1. GoB bei Auslagerung von rechnungsrelevanten Dienstleistungen sowie Cloud Computing – IDW RS FAIT 5

09/2019

Bei Auslagerung von betrieblichen Funktionen an andere Dienstleistungsunternehmen **durch Gewerbetreibende, die selbst rechnungslegungs- und ggf. prüfungspflichtig sind**, **verbleibt die Verantwortung** für die Einhaltung der gesetzlichen Anforderungen an die Ordnungsmäßigkeit der Rechnungslegung bei den gesetzlichen Vertretern des auslagernden (auftraggebenden) Unternehmens.

Neben den **Chancen**, die dieses Modell bereithält, sind auch die **Risiken** für das auslagernde Unternehmen zu beachten sowie deren Auswirkungen auf das interne Kontrollsystem.[1]

„*Der IDW RS FAIT 5 konkretisiert die bei der Auslagerung von rechnungslegungsrelevanten Prozessen und Funktionen (**IT-Outsourcing**)*

- aus den ***§§ 238, 239 und 257 HGB*** resultierenden ***Anforderungen*** an die Führung der Handelsbücher mittels IT-gestützter Systeme
- und verdeutlicht die beim Einsatz von ***Cloud Computing*** möglichen Risiken für die ***Einhaltung der Grundsätze ordnungsmäßiger Buchführung***."[2]

Den Steuerberater treffen hierbei Hinweispflichten, während der Abschlussprüfer seine Prüfung inhaltlich darauf auszurichten hat.

Stand: 04.10.2023

1.1 Inhalte

Der IDW RS gibt eingangs einen Überblick zu der **Auslagerung von rechnungslegungsrelevanten Dienstleistungen durch Gewerbetreibende**, bspw. zu Arten des Cloud Computings, und beschreibt die typische Vorgehensweise beim IT-Outsourcing.

Die **Einführung in die Fachsprache** des IDW RS FAIT 5 ermöglicht den Abschlussprüfern einen sachgerechten fachlichen Austausch mit dem **Mandanten** und eine strukturierte Dokumentation. Anschließend werden die **Sicherheit, die Ordnungsmäßigkeit und die Verantwortung der gesetzlichen Vertreter** auftragserteilender Gewerbetreibenden beim IT-Outsourcing dargestellt und die in diesem Zusammenhang auftretenden Risiken aufgezeigt.

Den Hauptteil bilden die Themen zur **Einrichtung des internen Kontrollsystems beim IT-Outsourcing**, insbesondere

- Kontrollumfeld und
- Organisation,

[1] Vgl. IDW RS FAIT 5, Tz. 1.

[2] http://www.idw.de/idw/portal/d657198

- IT-Infrastruktur,
- IT-Anwendungen,
- IT-gestützte Geschäftsprozesse.

Abschließend behandelt der IDW PS die Themen **Überwachung und Beendigung des IT-Outsourcings**.

1.2 Auslagerung rechnungslegungsrelevanter Dienstleistungen

Die Prüfungspflicht der ausgelagerten Dienstleistungen für die Rechnungslegung als Teil der Abschlussprüfung ist zu bejahen, sofern sie dazu bestimmt sind

- Daten über Geschäftsvorfälle, Ereignisse oder betriebliche Aktivitäten zu speichern oder zu verarbeiten,
- die entweder direkt in die Rechnungslegung einfließen oder dem Rechnungslegungssystem als Grundlage für Buchungen dienen.

1.2.1 Beispiele für ausgelagerte rechnungslegungsrelevante Dienstleistungen

IT-gestützte bzw. manuelle rechnungslegungsrelevante Geschäftsprozesse bei Gewerbetreibenden

- **zur Verarbeitung** von rechnungslegungsrelevanten Geschäftsvorfällen (= externe Buchungssysteme),
- **zur Bereitstellung** rechnungslegungsrelevanter Unterlagen in elektronischer oder anderer Form für den Abschluss des auslagernden Unternehmens (bspw. als Buchungsdaten oder Buchungsbelege) sowie die Bereitstellung ergänzender Informationen (bspw. für die Lageberichterstattung),
- **zur Erfassung und Verarbeitung** von für den Abschluss relevanten Ereignissen, die keine Geschäftsvorfälle sind (bspw. Bestellung von Sicherheiten für fremde Verbindlichkeiten),
- **für den Abschluss- und Lageberichterstellungsprozess** des auslagernden Unternehmens, einschließlich der Verfahren zur Ermittlung geschätzter Werte bzw. Angaben im Anhang bzw. im Lagebericht (= Inventuraufnahme durch Fremdunternehmen),
- **für Kontrolltätigkeiten** im Zusammenhang mit der Aufzeichnung von Geschäftsvorfällen, einschließlich nicht wiederkehrender bzw. ungewöhnlicher Geschäftsvorfälle, oder Kontrolltätigkeiten über Anpassungen im Abschlusserstellungsprozess.

Die Auslagerung von rechnungslegungsrelevanten Dienstleistungen kann je nach Bedarf von der

- **Datenerfassung und**
- **Speicherung bis hin zur**
- **vollständigen Verarbeitung** erfolgen.

