Fassung vom Juli 2018

Arbeitshilfe
für die Erstellung einer Risikobewertung bei sonstigem Fremdbezug von IT-Dienstleistungen

Inhalt

1. Hinweise zur Durchführung einer Risikobewertung

Gemäß BAIT-Modul 8, Tz. 53 ist für jeden sonstigen Fremdbezug von IT-Dienstleistungen vorab eine Risikobewertung durchzuführen.

Hinweis: Soweit IT-Dienstleistungen entsprechend den Erläuterungen zu AT 9 Tz 1 MaRisk seitens der Bank bereits als (wesentliche oder unwesentliche) Auslagerung einer regelmäßigen Risikoanalyse unterliegen, ist darüber hinaus keine zusätzliche Risikobewertung nach Modul 8 der BAIT notwendig.
Die Anwendung der Module 1 – 7 der BAIT erfolgt unabhängig von der Unterscheidung zwischen Auslagerung im Sinne von AT 9 MaRisk und sonstigem Fremdbezug von IT-Dienstleistungen gemäß Modul 8 der BAIT.

Art und Umfang der Risikobewertung beim sonstigen Fremdbezug von IT-Dienstleistungen kann die Bank unter Proportionalitätsgesichtspunkten flexibel festlegen. Die beigefügte **Arbeitshilfe bildet ein beispielhaftes Vorgehen** für den sonstigen Fremdbezug von IT-Dienstleistungen ab. Das Clustern von IT-Dienstleistungen für gleichartige Formen des sonstigen Fremdbezugs von IT-Dienstleistungen ist dabei sinnvoll, da für diese auf bestehende Risikobewertungen zurückgegriffen werden kann.

Einen Schwerpunkt der Risikobewertung bei IT-Dienstleistungen bilden die Informationsrisiken, die sich aus dem sonstigen Fremdbezug einer IT-Dienstleistung ergeben können. Es wird deshalb in der Arbeitshilfe vorrangig auf die Schutzziele der Geschäftsprozesse, Daten und IT-Systeme, für die die IT-Dienstleistung eine Rolle spielt, abgestellt. Tiefe und Umfang der Risikobewertung können sich z.B. abhängig vom Schutzbedarf unterscheiden.

Eine **erneute Risikobewertung** ist bei Änderungen beim Bezug einer IT-Dienstleistung (bei dauerhaftem Bezug) sowie dann erforderlich, wenn der Bank Umstände bekannt werden, die darauf schließen lassen, dass sich die bei der Bewertung verwendeten Risikofaktoren verändert haben (anlassbezogene Risikobewertung).
Zudem ist bei dauerhaftem Bezug oder Rückgriff auf bestehende Risikobewertungen bei gleichartigen Formen des sonstigen Fremdbezugs die Risikobewertung in regelmäßigen Zeitabständen zu erneuern, auch wenn kein Anlass besteht. Es wird ein Zeitraum von … Jahren für angemessen erachtet (regelmäßige Risikobewertung).[1]

[1] Die Bank könnte bei der Überprüfung der Risikobewertung beim sonstigen Fremdbezugs auf einen Zeitraum analog zur regelmäßigen Risikoanalyse bei nicht wesentlichen Auslagerungen (z.B. alle 3 Jahre) abstellen (vgl. Arbeitshilfe für die Erstellung einer Risikoanalyse bei Auslagerungen).

