IT-Outsourcing – aber wie?

Von Henrik Schulz

Quelle: pixabay

Das Outsourcing von IT-Dienstleistungen liegt im Kreditgewerbe im Trend. Die Einhaltung aller bankaufsichtlichen Vorgaben ist dabei von höchster Priorität. Henrik Schulz sieht dabei Dienstleister mit einem Fokus auf der Finanzbranche im Vorteil – für alle anderen lohne sich der Aufwand kaum. Aspekte, auf die die Aufsicht bei Prüfungen achtet, sind Informationssicherheit, Notfallvorsorge, Risikomanagement, Compliance sowie die Weiterverlagerung an Drittdienstleister. Red.

Das Auslagern von IT-Dienstleistungen gehört zur Finanzwirtschaft wie die Börse und das Kreditwesen. Laut einer aktuellen Studie[1)] wollen rund sieben von zehn Banken in Deutschland weitere IT-Aufgaben auslagern, 17 Prozent davon sogar in einem größeren Umfang. Das ergab eine Online-Befragung unter Fach- und Führungskräften aus den Abteilungen Risiko-Controlling, Kreditwesen, IT, interne Revision, Bankorganisation, Vertrieb und Kundenservice deutscher Banken zur Novelle der Mindestanforderungen an das Risikomanagement (MaRisk) 2017.

Dabei sind sich die Befragten bewusst, dass das Einhalten der rechtlichen Vorschriften mit steigendem Aufwand verbunden ist. Denn auslagernde Institute müssen sicherstellen, dass ihr IT-Dienstleister – obwohl er selbst kein Finanzinstitut ist – wesentliche gesetzliche und bankaufsichtliche Vorgaben aus der Finanzwirtschaft beachtet und umsetzt, wenn der Dienstleister Auslagerungen übernimmt. Insbesondere die Vorgaben aus der MaRisk sowie die daraus abgeleiteten Bankaufsichtlichen Anforderungen an die IT (BAIT) der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) sind hierbei maßgeblich.

Umsetzung der aufsichtlichen Anforderungen – ein enormer Aufwand

Damit trennt sich für Finanzdienstleister im IT-Outsourcing-Markt die Spreu vom Weizen. Denn die Berücksichtigung aufsichtsrechtlicher Anforderungen in der Finanzwirtschaft stellt auch an einen IT-Dienstleister besondere Anforderungen, die insbesondere Anpassungen in der Organisation und im Sicherheitsmanagement erfordern.

Die konsequente Umsetzung der Anforderungen lohnt sich in der Regel nur für Outsourcing-Dienstleister, die ihren oder einen wesentlichen Fokus auf die Finanzwirtschaft gelegt haben. Das verdeutlicht das Beispiel der Finanz Informatik Solutions Plus GmbH (FI-SP). Der IT-Dienstleister bietet Beratungs-, Entwicklungs- und Integrationsdienstleistungen sowie Outsourcing für Geschäftsanwendungen in der Finanzwirtschaft an.

Das Umsetzen der spezifischen Anforderungen der Branche an die Entwicklung und die Betreuung geschäftskritischer Anwendungen gehört daher zur DNA des Unternehmens. Und trotzdem musste das 100-prozentige Tochterunternehmen des zentralen IT-Dienstleisters der Sparkassen-Finanzgruppe, Finanz Informatik (FI), vor dem Hintergrund der 5. MaRisk-Novelle weitreichende Maßnahmen ergreifen, um auch in Zukunft den Anforderungen zu entsprechen, die die Aufsicht an Finanzdienstleister und damit auch an deren IT-Outsourcing-Partner stellt. Das Softwarehaus konnte dabei auf viele Best Practices der FI zurückgreifen und entsprechende Verfahren übernehmen.

Dennoch dauerten die Anpassungen und Neuaufstellungen in den von der Aufsicht besonders geprüften Gebieten Softwareentwicklung, Application Management, Informationssicherheit, Risikomanagement, Business Continuity Management (BCM), Compliance und Revision insgesamt rund zwei Jahre. Denn die Umsetzung der Anforderungen ist nicht

Zum Autor

Henrik Schulz, Zentralbereichsleiter Unternehmensservices, Finanz Informatik Solutions Plus GmbH, Frankfurt am Main

alleine durch Anpassungen von Verfahren und Prozessen zu erreichen. Sie erfordert vielmehr eine weitreichende Veränderung in der Art und Weise, wie IT-Dienstleistungen erbracht werden. Diesen Weg müssen auch die Mitarbeiter mitgehen und voller Überzeugung in sich tragen, wenn sie für Kunden aus der Finanzwirtschaft arbeiten.

Das Beispiel zeigt, dass IT-Dienstleister die aufsichtsrechtlichen Anforderungen nicht „mal eben nebenher" umsetzen, auch wenn sie bereits auf einer sehr guten Ausgangsbasis aufsetzen. Finanzdienstleister stehen daher vor der Herausforderung, bei Auslagerungsvorhaben einen Partner zu finden, bei dem ihre IT in guten Händen ist. Dazu empfiehlt es sich, bei der Anbieterwahl genau zu prüfen, wie die IT-Häuser ihre Informationssicherheit, Notfallvorsorge, Risikomanagement, Compliance sowie das Auslagerungsmanagement im Unternehmen umgesetzt haben und die Weiterverlagerung an Drittdienstleister organisieren. Denn das sind entscheidende Aspekte, auf die die Aufsicht bei Prüfungen achtet.