Stand: 04.10.2023

Hierbei werden dann auch IT-Systeme des Dienstleisters bereitgestellt:

- **Rechenzentrumsbetrieb**

  Verarbeitung von Daten über Geschäftsvorfälle, die in die IT-gestützten Rechnungslegungssysteme des auslagernden Unternehmens einfließen.
- **Business Process Outsourcing**

  Übernahme administrativer Routinetätigkeiten, bspw. Lohn- und Gehaltsabrechnungen.
- **Shared Service Center**

  Auslagerung von Funktionen, wie bspw. das Rechnungswesen, die Personalverwaltung, IT, Call-Center auf eigenständige Unternehmenseinheiten oder Gesellschaften.
- **Cloud Computing**

  Bereitstellung der Dienstleistung via Internet auf Abruf mit folgenden Besonderheiten gegenüber dem „herkömmlichen" IT-Outsourcing:
- Arbeiten über Browserfunktion
- Nutzung von „öffentlichen" Dienstleistungen und IT-Systemen, die nicht ausschließlich für das auslagernde Unternehmen bereit gestellt werden
- Vertragsbeziehung / Leistungsaustausch oft nur von kurzer Dauer, manchmal nur für einzelne Tage oder Monate
- Nutzung der Dienste von E-Mail-Systeme
- Nutzung von Buchungstools (Hotellerie, Kultureinrichtungen)
- und viele Produkte der Zukunft

Stand: 04.10.2023

1.2.2 Arten des Cloud Computings

Servicemodelle

- **IaaS – Infrastructure as a Service**

  Bei Bedarf wird dem auslagernden Unternehmen eine IT-Infrastruktur zur Verfügung gestellt, bspw. Festplattenkapazität, Netzwerkserverkapazität, Speicherkapazität.
- **PaaS – Platform as a Service**

  Dem auslagernden Unternehmen wird eine Umgebung zum Betrieb eigens entwickelter Software zur Verfügung gestellt, meist inklusive Softwareentwicklungswerkzeug, bspw. zur Entwicklung, zum Test, zum Betrieb von Anwendungen zur Reisekostenabrechnung, zur Fakturierung, zur Rechnungsprüfung.
- **SaaS – Software as a Service**

  Das auslagernde Unternehmen nutzt eine IT-Anwendung aus der Cloud, regelmäßig ohne Einfluss auf deren Ausgestaltung, bspw. Anlagenbuchführung, Verwaltung von Kundenbeziehungen.

Bereitstellungsmodelle

- **Public Cloud**
  Die Nutzung steht allen auslagernden Unternehmen zur Verfügung.
- **Private Cloud**
  Die Nutzung steht einem / dem auslagernden Unternehmen zur Verfügung.
- **Community Cloud**
  Die Nutzung steht einer ausgewählten Interessengruppe zur Verfügung.
- **Hybrid Cloud**
  Ist eine Mischform von zwei unterschiedlichen Bereitstellungsmodellen, die für sich selbständig betrieben werden, aber über eine Schnittstelle miteinander verbunden sind.

1.2.3 Vorgehensweise beim IT-Outsourcing

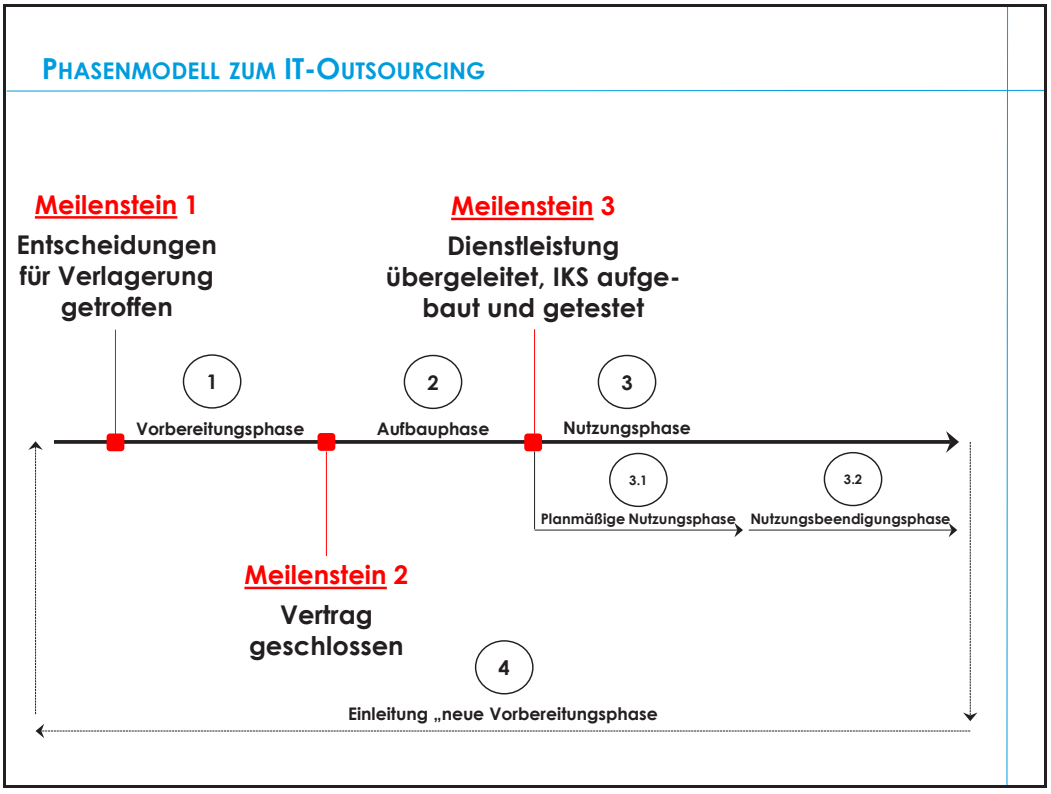

Abbildung 1: Phasenmodell zum IT-Outsourcing

I. Merkmale in der Vorbereitungsphase

1. Festlegung der auszulagernden rechnungslegungsrelevanten Dienstleistungen
2. Festlegung des **Nutzungszeitraums** und der **Nutzungsart**
3. Verhandlungen über **Art**, **Umfang** und **Preis**

Stand: 04.10.2023

II. Merkmale in der Aufbauphase

1. Schaffung der organisatorischen und technischen **Voraussetzungen** für die Erbringung der Dienstleistung
2. Anpassung und Verbindung des rechnungslegungsbezogenen internen Kontrollsystems beim Dienstleistungsunternehmen und beim auslagernden Unternehmen.
3. **Test, Freigabe** und **Dokumentation** zu erbringender Dienstleistungen

