, dass es sehr wenig Literatur bzw. wissenschaftliche Werke zu dem IDW ERS FAIT 5 gibt. Ein Werk wurde allerdings bei allen Suchdurchläufen mehrmals gefunden: das Buch mit dem Titel „IT-Services in der Cloud und der ISAE 3402“. Die Autoren (Lissen, Damhorst und Brünger) äußern sich in ihrem Werk zum FAIT 5 nur dahingehend, dass dieser in Zukunft die erste IDW Verlautbarung sein wird, die sich unmittelbar auf die Cloud-Thematik bezieht.[7]

Die durchgeführte Literaturrecherche zeigt unter Vorbehalt, dass es bisher keine Literatur zum IDW ERS FAIT 5 gibt.

1.3 Struktur und Aufbau der Arbeit

Nachdem bisher die Relevanz des Themas und der Stand der Forschung durchleuchtet worden sind, wird zum Abschluss des 1. Kapitels aufgezeigt, dass Experten zur Beantwortung der Forschungsfragen miteinbezogen werden. Die Funktion der Experten für diese Arbeit, sowie die Experten selbst und ihre zugehörigen Unternehmen werden in Abschnitt 1.4 beschrieben.

Im 2. Kapitel werden zunächst allgemeine Grundlagen zu Cloud Computing dargestellt, um einen Einblick in die Thematik zu gewähren. Neben der für diese Arbeit verwendeten Definition von Cloud Computing, der Abgrenzung von Cloud Computing zu IT-Outsourcing und die Beschreibung von essentiellen Charakteristika der Dienstleistung Cloud Computing, wird dem Leser das 3-Ebenenmodell der Cloud Service Modelle, sowie die verschiedenen Organisationsformen von Cloud Computing näher gebracht. Abgeschlossen wird das Kapitel mit einer ersten Darstellung von Risiken und Risikodimensionen, welche durch die Nutzung von Cloud Computing entstehen können.

Anschließend wird im 3. Kapitel die erste Forschungsfrage dieser Arbeit beantwortet. Diese beschäftigt sich mit den Verlautbarungen des IDW zur Thematik der IT-Prüfung beim eigenbetrieblichen Einsatz von IT und bei der Auslagerung von rechnungslegungsrelevanten Dienstleistungen. Dazu erfolgt zunächst eine Beschreibung des Ziels und der Grundlagen der Jahresabschlussprüfung. Im Anschluss wird die Rolle des IDW und dessen Verlautbarungen in Bezug auf Cloud

[6] Vgl. IDW ERS FAIT 5, S. 1

[7] Vgl. Lissen / Brünger / Damhorst (2014), S. 52

Computing näher erläutert und in einen logischen Zusammenhang gesetzt. Abschließend folgt ein Einblick in die Arbeitsweise des IT-Prüfers, indem die wichtigsten Prüfungsstandards für diese Arbeit dem Leser näher gebracht werden.

Mithilfe des 4. Kapitels wird die zweite Forschungsfrage beantwortet. Dabei werden die, aus den Verlautbarungen sich ergebenen Anforderungen an die Einrichtung eines IT-Systems mit dazugehörigen IKS und die damit verbundenen Verantwortungen der gesetzlichen Vertreter beim allgemeinen Einsatz von IT, sowie bei der Auslagerung von rechnungslegungsrelevanten Dienstleistungen näher erläutert und analysiert. Abschließend werden die daraus resultierenden Unterschiede und Zusammenhänge in einem Fazit deutlich gemacht.

Im 5. Kapitel wird die letzte Forschungsfrage betrachtet, um diese in einer Diskussion zu beantworten. Dafür wird untersucht, ob die im FAIT 5 definierten Anforderungen an IT und deren Umsetzung durch die gesetzlichen Vertreter, alle Sicherheitsrisiken abdecken können und somit eine absolute Sicherheit bei der Nutzung der Dienstleistung Cloud Computing vorliegt. Im Abschnitt 5.2 findet diesbezüglich eine Diskussion mit anschließender Würdigung des FAIT 5, einschließlich Verbesserungsempfehlungen, statt.

Die wichtigsten Erkenntnisse werden im Fazit zusammengefasst und es wird ein Ausblick auf die zukünftige Entwicklung der IT-Prüfung i.V.m. Cloud Computing gewährt (Kapitel 6).

1.4 Experteninterview

Für die Beantwortung der Forschungsfragen und um die Ausführungen dieser Arbeit zu unterstützen und zu ergänzen wurden Experteninterviews durchgeführt. Die Interviews dienen also nicht dazu grundlegende Erkenntnisse zu generieren, sondern der Vertiefung bereits gewonnener Kenntnisse. Durch die Stellungnahmen der Experten wird zudem ein direkter Praxisbezug hergestellt.