Informationssicherheit und BCM

Da sowohl Informationssicherheit als auch Business Continuity Management (BCM) in der MaRisk und der BAIT eine zentrale Rolle spielen, sollte der potenzielle Outsourcing-Partner nachweisen können, dass sich deren Geschäftsführung der großen Bedeutung der Informationssicherheit und des BCM bewusst ist. Ausdruck dessen ist unter anderem ein von der Geschäftsführung getragenes und unternehmensweit wirkendes Informationssicherheitsmanagement-System. Dieses wirkt entlang der gesamten Wertschöpfungskette und wird von allen Mitarbeitern angewendet. Es muss in der Lage sein, die aktuelle Bedrohungslage zu erkennen und auf dessen Grundlage wirksame Maßnahmen zum Schutz der Unternehmensinformationen zu definieren.

Um dies zu gewährleisten, hat beispielweise die FI-SP ihr Informationssicherheitsmanagement-System als kontinuierlichen Verbesserungsprozess etabliert. Dabei bezieht das System die Leitlinien und Ziele der Informationssicherheit ein und schützt Geschäftsprozesse, Mitarbeiter und Unternehmensinformationen unter risikoorientierten Gesichtspunkten. Es zielt darauf, dass die etablierten Prozesse, Methoden, Verantwortlichkeiten und Ressourcen in Kombination mit einer angemessenen Aufbauorganisation berücksichtigt und „gelebt" werden. BCM-Übungen und BCM-Planspiele sorgen dafür, dass die Praxistauglichkeit der BCM-Konzepte regelmäßig verifiziert wird. Damit stellt die FI-SP sicher, dass die Einhaltung des Sicherheits- und Kontinuitätsniveaus von Informationen nachhaltig und effektiv ist.

ISO/IEC 27001:2013 gibt Sicherheit

Auslagernde Unternehmen können prüfen, ob ein zukünftiger IT-Dienstleister ihres Vertrauens sein Informationssicherheitsmanagement-System und seinen BCM-Prozess auf Basis von ISO/IEC 27001:2013 zertifiziert hat. Dann haben Finanzdienstleister Gewissheit, dass beides auf Prozessen, Konzepten, Richtlinien und Kontrollen basiert, die einem international gültigen Sicherheitsstandard entsprechen.

Dazu gehört etwa auch, dass ausreichend Ressourcen für eine anpassungsfähige Informationssicherheits- und Notfallorganisation bereitgestellt werden können. Das ist eine wichtige Voraussetzung, um auch in Zukunft flexibel auf sich ändernde regulatorische Anforderungen reagieren zu können. Die FI-SP hat das ISO27001-Zertifikat seit 2014.

Risikomanagement und Compliance – Prüfungsschwerpunkte der Aufsicht

Wie IT-Dienstleister Risiken erkennen und managen ist ein weiterer Prüfungsschwerpunkt der Aufsicht. Finanzdienstleister sollten sich also von einem Dienstleister, dem sie eine Auslagerung übertragen wollen, nachweisen lassen, dass dieser über einen etablierten Risikomanagementprozess verfügt. Indem sie die Risikoberichte anfordern, bekommen auslagernde Unternehmen eine erste Indikation davon, ob und wie professionell ein Dienstleister seine Risiken erkennt, kontrolliert und steuert. Professionell aufgestellte IT-Unternehmen beziehen sich dabei nicht nur auf Unternehmens- sondern auch auf Projektrisiken. Das Berichtswesen erstreckt sich dabei über alle Geschäftsbereiche und Hierarchieebenen und gibt Auskunft über den aktuellen Risikobestand, die geplanten oder beauftragten Steuerungsmaßnahmen sowie die Veränderungen der Risiken im Zeitablauf.

Wichtig ist es außerdem zu prüfen, ob sich der Risikomanagementprozess an den gesetzlichen Anforderungen gemäß dem Gesetz zur Kontrolle und Transparenz im Unternehmen (KonTraG) und der MaRisk ausrichtet. Denn damit ist zum einen sichergestellt, dass Risiken frühzeitig erkannt, systematisch analysiert, angemessen gesteuert und überwacht werden. Zum anderen kann dann davon ausgegangen werden, dass das Risikomanagement wirklich mit der Unternehmensstrategie verzahnt ist und die Risikofelder sowie die Aufteilung von Risiken regulationskonform in interne und externe Schadenpotenziale definiert sind.

Eine systematische Steuerung von Risiken rundet das Risikomanagement ab. Orientiert sich der IT-Dienstleister an etablierten Modellen wie etwa dem Three-Lines-of-Defence-Modell, dann unternimmt er alles für einen risikoarmen Geschäftsbetrieb.

