▶ **IT-Revision**

# Auslagerung IT-Revision – (un)wesentlich?

Vor dem Hintergrund der steigenden Bedeutung von IT ist auch die „third line of defense", die IT-Revision, heutzutage besonders gefordert. Eine Auslagerung ist oft ein sehr guter Weg. Dabei stellt sich die Frage: Ist die Auslagerung der IT-Revision eigentlich als wesentlich oder unwesentlich zu betrachten?

Ihren Ursprung hat die IT-Revision in der Betriebswirtschaft bzw. dem Prüfungswesen. Durch die gestiegenen Anforderungen ist die IT-Revision ein spezieller Bestandteil der Internen Revision geworden. Allerdings setzt eine effektive IT-Revision interdisziplinäres Fachwissen voraus und damit kosten- und zeitintensive Seminare, um die zunehmende Komplexität der Prüfungsfelder bewältigen zu können.

Die IT-Revision muss in ihrer Rolle als dritte Verteidigungslinie unabhängig von den operativ Verantwortlichen oder den Beauftragtenfunktionen prüfen, dass alle IT-bezogenen normativen Bestimmungen eingehalten werden. IT-Revision setzt somit einen Schlusspunkt in der Schadensabwehr im Bereich der IT. Dazu gehören u. a.

- die Prüfung der Einhaltung unternehmensexterner und -interner Regelungen in der und für die IT – und somit der Schutz vor unsachgemäßem IT-Gebrauch (Datenverlust, Datendiebstahl etc.),
- die Prüfung auf Einhaltung der Regelungen des Datenschutzes,
- die Prüfung des Schutzes und der Sicherheit aller Informationssysteme, insbesondere der rechnungslegungsrelevanten IT-Systeme und Anwendungen – und damit die Identifizierung und Minimierung von Risiken und Ineffizienzen der IT-Infrastruktur sowie
- die Erstellung von Handlungsempfehlungen für das Management unter Berücksichtigung von Risikobewertungen und Schwachstellenanalysen.

Aufgrund der immer höheren Komplexitäten dieser Aufgaben bedienen sich viele Häuser mittlerweile der Expertise externer Fachleute. So ist z. B. das Angebot der DZ CompliancePartner GmbH zur Auslagerung der IT-Revision ein probates Mittel.

## Auslagerung der IT-Revision

Für die Auslagerung gelten die Vorgaben der §§ 25a, 25b Kreditwesengesetz (KWG) sowie der AT 9 der Mindestanforderungen an das Risikomanagement (MaRisk). Für wesentliche – künftig wohl gemäß EBA-Guideline „kritische" oder „wichtige" – Auslagerungen gelten darüber hinaus noch besondere Anforderungen an die Vertragsgestaltung, die Beendigung des Auslagerungsverhältnisses sowie die Steuerung und Überwachung. Ergänzend dazu sind noch die Bankaufsichtlichen Anforderungen an die IT (BAIT) zu beachten.

Die Gesamtverantwortung für eine bereits durchgeführte bzw. geplante Auslagerung obliegt nach AT 3 Tz. 1 MaRisk der gesamten Geschäftsleitung und besteht in der Erstellung und Umsetzung eines angemessenen und wirksamen Risikomanagements im Sinne des § 25a Abs. 1 KWG.

Die Geschäftsleitung benötigt zur Steuerung und Überwachung der mit der Auslagerung verbundenen Risiken einen Gesamtüberblick über die ausgelagerten Aktivitäten und Prozesse. Dazu wird künftig ein zentrales Register vorzuhalten sein, wobei z. B. das Tool „Auslagerungsmanagement kompakt" der DZ CompliancePartner eine gute Unterstützung darstellt.

Eine Auslagerung darf nicht dazu führen, dass die Ordnungsmäßigkeit des Geschäftsbetriebes, die Steuerungs- und Kontrollmöglichkeiten der Geschäftsleitung oder gar die Prüfungsrechte und Kontrollmöglichkeiten der Finanzaufsicht eingeschränkt werden. Die Auslagerung von Funktionen wie z. B. des Risikocontrollings, der Compliance-Funktion nach WpHG oder MaRisk oder der Internen Revision (= besondere Funktionen) ist grundsätzlich unter Beachtung der Voraussetzungen des AT 9 Tz. 5 MaRisk erlaubt.