III. Merkmale in der planmäßigen Nutzungsphase

1. Beginn mit der **Produktivsetzung**
2. **Überwachung** des eigenen rechnungslegungsbezogenen IKS und des korrespondierenden IKS beim Dienstleistungsunternehmen durch das auslagernde Unternehmen

IV. Merkmale in der Nutzungsbeendigungsphase

1. **Entscheidung** der gesetzlichen Vertreter für die Verlagerung der Dienstleistung auf ein anderes Dienstleistungsunternehmen oder zurück in das eigene Unternehmen ist getroffen
2. Schaffung der Voraussetzungen für eine **kontinuierliche Aufrechterhaltung** der Sicherheit und Ordnungsmäßigkeit der Rechnungslegung auch nach der Trennung vom bisherigen Dienstleister
3. Beginn einer **neuen Vorbereitungsphase**

1.3 Sicherheit beim IT-Outsourcing

Auch beim IT-Outsourcing sind die gesetzlichen Anforderungen und die Grundsätze ordnungsmäßiger Buchführung zu beachten.[3]

Daneben sind die im IDW RS FAIT 1 behandelten Sicherheits- und Ordnungsmäßigkeitsanforderungen, sowohl während der planmäßigen Nutzungsphase als auch während der Nutzungsbeendigungsphase, zu beachten, insbesondere im Zusammenhang mit dem Dienstleistungsunternehmen und gegebenenfalls mit Subdienstleistern:

> *„Voraussetzung für die Ordnungsmäßigkeit der IT-gestützten Rechnungslegung ist neben der Gesetzesentsprechung des Rechnungslegungssystems die Sicherheit der verarbeiteten rechnungslegungsrelevanten Daten."*[4]

[3] § 239 Abs. 4 HGB: „Die Handelsbücher und die sonst erforderlichen Aufzeichnungen können auch in der geordneten Ablage von Belegen bestehen oder auf Datenträgern geführt werden, soweit diese Formen der Buchführung einschließlich des dabei angewandten Verfahrens den Grundsätzen ordnungsmäßiger Buchführung entsprechen. Bei der Führung der Handelsbücher und der sonst erforderlichen Aufzeichnungen auf Datenträgern muss insbesondere sichergestellt sein, dass die Daten während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können. Absätze 1 bis 3 gelten sinngemäß."

[4] IDW RS FAIT 1, Tz. 19

Stand: 04.10.2023

Gemäß IDW RS FAIT 1, Tz. 23 haben IT-Systeme folgende **Sicherheitsanforderungen** zu erfüllen:

- **Vertraulichkeit**

  Von Dritten erlangte Daten dürfen nicht unberechtigt weitergegeben werden, bspw. durch **Verschlüsselungstechniken**, eindeutige Verifizierung des „berechtigten" Empfängers.

- **Integrität**

  Daten, IT-Infrastruktur und IT-Anwendungen müssen vollständig und richtig zur Verfügung stehen und vor **Manipulation** oder ungewollten oder fehlerhaften Änderungen **geschützt** werden, bspw. durch Test- und Freigabeverfahren.

- **Verfügbarkeit**

  Gewährleistung der **ständigen Verfügbarkeit** der IT-Infrastruktur, der IT-Anwendungen und Daten, bspw. **Back-Up-Verfahren** zur Notfallvorsorge.

- **Autorisierung**

  Zugriff und **Ausübung von Rechten** (lesen, ändern, löschen) nur durch im Voraus festgelegte autorisierte Personen, bspw. durch Zugriffsschutzmaßnahmen – Passwortschutz.

- **Authentizität**

  Zuordnung des Geschäftsvorfalls zu einem Verursacher, bspw. durch **Berechtigungsverfahren** oder Identifizierung durch digitale Signatur- oder passwortgestützte Identifikationsverfahren.

- **Verbindlichkeit**

  Gewollte Rechtsfolgen sollen verbindlich herbeigeführt werden, bspw. einzelne Transaktionen sind **bis zum Verursacher nachvollziehbar** und transparent.

Daneben haben IT-Systeme gemäß IDW RS FAIT 1, Tz. 25 ff. folgende **Ordnungsmäßigkeitskriterien** zu erfüllen:

- **Vollständigkeit**

  Lückenlose Erfassung aller rechnungslegungsrelevanten Geschäftsvorfälle und Ausschluss der Mehrfacherfassung.

- **Richtigkeit**

  Inhaltlich **zutreffende Abbildung** des Geschäftsvorfalles – in Übereinstimmung mit den tatsächlichen Verhältnissen und im Einklang mit den rechtlichen Vorschriften.

- **Zeitgerechtheit**

  Zuordnung der einzelnen **Geschäftsvorfälle** zu Buchungsperioden und zeitnahe Erfassung zur Entstehung des Geschäftsvorfalles.

Stand: 04.10.2023

- **Ordnung**

  Das Buchführungssystem muss die Geschäftsvorfälle sowohl in **zeitlicher als auch in sachlicher Abfolge** darstellen können – Journal- und Kontenfunktion.

- **Nachvollziehbarkeit**

  Ein sachverständiger Dritter muss in der Lage sein, sich in angemessener Zeit einen **Überblick** über die Geschäftsvorfälle und die Lage des Unternehmens zu verschaffen.

- **Unveränderlichkeit**

  Eintragungen und Aufzeichnungen dürfen **nicht** in der Form **verändert** werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. Spätere Eintragungen müssen dieses Kriterium erfüllen und dabei deutlich die Änderung kennzeichnen – auch in zeitlicher Hinsicht, Datumsangabe.