Zwar stellt die Aufsicht keine besonderen Anforderungen an das Compliance Management eines externen Partners. Doch sollte ein Dienstleister grundsätzlich nachweisen können, dass er über Mechanismen verfügt, mit denen er gesetzliche,

regulatorische und vertragliche Anforderungen kontinuierlich überwacht.

Auslagerungsmanagement als Prozess

IT-Dienstleister decken Lastspitzen, Spezialaufgaben oder auch Regeltätigkeiten zum Teil durch externe Mitarbeiter oder Subdienstleister ab. Ein professionelles Auslagerungsmanagement gehört deshalb zum Selbstverständnis eines geeigneten Outsourcing-Nehmers. Dazu gehört, dass er etwaige Subdienstleister auf die Einhaltung aufsichtsrechtlich relevanter Tatbestände verpflichtet und dieses auch überprüft wird. Das Auslagerungsmanagement als Prozess ist dabei mit anderen Prozessen, etwa dem Risikomanagement und der Informationssicherheit, verbunden, was sich in dem Reporting an das auslagernde Institut widerspiegelt. Schließlich gehört es zu seinen Pflichten, dass ein Dienstleister über die Weiterverlagerung von Aufgaben uneingeschränkte Transparenz walten lässt.

Im Falle einer Übertragung von Aufgaben an Externe weisen professionelle Outsourcing-Partner nach, dass sie mit ihren Subdienstleistern Vereinbarungen getroffen haben, die den betroffenen Outsourcing-Gebern die notwendigen Prüfungs- und Kontrollrechte einräumen. Zudem stellen sie sicher, dass bei Auftragsvergabe an Subdienstleister vorab eine Risikoanalyse durchgeführt und die Leistungserbringung während der Auslagerung in einer geeigneten Weise überwacht und gesteuert wird, damit gegebenenfalls vorhandene Risiken reduziert werden. Und last, but not least definieren professionelle Outsourcing-Nehmer eindeutige Regelungen, um die Beauftragung an Subdienstleister wirkungsvoll beenden zu können, wenn es die Situation erfordert (Exit-Strategie).

Nahezu selbstverständlich ist es bei der Auslagerung im Finanzdienstleistungsumfeld, dass Auftraggeber ihre Auftragnehmer auf die Einhaltung des Datenschutzes verpflichten. Das gilt sowohl für die Beauftragung der Subdienstleister durch die Outsourcing-Nehmer als auch für die Auftragsvergabe durch auslagernde Institute selbst.

Die uneingeschränkte Berücksichtigung der EU-DSGVO ist dabei das Maß der Dinge, an dem sich jede Zusammenarbeit messen lassen muss. Eine Integration von Datensicherheit und Datenschutz in den Risikomanagementprozess hat sich dabei bewährt.

Revision – durch die Bank oder den IT-Dientsleister

Das auslagernde Unternehmen hat die mit Auslagerungen verbundenen Risiken angemessen zu steuern und die Ausführung der ausgelagerten Aktivitäten und Prozesse ordnungsgemäß zu überwachen. Dies umfasst auch die regelmäßige Beurteilung der Leistung des Auslagerungsunternehmens. Um dieser Anforderung gerecht zu werden, kann der Finanzdienstleister diese Leistungen selbst prüfen oder auf Ergebnisse der internen Revision des Auslagerungsunternehmens zurückgreifen.

Die FI-SP hat sich dafür entschieden, eine interne Revision zu etablieren, die risikoorientiert und prozessunabhängig die Wirksamkeit und Angemessenheit des Risikomanagements des Unternehmens im Allgemeinen und des internen Kontrollsystems im Besonderen sowie die Ordnungsmäßigkeit grundsätzlich aller Aktivitäten und Prozesse prüft und beurteilt, unabhängig davon, ob diese ausgelagert sind oder nicht. Durch eine vertraglich vereinbarte regelmäßige Revisionsberichterstattung hat das auslagernde Unternehmen die Gewissheit, dass die Revision MaRisk-konform aufgestellt ist und eine unabhängige Bewertung der ausgelagerten Prozesse und Dienstleistungen bekommt.

Die Suche nach dem richtigen Partner

Keine Frage, die Regulatorik bedeutet für Finanzinstitute und damit auch für deren Dienstleister einen höheren Aufwand. Ein Aufwand, dem kein unmittelbarer finanzieller Ertrag entgegensteht, den aber jedes Institut tragen muss. Zu einem Wettbewerbsvorteil kann er sogar werden, wenn Finanzinstitute in der Lage sind, ihren regulationsbedingten Aufwand auf mehrere Schultern zu verteilen.

Branchenversierte IT-Dienstleister bieten nicht nur die Sicherheit, dass die aktuellsten aufsichtsrechtlichen Anforderungen eingehalten werden. Sie bieten den Instituten auch die Chance, von Skaleneffekten zu profitieren. Denn sie arbeiten für zahlreiche, auch systemrelevante Häuser. Damit sind sie in der Lage, Skaleneffekte zu erzielen, von denen alle auslagernden Institute profitieren.

1) Studie „MaRisk-Novelle 2017 – Befragung unter 100 Fach- und Führungskräften in Banken", Procedera Consult