Die IT-Revision ist eine spezielle Kategorie im Rahmen der Internen Revision und kann somit als Teilkontrollfunktion der Internen Revision gemäß den MaRisk unter Berücksichtigung einer MaRisk-konformen Vertragsgestaltung sowie einer angemessenen Überwachung der Leistungserstellung ausgelagert werden.

## Risikoanalyse zur Auslagerung

Eine Antwort auf die Frage, ob die Auslagerung der IT-Revision wesentlich oder unwesentlich ist, liefern die MaRisk jedoch nicht. Sie überlassen die Bewertung der Risiken für den Geschäftsbetrieb und damit die Einwertung der Auslagerung den Häusern selbst.

Die Art der Auslagerung – wesentlich oder unwesentlich – wird somit

- auf Grundlage einer Risikoanalyse nach AT 9 Tz. 2 MaRisk,
- im Vorfeld der Auslagerung und
- unter Beachtung der individuellen Situation, d. h., welche Risiken mit der geplanten Maßnahme überhaupt verbunden sind, entschieden.

Die Ausprägung, Tiefe oder Methodik der Risikoanalyse liegen dabei im Ermessen des jeweiligen Instituts und sollen eine Beurteilungsgrundlage schaffen, welches Risikopotenzial im Sinne der MaRisk von einer Auslagerung ausgeht, und ob sie demzufolge insgesamt als wesentlich oder als nicht wesentlich zu bewerten ist.

Die MaRisk verzichten auf detaillierte Vorgaben zu notwendigen Inhalten der Risikoanalyse. Das Institut führt diese eigenverantwortlich unter Risikogesichtspunkten aus und wiederholt diese regelmäßig, falls es zu der Auslagerung gekommen ist. Dabei sind zudem die maßgeblichen Organisationseinheiten sowie im Rahmen ihrer Aufgaben auch die Interne Revision bei der Erstellung mit einzubeziehen (vgl. AT 9 Tz. 2 MaRisk).

Bei der Risikoanalyse können unterschiedlichste Aspekte eine Rolle spielen: der konkrete Gegenstand der Auslagerung, welche Auswirkungen die Maßnahme auf das Institut hat, der Ort der Leistungserbringung, die Komplexität der geplanten Maßnahme, die Eignung potenzieller Dienstleister etc. Die Intensität der Analyse hängt somit von Art, Umfang, Komplexität und Risikogehalt der ausgelagerten Aktivitäten und Prozesse ab.

## Unwesentlich oder wesentlich?

Für einige der zu bewertenden, relevanten Kriterien werden seitens des BVR Vorschläge unterbreitet. Dabei werden die Vorteile von Auslagerungen innerhalb der Genossenschaftlichen FinanzGruppe positiv berücksichtigt. So kann z. B. bei Auslagerungen innerhalb der Genossenschaftlichen FinanzGruppe das Risiko, keinen Ersatzanbieter zu finden, unberücksichtigt bleiben. Gleiches gilt für die Herausforderung, die Tätigkeit ggf. nicht wieder eingliedern zu können. Auch die Risikokonzentration ist bei Auslagerungen innerhalb der Gruppe aufgrund der Governance-Strukturen grundsätzlich mit gering vorzubelegen. Als wichtig werden aber auch hier die Anforderungen an das Qualitätsniveau der Auslagerung, die Komplexität oder der mögliche Verstoß gegen spezialgesetzliche Vorgaben angesehen. Demzufolge sind sowohl die Risiken der Auslagerung selbst wie auch die Eignung des Auslagerungsunternehmens vorab zu berücksichtigen.

Hinsichtlich der Bewertung der Auslagerungsrisiken per se ist es ratsam, die von der Auslagerung betroffenen Prozesse zu bewerten, sich ein Bild über die betriebsinternen Abläufe vor und nach der Auslagerung zu machen und abzuklären, inwieweit es möglich ist, klare Definitionen über die Aufgabenallokationen zwischen Auftraggeber und Auftragnehmer zu treffen.

In Bezug auf die Wahl des Anbieters wären vor dem Hintergrund möglicher rechtlicher Risiken und/oder Ausfallrisiken bei der Bewertung des Auslagerungsunternehmens Nachfragen zur Kapitalausstattung, zum Reputationsrisiko oder dem Risiko aus möglichen Weiterverlagerungen indiziert.