1.4 Risiken beim IT-Outsourcing

1.4.1 Sicherheitsrisiken

- **Organisation und Aufgabenteilung**

  Durch das Zusammenspiel der Funktionen des auslagernden Unternehmens und des Dienstleistungsunternehmens entstehen veränderte Zuständigkeiten und Arbeitsteilungen.

- Hierbei bestehen **Risiken** im Bereich der Autorisierung – Zugriff und Ausübung von Rechten.

- **Schnittstellen und genutzter Übertragungsweg**

  Zum Transfer der Daten aus dem Unternehmen oder in das Unternehmen sind Schnittstellen erforderlich.

- Hierbei besteht **Risiken** hinsichtlich der Integrität und Verfügbarkeit – Schutz vor Manipulation und ständige Verfügbarkeit der Daten und Systeme.

- **Datenspeicherung und Speicherort**

  Beim Outsourcing via Cloud Computing sind die Anwendungen und Daten auf einem „fremden“ Server abgelegt. Der Zugriff erfolgt in der Regel via Internetbrowser – Online Anwendung.

- In diesem Fall bestehen die **Risiken** hinsichtlich Integrität, Autorisierung, Authentizität aufgrund von Sicherheitslücken beim Dienstleistungsunternehmen, bspw. unberechtigter Zugriff eines anderen Cloud-Nutzers auf die Rechteverwaltung und die Daten des auslagernden Unternehmens.

- **Change Management**

  Die Verwaltung und Pflege des Angebots liegt regelmäßig in der Verantwortung des Dienstleistungsunternehmens.

Stand: 04.10.2023

- Es besteht das **Risiko** der Verfügbarkeit und der Integrität, bspw. sofern Dienstleistungsunternehmen Änderungen an den angebotenen Programmen, der Hardware oder dem Speicherort der Daten, ohne vorherigen Information bzw. Absprache mit dem auslagernden Unternehmen, vornehmen.

1.4.2 Risiken der Ordnungsmäßigkeit

Aufgrund der Besonderheit, dass beim IT-Outsourcing und insbesondere beim Cloud Computing die Daten, Anwendungen und Systeme außerhalb des auslagernden Unternehmens verwaltet werden, bestehen **folgende Risiken der Ordnungsmäßigkeit:**

- Nichteinhaltung der **steuerrechtlichen Vorschriften** zu Verarbeitung, Zugriff und Aufbewahrung - §§ 145 ff. AO und GoBD,
- **Unvollständige oder verspätete Verarbeitung** von Geschäftsvorfällen und Daten,
- Missachtung der **Sicherheits- und Ordnungsvorschriften** - §§ 238 ff HGB - von Subdienstleitern im Rahmen des Cloud Computing, bspw. Speicherung von Daten und Anwendungen auf Servern in Drittländern,
- Fehlerhafte oder unvollständige **Übertragung** der Daten zwischen dem auslagernden Unternehmen und dem Dienstleistungsunternehmen,
- Das **Buchführungsverfahren** erfüllt nicht die Voraussetzungen der Beleg-, Journal- und Kontenfunktion,
- Risiko hinsichtlich der Nichterfüllung von **Aufbewahrungspflichten** gemäß § 257 HGB aufgrund Kontrollverlust hinsichtlich der ausgelagerten Daten.

1.4.3 Rechtliche Risiken

Die rechtlichen Risiken stehen nicht in Zusammenhang mit den Anforderungen der §§ 238 ff HGB oder des IDW RS FAIT 1.

Sie können bspw. aufgrund der Anforderungen zum **Schutz von personenbezogenen Daten oder Urheberrechten** entstehen.

Eine rechtliche Grundlage ist dabei bspw. das **Bundesdatenschutzgesetz** mit seinen Sicherungsmaßnahmen zum Schutz vor unbefugten Abfragen von Daten aller Art.

Daneben bestehen **Risiken aufgrund des grenzüberschreitenden Dienstleistungsaustauschs** – Datenspeicherung und Nutzung.

Risikobereiche sind hierbei:

- Auswirkungen strafrechtlicher **Ermittlungen gegen das Dienstleistungsunternehmen** oder deren Kunden auf die Vertraulichkeit von Anwendungs- oder Nutzerdaten,

Stand: 04.10.2023

- Das Bestehen **unterschiedlicher Anforderungen** hinsichtlich der **Speicherung, Aufbewahrung und Löschung** personenbezogener Daten – insbesondere beim Dienstleistungsaustausch mit so genannten Drittländern gelten einschränkende Regelungen des Bundesdatenschutzgesetzes,
- **Aufbewahrungspflicht steuerrelevanter Daten** im Inland oder innerhalb der EU bzw. EWR - § 146 ff. AO[5]

1.5 Verantwortung der gesetzlichen Vertreter beim IT-Outsourcing – Leitfaden für die Einführung

Bei Auslagerung von betrieblichen Funktionen an andere Dienstleistungsunternehmen **verbleibt die Verantwortung** für die Einhaltung der gesetzlichen Anforderungen an die Ordnungsmäßigkeit der Rechnungslegung bei den gesetzlichen Vertretern des auslagernden Unternehmens.

Hier ist die Beratung des Steuerberaters / Wirtschaftsprüfers unabdingbar (**= Beratungsfeld**).

1.5.1 Vorbereitungsphase

Neben den Chancen, die dieses Modell bereithält, sind auch die Risiken für das auslagernde Unternehmen zu beachten sowie deren Auswirkungen auf das interne Kontrollsystem.[6]

Die Risiken sind zu analysieren, zu strukturieren. Daneben sind deren **Auswirkungen auf das interne Kontrollsystem** zu ermitteln. Das interne Kontrollsystem muss angemessen ausgestaltet und wirksam sein – **Erweiterung des IKS um Grundsätze, Verfahren und Maßnahmen zur Steuerung des IT-Outsourcings und zur Überwachung der Einhaltung dieser Regelungen**.