Über die genaue Bedeutung des Begriffs „Experteninterview“ streiten die Organisationsforscher und somit existiert diesbezüglich auch keine allgemein gültige Definition. Im Rahmen dieser Arbeit werden die folgenden Ausführungen dieses Abschnitts als Definition verwendet. Das Experteninterview ist als ein Einzelgespräch auf qualitativer Basis zu verstehen. Die Gesprächsteilnehmer sind ein Interviewer und ein Experte. Der Interviewer erhebt durch das Gespräch Daten, welche beispielweise für ihn neue Erkenntnisse generieren können oder bereits aufgestellte Hypothesen untermauern. Als Experten werden Fachleute, Sachverständige oder Kenner bezeichnet, die über einen solch besonderen Wissensbestand verfügen, um

fachlich komplexe Sachverhalte für außenstehende Dritte nachvollziehbar zu durchleuchten.[8]

Der Aufbau des Interviews ist so gestaltet, dass sich die ersten Fragen auf die Relevanz des Themas und auf den befragten Experten selbst beziehen. Die nachfolgenden Fragen beziehen sich in chronologischer Reihenfolge auf die drei Forschungsfragen. Insgesamt sind vier Interviews mit den Vertretern der „Big Four“ Gesellschaften durchgeführt worden. Der Fragebogen, sowie die wichtigsten Ergebnisse der Interviews sind im Anhang dieser Arbeit abgebildet. Die folgende Tabelle dient der Veranschaulichung der interviewten Experten.

Name	Gesellschaft	Position
Markus Vehlow	PricewaterhouseCoopers	Partner
Markus Scherer	KPMG	Assistent Manager
Vladyslav Dunajevski	Deloitte & Touche	Manager
Boris Gurewitsch	EY	Manager

Tabelle 2: Übersicht der Experten
Quelle: Eigene Darstellung

Es sind explizit Vertreter der Big Four Gesellschaften angesprochen wurden, da diese zusammen einen signifikant hohen Marktanteil in Deutschland und auch weltweit einnehmen. So werden beispielsweise alle Dax-30 und 48 von 50 M-Dax Unternehmen von einer Gesellschaft der Big Four Gruppierung geprüft. Insgesamt nehmen die Big Four einen Marktanteil von ungefähr 83% in Deutschland ein.[9] [10]

[8] Vgl. Taffertshofer / Kühl / Strodtholz (2009), S. 32 - 34

[9] Vgl. wp.net e.V. (o.J.)

[10] Vgl. steuerazubi UG (o.J.)

auf das Bereitstellungsmodell der Public Cloud beschränken. Ergänzungen für die Private Cloud sind dringend erforderlich.[121] [122] [123]

Auf Basis der mit Mängel behafteten Stellung des FAIT 5 könnte man zu dem Ergebnis kommen, dass der FAIT 5 überflüssig ist. Doch der FAIT 5 stellt für den Abschlussprüfer die Grundlage der Prüfung von Cloud Computing dar, welche den Rahmen der Prüfung definiert. Zudem gilt der Standard als Instrument, das vor dem Mandanten die Notwendigkeit der Prüfung durch die Abschlussprüfer rechtfertigt, da er den konkreten Auftrag der Prüfung definiert.[124]

Es gilt also, festzuhalten, dass der FAIT 5, nach seiner offiziellen Verabschiedung, ein etabliertes Dokument im Prüfungsalltag wird, das den Abschlussprüfer unterstützt, jedoch alleine nicht alle Sicherheitsrisiken abdeckt.

6. Fazit, Limitation und Ausblick

Ziel dieser Arbeit war es, die drei Forschungsfragen zu beantworten, um so die IT-Prüfung beim Einsatz von Cloud Computing näher zu durchleuchten und somit eine Aussage über die Rolle und Bedeutung des IDW ERS FAIT 5 zu bilden.

Forschungsfrage
1. Welche Verlautbarungen des IDW sind für die Abschlussprüfung beim Einsatz von IT und bei der Auslagerung rechnungslegungsrelevanter Dienstleistungen, insbesondere Cloud Computing, relevant?
2. Welche Anforderungen ergeben sich aus den Verlautbarungen, FAIT 1 und FAIT 5, an die IT und an die damit verbundene Umsetzung durch die gesetzlichen Vertreter und was sind die größten Unterschiede in den Anforderungen?
3. Kann die Hypothese bestätigt werden, dass beim Einsatz von Cloud Computing absolute Sicherheit für das auslagernde Unternehmen vorliegt, wenn die aus dem IDW FAIT 5 definierten Anforderungen eingehalten werden?