2. Risikobewertung

IT-Dienstleistung	BankingGuide ZV auf der Vertriebsplattform		
IT-Dienstleister	BankingGuide GmbH		
Kriterien	**Beurteilungs-ergebnis** (Bitte eintragen / ankreuzen)		**Bemerkungen/Erläuterungen/ abzuleitende Maßnahmen[2]** sowie ggf. Verweis auf Unterlagen etc.(Bitte Spalte ausfüllen)
Anforderungen an die IT-Dienstleistung			
(höchster) Schutzbedarf der Geschäftsprozesse, Daten bzw. IT-Systeme, die mit der IT-Dienstleistung im Zusammenhang stehen [3]	Verfügbarkeit (1 niedrig, 2 mittel, 3 hoch, 4 sehr hoch)	mittel	Verfügbarkeit: Beim BankingGuide 2.0 handelt es sich um keine Kundenanwendung. Der BankingGuide 2.0 ist eine Beratungsanwendung und steht dem ZV-Berater im operativen Geschäft zur Verfügung. Ausfallzeiten haben jedoch keine erheblichen Auswirkungen auf das gesamte Kundengeschäft, da maximal einzelne Termine zu Ausfallzeiten nicht durchführbar sind und nachgeholt werden müssen. Der Ausfall des BankingGuide 2.0 hat zu keinem Zeitpunkt Auswirkungen auf das gesamte Kundenportfolio. Integrität: Die Verarbeitung von falschen Daten könnte zu falschen Produktempfehlungen führen. Dies wird im BankingGuide 2.0 verhindert, indem fachliche Änderungen zuerst in einer Redaktionsinstanz eingespielt und getestet werden können. Erst nach erfolgter Qualitätssicherung werden die Änderungen in die Produktionsinstanz übernommen. Dort führt der fachkundige Berater die Beratung mit Unterstützung der Anwendung durch und kann jederzeit in die Empfehlungen eingreifen. Auch an dieser Stelle können falsche Produktzuordnungen vom Berater
	Integrität (1 niedrig, 2 mittel, 3 hoch, 4 sehr hoch)	Mittel	

[2] inklusive Hinweis, ob eine Berücksichtigung bei der Vertragsgestaltung erforderlich ist
[3] gemäß AT 7.2 MaRisk iVm. BAIT Modul 3 Tz. 11 jeweils für die Schutzziele Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität

			noch erkannt und korrigiert werden. Es werden keine Lösungen vorgegeben, sondern lediglich Empfehlungen. Vertraulichkeit: Der BankingGuide wird auf der Vertriebsplattform, auf Servern der Fiducia GAD IT betrieben und genießt dadurch größte Sicherheit. Durch die Kompetenzgesteuerte Verfügbarkeit sind sowohl die Daten als auch der Zugriff auf die Konfigurationseinstellungen nur vom berechtigten, durch entsprechende Kompetenzprofile definierte, Personenkreise aufzurufen. Die Verwaltung der Kompetenzprofile erfolgt über die Vertriebsplattform. Authentizität: Die Anwendung ist in die Vertriebsplattform der Fiducia GAD IT integriert und wird innerhalb des Bankensystems zur Verfügung gestellt. Die Kommunikationspartner sind hierüber klar zu identifizieren. Dritte haben keinen Zugriff.
	Vertraulichkeit (1 niedrig, 2 mittel, 3 hoch, 4 sehr hoch)	gering	
	Authentizität (1 niedrig, 2 mittel, 3 hoch, 4 sehr hoch)	gering	
Anforderungen an die Qualität der Dienstleistung	Hoch		Die Antworten des Kunden führen zu Produktempfehlungen. Diese können jederzeit vom Berater und vom Kunden übersteuert werden. Die Beratungsanwendung nimmt keinen Einfluss auf Kreditentscheidungen und beeinflusst nicht die Adressausfallrisiken.
	Mittel	x	
	Gering		
Zeitkritische Bedeutung der IT-Dienstleistung [4] (Einbezug in Notfallplanung AT 7.3 MaRisk notwendig?)	Hoch		Der BankingGuide 2.0 ist eine Beratungssoftware, allerdings sind Ausfallzeiten jederzeit durch den Berater aufzufangen und betreffen niemals den gesamten Kundenbestand. Die Software dient zur Unterstützung im Beratungsgespräch, ersetzt aber nie den Kundenberater.
	Mittel		
	Gering	x	
	Nicht relevant		

[4] Zusammenhang zum Schutzbedarf (Schutzziel Verfügbarkeit) beachten: ein zeitkritischer Prozess impliziert, dass die dafür benötigte IT-Anwendung auch eine entsprechend hohe bzw. sehr hohe Verfügbarkeit i.S. des Schutzbedarfs haben sollte