Von der Entscheidung zur Auslagerung rechnungslegungsrelevanter Dienstleistung bis zu deren Beendigung ist das IT-Outsourcing zu steuern und zu überwachen – **Dienstleistermanagement.**

Stand: 04.10.2023

[5] Vgl. IDW RS FAIT 5, Tz. 44.

[6] Vgl. IDW RS FAIT 5, Tz. 1.

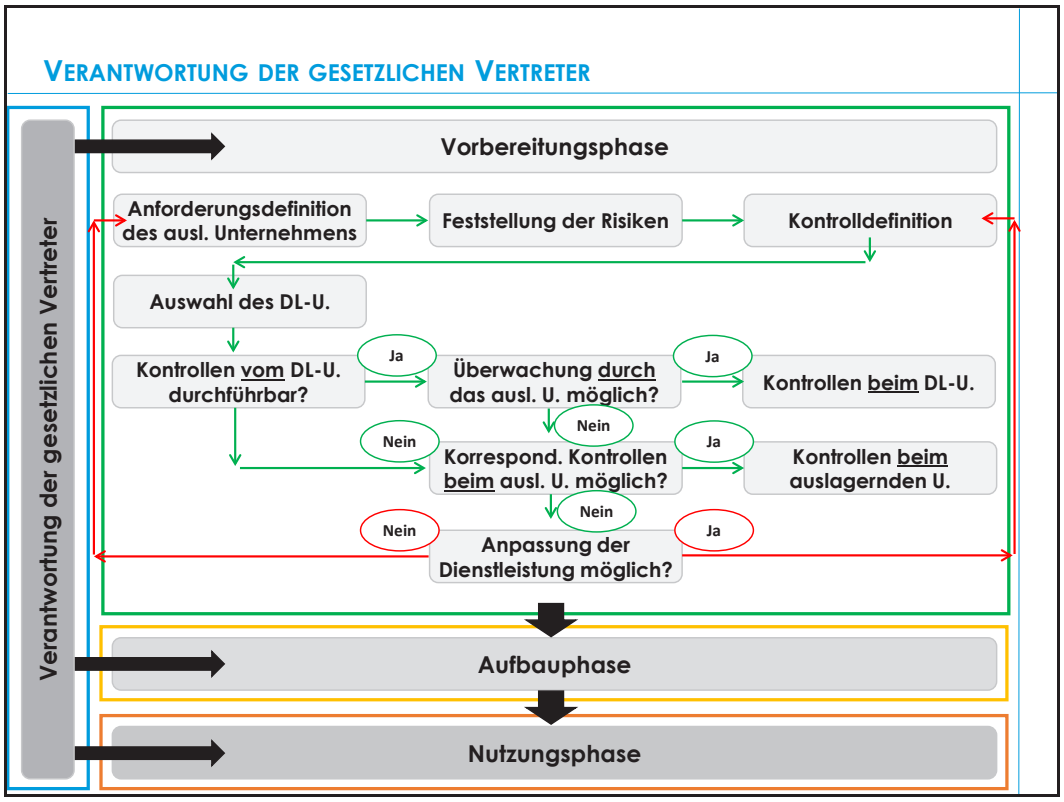

Abbildung 2: Verantwortung der gesetzlichen Vertreter[7]

1.5.2 Aufbauphase

An die Vorbereitungsphase schließen sich die Vertragsverhandlungen an. Hierbei ist darauf zu achten, dass insbesondere die Einhaltung der erforderlichen Kontrollen und Maßnahmen mit dem Dienstleistungsunternehmen vereinbart werden, die sich aus IDW RS FAIT 1 ergeben – Sicherheits-, Ordnungsmäßigkeits-, und Kontrollanforderungen.

Wichtige Vertragsinhalte:

- Verantwortlichkeiten zur **Aufbewahrung und Aushändigung** von Unterlagen, Dokumentationen und Daten,
- **Prüfungsrechte** der internen Revision und des Abschlussprüfers des auslagernden Unternehmens in Bezug auf das eingerichtete interne Kontrollsystem beim Dienstleister bzw. Subdienstleister,
- Vereinbarung, dass die **gesetzlichen Anforderungen eingehalten** und die Kontrollen dokumentiert werden, so dass sie von einem unabhängigen Prüfer nachvollzogen werden können,
- **Unterrichtung des auslagernden Unternehmens** zu Veränderungen in den Bereichen IT-Infrastruktur, IT-Anwendungen, IT-gestützte Geschäftsprozesse, die für die Sicherheit und Ordnungsmäßigkeit relevant sind,

[7] IDW RS FAIT 5, Tz. 51.

Stand: 04.10.2023

- **Ort der Verarbeitung und Speicherung** von Daten des auslagernden Unternehmens
- Beendigung der vertraglichen Beziehung und **nachvertragliche Pflichten**, bspw. Datenrückgabe.[8]

Wird vereinbart, dass einzelne **Kontrollen vom Dienstleistungsunternehmen** eingerichtet und durchgeführt werden, muss sich das auslagernde Unternehmen von deren Angemessenheit überzeugen.[9]

Sofern einzelne Bestandteile nicht mit dem Dienstleistungsunternehmen vereinbart werden können, muss das auslagernde Unternehmen für diese Fälle ausgleichende Kontrollen einrichten oder nach einem anderen Dienstleister Ausschau halten – Dienstleistermanagement.

1.5.3 Nutzungsphase

Im Rahmen der Nutzungsphase haben die **gesetzlichen Vertreter** sicherzustellen, dass das auslagernde Unternehmen in der **Release- und Änderungsplanung** und in das Test- und Freigabeverfahren tatsächlich einbezogen werden – Festlegung von Regelungen für

- Testdurchführung,
- Testdokumentation,
- Testfreigabe,
- Testarchivierung.