Wurde die Risikoanalyse abgeschlossen, ist anhand der gewonnenen Erkenntnisse final die Frage zu beantworten, ob es sich um eine wesentliche oder nicht wesentliche Auslagerung handelt.

Dies fordert auch § 9 Abs. 3 Prüfberichtsverordnung (PrüfbV) als Anforderung für den Abschlussprüfer: „Dabei ist eine Aussage darüber zu treffen, ob die Einstufung von >

Auslagerungen als wesentlich oder unwesentlich unter Gesichtspunkten des Risikos, der Art, des Umfangs und der Komplexität nachvollziehbar ist."

Insgesamt verweist auch der BVR in seiner Übersicht zu ausgelagerten Geschäftsprozessen in Anlehnung an den § 9 Abs. 3 PrüfbV vom 3. Juli 2019 darauf, dass auf alle Fälle eine Prüfung durch die Institute im Einzelfall vorzunehmen ist. Seine grundsätzliche Annahme lautet, dass „eine solche Auslagerung regelmäßig als ‚wesentlich' einzustufen sein dürfte".

Somit verbleibt die grundsätzliche Beurteilung, ob wesentlich oder unwesentlich, letztendlich doch bei dem einlagernden Unternehmen selbst. Relevant ist diese Entscheidung vor allen Dingen in Bezug auf den Umfang der Maßnahmen und Kontrollen, die sich zur Steuerung der Auslagerung ergeben. Sollte das Unternehmen nach Abwägung aller geforderten Parameter zu dem Schluss kommen, dass die Auslagerung der IT-Revision unwesentlich ist, dann muss dies gut begründet sein.

Eventuell ergeben sich künftig durch die neuen EBA-Guidelines, deren Geltung die BaFin für 2020 auf ihr Programm genommen hat („comply or explain"), erleichternde Aspekte in Bezug auf Gruppen- oder Konzernauslagerungen.

## Bewertung der Auslagerungsdienstleistung der DZ CompliancePartner

Hinsichtlich der Risikoeinschätzung im Rahmen einer Auslagerung der IT-Revision an die DZ CompliancePartner könnte eine Bewertung auf Basis folgender Annahmen vorgenommen werden:

- Das Ausfallrisiko der DZ CompliancePartner als Auslagerungsdienstleister wird gemäß einem Gutachten der AWA-DO Deutsche Audit GmbH vom 15. März 2019 als gering eingestuft.
- Rechtliche Risiken sind aufgrund der Nutzung eines Auslagerungsvertrages nach BVR-Vorgaben überschaubar.
- Die DZ CompliancePartner setzt in diesem Bereich ausschließlich spezialisierte IT-Revisoren mit langjähriger Expertise ein und stellt deren laufende Aus- und Weiterbildung sicher.
- Die Durchführung der Prüfung wird in das Revisionskonzept der Bank integriert.
- Die Erkenntisse der Prüfungen werden durch die Bank aufgenommen und final geschlossen.
- Alle Arbeitspapiere der Prüfung verbleiben in der Bank. Der Vorstand wird unmittelbar und direkt informiert.
- Die IT-Systemlandschaft der Banken ist aufgrund der Nutzung der Systeme der Fiducia & GAD IT AG klar definiert und somit die Komplexität reduziert.
- Das Risiko einer Weiterverlagerung wird ausgeschlossen.

Diese Vorgehensweise ermöglicht es den Banken, einen externen IT-Revisor auch unmittelbar in das IKS der Bank einzubinden. Dadurch hat auch der Vorstand des Unternehmens die Möglichkeit (und die Verpflichtung), die Qualität der Dienstleistungserbringung direkt zu beurteilen, da der Bank sämtliche relevante Informationen zur Bewertung der Auslagerung zur Verfügung stehen. Gleichwohl bleibt die Erkenntnis, dass das jeweilige Institut, das einen externen IT-Revisor langfristig beauftragen möchte, eine Entscheidung hinsichtlich der Auslagerung der IT-Revision – unwesentlich oder wesentlich – bewusst und dokumentiert treffen muss. ▬

**AUTOR UND ANSPRECHPARTNER**

**Thomas Grebe**
Leiter IT-Audit,
E-Mail: thomas.grebe@dz-cp.de