Kriterien	**Beurteilungs-ergebnis** (Bitte ankreuzen)		**Bemerkungen/Erläuterungen/ abzuleitende Maßnahmen[5]** sowie ggf. Verweis auf Unterlagen etc.(Bitte Spalte ausfüllen)
Risikobewertung			
Hat die Erbringung oder Schlechtleistung der IT-Dienstleistung Einfluss auf die Erfüllung der Schutzziele?[6]	Hoch		Der Dienstleister hat umfangreiche Maßnahmen zur Sicherstellung der Schutzziele getroffen. Die Anwendung wird über das Rechenzentrum der Volks- und Raiffeisenbanken (Fiducia GAD IT AG) in Deutschland betreiben.
	Mittel	x	
	Gering		
	nicht relevant		
Risiko, dass die IT-Dienstleistung selbst oder Aktivitäten und Prozesse des Dienstleisters ausfallen oder der Dienstleister insgesamt wegfällt, z. B. durch Kündigung, Vertragsbeendigung, Insolvenz, Betriebsaufgabe (Ausfall)	Hoch		Beim BankingGuide 2.0 der BankingGuide GmbH handelt es sich um ein Gemeinschaftsprodukt der DZ Bank AG und der BMS Consulting GmbH. Die Kündigungsfrist des BankingGuide 2.0 beträgt 12 Monate zum Jahresende. Die DZ Bank AG ist als genossenschaftliche Zentralbank wirtschaftlich sehr stark und über jeden Zweifel erhaben. Die BMS Consulting ist seit über 15 Jahren exklusiv für die genossenschaftliche Finanzgruppe als Beratungsunternehmen und Softwareentwickler tätig. Derzeit beschäftigt die BMS-Group ca. 200 Mitarbeiter. Die Jahresabschlüsse gem. Bundesanzeiger sind sehr solide.
	Mittel		
	Gering	x	
	nicht relevant		
Risiko, bei Ausfall oder Schlechtleistung zeitnah keinen Ersatzanbieter für die IT-Dienstleistung zu finden, so dass es zu erheblichen Beeinträchtigungen im Geschäftsbetrieb kommt	Hoch		Aktuell gibt es am Markt keinen Anbieter welcher die erbrachte Leistung hinsichtlich der Qualität und Effizienz adäquat substituieren kann. Bei einem Ausfall des Systems kommt es jedoch nicht zu einer erheblichen Beeinträchtigung des Geschäftsbetriebes.
	Mittel	x	
	Gering		
	nicht relevant		
Risiko, dass die IT-Dienstleistung oder der Dienstleister gegen	Hoch		Die Beratungssoftware dient vor allem der Beratung von Firmen- und Unternehmenskunden der Bank, wird
	Mittel		

[5] inklusive Hinweis, ob eine Berücksichtigung bei der Vertragsgestaltung erforderlich ist
[6] gemäß AT 7.2 MaRisk iVm BAIT Modul 3 Tz. 11 / 12

rechtliche Vorgaben (z. B. zivilrechtliche Vorgaben, aufsichtsrechtliche Vorgaben) verstößt	Gering	x	über das Rechenzentrum angeboten und wertet keine Kundenangaben insofern aus, als dass für den Kunden in irgendeiner Art und Weise Konsequenzen seitens der Bank entstehen. Keine Auswirkungen auf Kreditentscheidungen, keine Beeinflussung ratingrelevanter Daten.
	nicht relevant		
Risiko eines erheblichen Reputationsschadens durch Mängel der Dienstleistung bzw. Schlechtleistung oder Ausfall des Dienstleisters	Hoch		Der Reputationsschaden ließe sich in dem Fall vermuten, wenn dem Kunden aus der Beratungssoftware ein Produkt empfohlen wird, welches nachweislich falsch oder zu teuer wäre, sodass der Kd. sich benachteiligt fühlt. Jedoch kann hier, wie oben beschrieben, der Berater jederzeit diesem Mangel identifizieren und die Produktempfehlung übersteuern sowie den Mangel melden und zeitnah (durch die bankeigene Konfigurationsfähigkeit) beheben lassen. Weitere Mängel sind in der
	Mittel		
	Gering	x	
	nicht relevant		

Datum: _____

Erstellt durch: _____

Einbindung der Funktion Informationssicherheit: _____

Einbindung der Funktion Notfallmanagement: _____

Einbindung der Funktion Risikocontrolling: _____
(nur bei Bedarf)