Beim Einsatz von Datenverschlüsselungstechniken ist eine verlässliche Schlüsselverwaltung zu realisieren - Dienstleistermanagement zur Sicherstellung von Aktualität und Angemessenheit.

Bei Beendigung der Nutzungsphase haben die gesetzlichen Vertreter sicherzustellen, dass die ausgelagerte Dienstleistung entweder selbst weitergeführt werden kann oder auf ein anderes Dienstleistungsunternehmen übertragen werden kann.

1.6 Praktische Aspekte zur Einrichtung des internen Kontrollsystems beim IT-Outsourcing

1.6.1 Umfeld und Organisation

a. Wirksamkeit

Die **Wirksamkeit** eines internen Kontrollsystems hängt entscheidend davon ab, ob ein **geeignetes Kontrollumfeld** und das **Bewusstsein** der gesetzlichen Vertreter und der Mitarbeiter hinsichtlich der möglichen Risiken im Zusammenhang mit IT-Outsourcing geschaffen werden kann.

---

[8] IDW RS FAIT 5, Tz. 53.

[9] IDW RS FAIT 5, Tz. 56.

Stand: 04.10.2023

Das einmal eingerichtete interne IT-Kontrollsystem ist fortlaufend auf **Aktualität und Angemessenheit** zu überprüfen. Bei Inanspruchnahme von **Cloud Computing** ist das zugehörige Sicherheitskonzept um nachfolgend genannte Inhalte zu erweitern:

- Definition und Klassifizierung der Daten, die mit Hilfe von Cloud Computing verarbeitet werden dürfen,
- Verschlüsselungstechnik zur Übertragung und Speicherung der Daten.

Die ausgelagerten Dienstleistungen sind mit den Geschäftsprozessen des auslagernden Unternehmens ordnungsgemäß und organisatorisch abzustimmen und zu verbinden.[10]

b. Aufbau- und Ablauforganisation

Verantwortlichkeiten und Kompetenzen des Dienstleistungsunternehmens, zur Einhaltung der für das auslagernde Unternehmen geltenden gesetzlichen Anforderungen, sind in diesem Schritt festzuhalten – sogenannte Service Level Agreements mit Angaben zu

- **Verfügbarkeiten,**
- **Reaktionszeiten,**
- **Qualitätsniveaus**.

Auf der Basis messbarer Größen, kann die Beurteilung der Wirksamkeit der **Kontrollen** beim Dienstleistungsunternehmen vorgenommen werden.

Zu den **Beurteilungsgrundlagen** zählen unter anderem

- Messgrößen und -verfahren,
- Berichterstattungen und
- Auswertungen

des Dienstleistungsunternehmens gemäß der vereinbarten Service Level Agreements.

Sofern beim Dienstleistungsunternehmen **Mängel** festgestellt werden, stellen sich folgende Fragen:

- Sind **kompensierende Kontrollmaßnahmen** des auslagernden oder des Dienstleitungsunternehmens vorzunehmen?
- Welche **kompensierenden Kontrollmaßnahmen** des auslagernden oder des Dienstleitungsunternehmens sind vorzunehmen?

Stand: 04.10.2023

[10] Vgl. IDW RS FAIT 5, Tz. 68.

c. Change Management

Originäre Aufgaben im Rahmen des **Change Managements** sind bspw.:

- Wartungsarbeiten – Patch-Management,
- Überwachung von administrativen Tätigkeiten des Dienstleistungsunternehmens und der Änderung von Kontrollen in Geschäftsprozessen.

Das **Dienstleistermanagement** des auslagernden Unternehmens hat dabei auch folgende Aufgaben wahr zu nehmen:

- Koordination der Dienstleistungsänderungen,
- Beurteilung der potenziellen Auswirkungen auf das interne Kontrollsystem,
- Beurteilung der Angemessenheit und Wirksamkeit des internen Kontrollsystems,
- Anpassung des internen Kontrollsystems,
- Prüfung, ob die Compliance- und Sicherheitsanforderungen eingehalten werden.[11]

d. Dokumentation

Die Dokumentation erfolgt in der Regel durch den Einsatz von Betriebshandbüchern mit den Inhalten:

- Aufbau- und Ablauf der Unternehmensprozesse,
- Organisatorische und technische Schnittstellen,
- Kontrollen und organisatorische Sicherungsmaßnahmen,
- Eskalationsverfahren in Zusammenarbeit mit den Dienstleistungsunternehmen bei eingeschränkter Verfügbarkeit,
- Dokumentation des internen Kontrollsystems.

1.6.2 IT-Infrastruktur

Die Bestandteile der IT-Infrastruktur bilden die Basis für die Erbringung von IT-Leistungen:

- Rechenzentren,
- Hardware,
- Netzwerke,
- Systemsoftware,
- und auch Komponenten zur Verbindung der IT des auslagernden Unternehmens mit der IT des Dienstleistungsunternehmens.[12]

IT-Leistungen werden grundsätzlich im Regelbetrieb und ausnahmsweise im Notfallbetrieb erbracht.

---

[11] Vgl. IDW RS FAIT 5, Tz. 72.

[12] Vgl. IDW RS FAIT 5, Tz. 77.

