

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

Inhalt

- 1. Hinweise zur Durchführung einer Risikobewertung**
- 2. Risikobewertung**

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	(Kundenselbst-)Beratungsanwendungen im VR Payment-Leistungspaket		
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	Ausfallzeiten haben keine erheblichen Auswirkungen auf das gesamte Kundengeschäft, da – nur ein kleiner Kundenkreis (Geschäfts- und Gewerbekunden mit POS-Geschäft) vorübergehend keine Produktbestellungen durchführen bzw. Berater*innen keine Produkthanträge digital zur VR Payment senden können. Es besteht – in diesem Fall - die Möglichkeit, die Produkthanträge papierhaft (über entsprechende Serviceanträge) an VR Payment zu senden. Der Ausfall des BankingGuide 2.0 hat zu keinem Zeitpunkt Auswirkungen auf das gesamte Kundenportfolio.
	Integrität (1 niedrig, 2 mittel, 3 hoch, 4 sehr hoch)	Mittel	Die Verarbeitung von falschen Daten könnte zu falschen Produktbestellungen führen. Dies wird in allen Anwendungen dadurch verhindert, dass fachliche Änderungen zuerst in einer Redaktionsinstanz eingespielt und getestet werden können und erst nach erfolgter Qualitätssicherung als Änderungen in die Produktionsinstanz übernommen werden. Es werden keine Lösungen vorgegeben, sondern lediglich Empfehlungen ausgesprochen. Führt der Kunde eine Bestellung im Self-Service (Online- Banking, Homepage) eigenständig durch, hat dieser

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

			ein entsprechendes Widerrufsrecht für die getätigte Bestellung.
	Vertraulichkeit (1 niedrig, 2 mittel, 3 hoch, 4 sehr hoch)	gering	<p>Die Anwendungen des Leistungspakets werden auf Servern der Atruvia AG betrieben und genießen dadurch größte Sicherheit.</p> <p>Für Anwendungen des Leistungspakets, die der Kunde auf der Homepage oder im Online-Banking selbstständig nutzt: Durch gesicherte Aufruf-Wege (Homepage: https-Verschlüsselung / Online-Banking: Kunden-Login) sind Kundendaten und -eingaben vor Manipulation und Datenklau geschützt.</p> <p>Für Anwendungen des Leistungspakets, welche im BankingWorkspace betrieben werden: 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 den BankingWorkspace.</p>
	Authentizität (1 niedrig, 2 mittel, 3 hoch, 4 sehr hoch)	gering	<p>Die Anwendungen sind in bekannte Plattformen der genossenschaftlichen Finanzgruppe (betrieben von VR-NetWorld und ATRUVIA) integriert und ein Zugriff ist auch nur über die genannten Plattformen möglich.</p> <p>Die Kommunikationspartner sind hierüber klar zu identifizieren. Dritte haben keinen Zugriff.</p>
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
	Mittel	x	
	Gering		

			Kreditentscheidungen und beeinflusst nicht die Adressausfallrisiken.
Zeitkritische Bedeutung der IT-Dienstleistung ⁴ (Einbezug in Notfallplanung AT 7.3 MaRisk notwendig?)	Hoch		Der (Kundenselbst-)Beratungswendungen des Leistungspakets dienen allesamt dem Zweck digitale Produktabschlüsse zu generieren und sind somit Vertriebswerkzeuge. Ausfallzeiten können jederzeit durch alternativ zur Verfügung stehende manuelle Prozesse aufzufangen und betreffen niemals den gesamten Kundenbestand. Die Software dient zur Unterstützung des Produktvertriebs der Bank, ersetzt aber nie den Kundenberater.
	Mittel		
	Gering	x	
	Nicht relevant		
Kriterien	Beurteilungsergebnis (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 (Atruvia 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		Der Anbieter des Leistungspakets ist die BankingGuide GmbH, welche im Besitz der DZ BANK AG (60%) sowie der BMS Consulting GmbH (40%) ist. Die Kündigungsfrist des Leistungspakets 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. 250 Mitarbeiter.
	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

⁵ inklusive Hinweis, ob eine Berücksichtigung bei der Vertragsgestaltung erforderlich ist

⁶ gemäß AT 7.2 MaRisk iVm BAIT Modul 3 Tz. 11 / 12

			Die Jahresabschlüsse beider Gesellschafter (einzusehen im Bundesanzeiger) sind sehr solide.
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 rechtliche Vorgaben (z. B. zivilrechtliche Vorgaben, aufsichtsrechtliche Vorgaben) verstößt	Hoch		Die Anwendungen des Leistungspakets dienen vor allem dem Produktvertrieb bei sowie der Beratung von Firmenkunden der Bank. Die Anwendungen werden über das Rechenzentrum der Genossenschaftlichen Finanzgruppe (ATRU VIA) angeboten und werten 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.
	Mittel		
	Gering	x	
	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 den Anwendungen heraus ein Produkt empfohlen wird, welches nachweislich nicht den Kundenbedarf deckt oder zu teuer wäre, sodass der Kd. sich benachteiligt fühlt. Mit einer lösungsorientierten Kommunikation gegenüber dem Kunden ließe sich ein solcher – vermeintlicher – Reputationsschaden jedoch schnell beheben.
	Mittel		
	Gering	x	
	nicht relevant		

Datum: _____

Erstellt durch: _____

Einbindung der Funktion Informationssicherheit: _____

Einbindung der Funktion Notfallmanagement: _____

Einbindung der Funktion Risikocontrolling:
(nur bei Bedarf) _____

BEISPIEL