Abbildung 12: Übersicht der Forschungsfragen
Quelle: Eigene Darstellung

Das Ergebnis der 1. Forschungsfrage ist, dass der IDW ERS FAIT 5 als die erste Verlautbarung des IDW identifiziert worden ist, die einen direkten Bezug zum Thema Cloud Computing herstellt. Im Rahmen der Experteninterviews ist dabei hervorgegangen, dass lediglich PwC, als bisher einziges Unternehmen der Big Four, den FAIT 5 bei der Prüfung miteinbezieht. Bezogen auf die 2. Forschungsfrage ist

[121] Vgl. Anhang 3

[122] Vgl. Anhang 4

[123] Vgl. Anhang 5

[124] Vgl. Anhang 3

festzuhalten, dass sowohl der FAIT 5, als auch sein Schwesternstandard, der FAIT 1, eine Unmenge von Anforderungen an die IT und an die damit verbundene Umsetzung durch die gesetzlichen Vertreter der Unternehmen vorgibt. Während der FAIT 5 hinsichtlich der Anforderungen an die IT keine signifikant veränderten Neuerungen definiert, kommen auf die gesetzlichen Vertreter erhebliche Veränderungen zu. Als ein Beispiel ist aufzuführen, dass für die gesetzlichen Vertreter der auslagernden Unternehmen beim Einsatz von Cloud Computing nicht nur die eigene ordnungsmäßige IT relevant ist, sondern auch die IT des Dienstleisters. So kommen auf die gesetzlichen Vertreter die neuen Aufgaben der Überwachung, Kontrolle und Steuerung des Dienstleisters zu. Hat ein Unternehmen mehrere Dienstleister beauftragt, so steigt das benötigte Arbeitsvolumen proportional mit der Anzahl der Dienstleister. Dies führt dazu, dass die auslagernden Unternehmen in diesem Bereich personelle Veränderungen vorzunehmen haben. Sie brauchen daher entweder mehr Personal, Personal einer höheren Qualität oder eine Kombination von Beidem. Hinsichtlich der 3. Forschungsfrage ist festzuhalten, dass sowohl die Literaturanalyse, als auch die Experteninterviews die Hypothese widerlegen. Ein Unternehmen, das ihr IT-System strikt nach den Vorgaben des FAIT 5 aufbaut, wird dadurch keine absolute Sicherheit generieren können. Auf der anderen Seite ist eine Prüfung, die lediglich nach FAIT 5 stattfindet ebenfalls nicht vollständig. Auf beiden Seiten bedarf es die Ergänzung durch andere, branchenspezifische Standards, um zumindest hinreichende Vollständigkeit zu gewährleisten. Abschließend ist festzuhalten, dass der Entwurf des FAIT 5 in der Praxis aus der Sicht der Prüfer durchaus willkommen ist, denn er legitimiert und rechtfertigt die Prüfung und schafft den Prüfungsrahmen.

Da es sich beim FAIT 5 bisher nur um einen Entwurf handelt, wird diese Arbeit dadurch limitiert. Alle Ausführungen mit zugehörigen Ergebnissen beziehen sich auf den Entwurf. Wird der FAIT 5 offiziell vom IDW verabschiedet und beinhaltet der FAIT 5 dann die in Abschnitt 5.2 beschriebenen, grundlegenden Änderungen, so kann dies einen signifikanten Einfluss auf den Aussagewert der Ergebnisse dieser Arbeit haben.

Für einen Ausblick in die Zukunft lässt sich ein klarer Trend erkennen, denn der Anteil der Unternehmen in Deutschland, die Cloud Computing einsetzen, wird weiter kontinuierlich zunehmen. Dadurch, dass Cloud Computing im Unternehmen zunimmt, wird auch der IT-Prüfung, die Cloud Computing miteinbezieht, eine höhere Bedeutung zu teil. Die Bekämpfung der wohl bedeutsamsten Risiken von Cloud Computing, Compliance, Datenschutz und Datensicherheit, ist bereits in der Gegenwart eine große Herausforderung. Dazu bedarf es der Entwicklung von weiteren Standards, Erweiterungen bereits etablierter Standards und allgemeinen Lösungen, um diesen Risiken entgegenzuwirken.

Gemäß den Aussagen von Herrn Vehlow lassen sich darüber hinaus in naher und ferner Zukunft zwei bedeutsame Entwicklungen erkennen. In naher Zukunft wird es so sein, dass der Begriff Intercloud für ein neues Risiko sorgt. Der Begriff steht für die Cloud in der Cloud. Dies bietet den Unternehmen bspw. die Möglichkeit, ihr ERP-System schnell und unkompliziert von einem anderen, kostengünstigeren Provider betreiben zu lassen. Dadurch ist es kaum nachvollziehbar, wo sich die Daten überhaupt befinden. Im Umkehrschluss stellt dies eine erhebliche Gefährdung der Daten dar. In ferner Zukunft wird sich die gesamte Abschlussprüfung revolutionierend verändern müssen. Dies wird das Berufsbild des Wirtschaftsprüfers komplett verändern und möglicherweise auch überflüssig machen, denn die Systeme werden in der Lage sein, sich selbst zu zertifizieren und zu prüfen. Wirtschaftsprüfungs-gesellschaften werden sich andere Möglichkeiten suchen müssen, um Wert-schöpfung zu betreiben.[125]

Abschließend bleibt festzuhalten, dass sich nicht nur der Markt für Cloud Computing, sondern auch der gesamte Bereich der Jahresabschlussprüfung einer spannenden und innovativen Entwicklung unterziehen wird. Wie genau die Zukunft gestaltet wird und wann sie beginnen wird, bleibt abzuwarten.

[125] Vgl. Anhang 3