Im Rahmen des IT-Outsourcing hat das auslagernde Unternehmen sicher zu stellen, dass

- die Verfahren des Regel- und des Notfallbetriebs vollständig, nachvollziehbar und lückenlos, insbesondere hinsichtlich Schnittstellen zum Dienstleister, dokumentiert sind und in der beschrieben Form auch tatsächlich durchgeführt werden.[13]

Vorgehensweise beim auslagernden Unternehmen

- Verschaffung eines Überblicks in Bezug auf die IT-Infrastruktur, die Schutzmaßnahmen, die Sicherheitsvorkehrungen und die IT-Prozesse beim Dienstleistungsunternehmen,
- Abstimmung von Maßnahmen für den Notfall und regelmäßig Prüfung durch Tests,
- Sofern die Verwaltung der IT-Infrastruktur beim Dienstleistungsunternehmen erfolgt, ist die Angemessenheit und Funktionsfähigkeit der beim Dienstleistungsunternehmen eingerichteten Kontrollen regelmäßig zu überprüfen,
- Richtlinien und Verfahrensanweisungen zum Zugriffsschutz und zur Datenverschlüsselungstechnik,
- Regeln zu Änderungen an der IT-Infrastruktur (Change Management: Plan, Test, Implementierung, Dokumentation).[14]

1.6.3 IT-Anwendungen

Bei der Auslagerung einzelner rechnungslegungsrelevanter Funktionen auf Dienstleistungsunternehmen müssen, wie beim Eigenbetrieb, die Anforderungen der Sicherheit und Ordnungsmäßigkeit sowie des rechtlichen Umfeldes beachtet und durch laufende Kontrollen sichergestellt werden.

a. Individualsoftware

Beim Einsatz von Individualsoftware ist mit dem Dienstleistungsunternehmen eine Regelung zum **Softwareentwicklungsverfahren** mit folgenden Inhalten zu vereinbaren:

- **Eingabe-, Verarbeitungs- und Ausgabekontrollen** gemäß Vorgaben des auslagernden Unternehmens,
- **Angemessenes Projektmanagement** in Abhängigkeit der Projektgröße,
- **Einhaltung der von den gesetzlichen Vertreter** des auslagernden Unternehmens geforderten Richtlinien zum Qualitätsmanagement,
- angemessene Unterstützung für Design, Realisierung, Test, Freigabe,
- angemessenes **Change Management**.[15]

[13] Vgl. IDW RS FAIT 5, Tz. 78.

[14] Vgl. IDW RS FAIT 5, Tz. 79 ff.

Stand: 04.10.2023

b. Standardsoftware

Beim Customizing von Standardsoftware ist ein **Change Management Prozess** zu designen. Hiermit wird sichergestellt, dass nur die vom auslagernden Unternehmen gewünschten und freigegebenen Änderungen vorgenommen und in den Produktivbetrieb übernommen werden.[16]

c. Anwendungsbezogene Kontrollen

- **Integrationstests zur Feststellung**, ob die Übertragung der Daten und Dokumente zwischen Prozessen und IT-Systemen des auslagernden Unternehmens und dem ausgelagerten IT-System vollständig und richtig erfolgt,
- Einrichtung und Aufrechterhaltung eines **angemessenen Berechtigungssystems** für den Zugriff auf die ausgelagerte IT-Anwendung sowie die zugehörigen Daten,
- systematische Auswertung anwendungsbezogener **Verarbeitungsprotokolle** auf unerwartete Ereignisse, bspw. Datenbankfehler,
- **Anwendungs- und schnittstellenbezogene Kontrollen** zur Sicherstellung, dass die ausgetauschten Daten richtig, vollständig und zeitnah verarbeitet werden, bspw. durch Kontrollsummen hinsichtlich Anzahl der Buchungen.[17]

d. Überwachende Kontrollen

- Durchsicht von **Änderungsnachweisen**,
- Abgleich der an das Dienstleistungsunternehmen übermittelten und vom Dienstleistungsunternehmen erhaltenen Daten.[18]

e. Generelle Kontrollen

- Nachweise über **kritische Systemberechtigungen** und deren Nutzung,
- **Protokolle** über nicht erfolgreiche Systemzugriffe, bspw. mehrmalige Falscheingabe eines Passworts,
- Protokolle über unerwartete Ereignisse, bspw. **Systemabstürze und -neustarts**,
- Nachweise über Systemänderungen, bspw. **Softwareupdate** oder -release,
- Nachweise über Tests des Dienstleistungsunternehmens,
- Berichte der internen Revision des Dienstleistungsunternehmens.[19]

---

[15] Vgl. IDW RS FAIT 5, Tz. 92.
[16] Vgl. IDW RS FAIT 5, Tz. 93.
[17] Vgl. IDW RS FAIT 5, Tz. 94.
[18] Vgl. IDW RS FAIT 5, Tz. 96.
[19] Vgl. IDW RS FAIT 5, Tz. 97.

1.6.4 IT-gestützte Geschäftsprozesse

Bei der Auslagerung von IT-gestützten Geschäftsprozessen erfolgt die Verarbeitung sowie die Bereitstellung der rechnungslegungsrelevanten Daten in der Regel durch das Dienstleistungsunternehmen. Anschließend werden die bereitgestellten Daten in die Rechnungslegung des auslagernden Unternehmens übernommen.

Zur Einhaltung der Vorgaben zur Sicherheit, Ordnungsmäßigkeit und Kontrolle in Bezug auf die ausgelagerten Geschäftsprozesse sind mit dem Dienstleistungsunternehmen **Regelungen** zu treffen.

Die **Dokumentation** der Regelungen erfolgt In Betriebshandbücher oder mit Hilfe von Service Level Agreements – Inhalte:

- **anwendungsorientierte und prozessintegrierte Kontrollen** bei der Erfassung und Verarbeitung von Geschäftsvorfällen beim Dienstleistungsunternehmen, bspw. Plausibilitätskontrollen, sachliche und rechnerische Belegprüfung, Abstimmverfahren zwischen Teilprozessen,
- Übertragungsweg und Format der rechnungslegungsrelevanten Daten bei der Übertragung vom auslagernden Unternehmen an das Dienstleistungsunternehmen,
- Übertragungsweg und Format der rechnungslegungsrelevanten Daten bei der Übertragung vom Dienstleistungsunternehmen an das auslagernde Unternehmen.[20]

a. Schnittstellenkontrollen

Sowohl beim auslagernden Unternehmen als auch beim Dienstleistungsunternehmen sind **Schnittstellenkontrollen** durchzuführen, bspw.

- **Abstimmung Anzahl der übergebenen und übernommenen Datensätze,**
- **Plausibilitätskontrolle von übertragenen Stammdaten.**

b. Teilprozesse

Bei der Auslagerung von Teilprozessen ist darauf zu achten, dass die Sicherheit und Ordnungsmäßigkeit der rechnungslegungsrelevanten Daten über den gesamten IT-gestützten Geschäftsprozess gewährleistet ist.[21]

c. Cloud Computing

Beim Cloud Computing sind die Kontroll- und Abstimmverfahren des Dienstleistungsunternehmens in der Regel vorgegeben.

Stand: 04.10.2023

[20] Vgl. IDW RS FAIT 5, Tz. 106.

[21] Vgl. IDW RS FAIT 5, Tz. 108.

Dies bedeutet, dass die Dienstleistungsunternehmen kaum individuelle Anpassungen auf Wunsch des auslagernden Unternehmens umsetzen werden.

In diesem Fall ist entweder der IT-gestützte Geschäftsprozess beim auslagernden Unternehmen an die vorgegebenen Kontroll- und Abstimmverfahren des Dienstleistungsunternehmens anzupassen oder es sind zusätzliche Kontrollen beim auslagernden Unternehmen einzurichten.[22]

1.6.5 Beispiel: Verwaltung der IT-Infrastruktur und der IT-Anwendungen durch das Dienstleistungsunternehmen

Erfolgt die Verwaltung bzw. Administration der IT-Infrastruktur und der IT-Anwendungen durch das Dienstleistungsunternehmen, muss sich das auslagernde Unternehmen davon überzeugen, dass

- die physischen Sicherungsmaßnahmen zum Schutz der IT- Infrastruktur beim Dienstleistungsunternehmen wirksam sind.

Daneben sind Zugriffe von Administratoren und anderen privilegierten Nutzern zu kontrollieren.

a. Folgende Nachweise bieten sich hierzu an:

1. Aufzeichnungen und Auswertungen des Dienstleistungsunternehmens an, aus denen sich die Kontrollen und deren Wirksamkeit ersehen lassen,
2. aktuelle Berichterstattung gemäß IDW PS 951 n.F.,
3. aktuelle Berichte der internen Revision des Dienstleistungsunternehmens.

b. Folgende Handlungen zur Beurteilung der Wirksamkeit der Kontrolldurchführung beim Dienstleistungsunternehmen bieten sich an:

1. Auswertung der Verarbeitungsergebnisse des Dienstleistungsunternehmens mit Hilfe eigener Datenanalysen,
2. Nachvollziehung der Verarbeitungsergebnisse mit Hilfe von stichprobenartigen Berechnungen,
3. Auswertung von vom Dienstleistungsunternehmen erhaltenen Unterlagen, bspw. Verfahrensdokumentation und Kontrollen betreffend IT-Prozesse.[23]

1.7 Überwachung des IT-Outsourcings

a. Maßnahmen zur prozessunabhängigen Überwachung

- Regelmäßige Beurteilung, ob die **Leistungserbringung** des Dienstleistungsunternehmens **überwacht** wird,

[22] Vgl. IDW RS FAIT 5, Tz. 109.

[23] Vgl. IDW RS FAIT 5, Tz. 76.

- Regelmäßige Beurteilung, ob **Abweichungsanalysen** zur Feststellung des Zielerreichungsgrades der umgesetzten IT-Strategie durchgeführt werden.

b. Vertraglich vereinbarte Prüfrechte

Sofern Prüfrechte vertraglich vereinbart wurden, kann das auslagernde Unternehmen **eigene Prüfungshandlungen** beim Dienstleistungsunternehmen durchführen:

- Feststellungen zur Wirksamkeit der Kontrollen,
- Feststellungen zur Vollständigkeit und Richtigkeit der regelmäßigen Auswertungen und Berichterstattungen des Dienstleistungsunternehmens.

Neben der Durchführung von eigenen Prüfungshandlungen kann das auslagernde Unternehmen auch auf **Unterlagen des Dienstleistungsunternehmens** zugreifen:

- Berichte der internen Revision des Dienstleistungsunternehmens zur Einhaltung der zugesicherten Eigenschaften der Dienstleistung.

Des Weiteren kann das auslagernde Unternehmen **Prüfungen durch unabhängige Dritte** beim Dienstleistungsunternehmen durchführen lassen:

- Reports oder Berichte zur Einhaltung der zugesicherten Eigenschaften der Dienstleistung,
- Berichterstattungen gemäß IDW PS 951 n.F.

1.8 Risikobegrenzung bei der Beendigung des IT-Outsourcings

Bereits vor Beendigung des IT-Outsourcings ist zu prüfen, ob sich die einst festgelegten Verfahren zur Rückführung auf das auslagernde Unternehmen oder zum Übertrag auf einen anderen Dienstleister aktuell noch anwendbar und sachgerecht sind – gegebenenfalls sind Anpassungen zu vereinbaren.

Erarbeitung eines **Konzepts zur Daten- und Dienstleistungsmigration** – durch das auslagernde Unternehmen, das bisherige und eventuell das neue Dienstleistungsunternehmen – mit Regelungen zu folgenden Sachverhalten:

- **Art und Umfang** der überzuleitenden Dienstleistung,
- Art, Umfang und **Struktur der überzuleitenden Produktivdaten**,
- Umgang mit **archivierten Daten** und Dokumenten,
- **Zuverlässige Löschung** der Daten beim bisherigen Dienstleistungsunternehmen,
- **Rückgabe von Datensicherungen** in einem definierten Format,
- Umfang eines eventuellen **Parallelbetriebs**,
- **Test- und Freigabeverfahren**.

Stand: 04.10.2023