Anlage Schnittstellenbeschreibung

Zum Auslagerungsvertrag zur Übernahme der Auslagerungssteuerung die Fiducia & GAD IT AG betreffend

zwischen

Firma
Straße Hausnummer
PLZ Ort
Registernummer HR/GR: xx

vertreten durch den Vorstand/die Geschäftsleitung
(nachfolgend Auftraggeber oder F&G)

und

ZAM eG
Wilhelm-Haas-Platz,
63263 Neu-Isenburg/Zeppelinheim-Ost
Registergericht Offenbach GnR 4013

vertreten durch den Vorstand
(nachfolgend Auftragnehmer oder ZAM eG)

1 Hinweise zum Auslagerungsmanagement nach MaRisk AT 9

1. Die Auslagerung der Funktion des Auslagerungsmanagements auf eine zentrale Steuerungsinstanz und der Teilauslagerung von Unterstützungsleistungen für die interne Revision stellen regelmäßig eine wesentliche Auslagerung im Sinne der Mindestanforderungen an das Risikomanagement (MaRisk) Abschnitt AT 9 ~~dar~~ sowie § 25b KWG dar. Nicht ausgelagert ist mit diesem Vertrag die Steuerung und Überwachung der Auslagerung auf die ZAM eG.

2. Bei der ZAM eG handelt es sich um einen Mehrmandantendienstleister. Die nach den MaRisk im Abschnitt AT 9 eingeräumten Erleichterungen können aus den nachfolgend dargestellten Gründen in Anspruch genommen werden:

   a. Die ZAM eG verfügt über eine gemäß den Anforderungen der MaRisk organisierte Interne Revision.

   b. Die Ordnungsmäßigkeit der Dienstleistungserbringung wird einer jährlichen Prüfung durch eine unabhängige Wirtschaftsprüfungsgesellschaft in Anwendung des Prüfungsstandards des Instituts der Wirtschaftsprüfer (IDW) PS 951 „Die Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen“ unterzogen.

3. Die nachfolgend dargestellte Schnittstellenbeschreibung, die Bestandteil des Auslagerungsvertrages ist, spezifiziert die Schnittstellen zwischen dem auslagernden Institut (Auftraggeber) und der ZAM eG sowie die jeweils zu erbringenden Leistungen/Sicherungsmaßnahmen hinreichend klar.

4. Vor diesem Hintergrund ergibt sich folgendes grundsätzliches Prüfungskonzept:

   4.1 Tätigkeiten, die nach dieser Schnittstellenbeschreibung beim Auftraggeber verbleiben, sind wie bisher in das IKS/die Prüfungen des Auftraggebers aufzunehmen.

   Es wird ausdrücklich darauf hingewiesen, dass die in der Schnittstellenbeschreibung für die Interne Revision des Auftraggebers genannten Prüfungshandlungen ausschließlich empfehlenden Charakter tragen und keinen Eingriff in die eigenverantwortliche Erstellung einer risikoorientierten Prüfungsplanung und -durchführung darstellen.

   4.2 Für Tätigkeiten/Sicherungsmaßnahmen, die nach der Schnittstellenbeschreibung im Verantwortungsbereich der ZAM eG liegen, kann, soweit keine wesentlichen Beanstandungen durch den Abschlussprüfer, den Prüfer nach IDW 951.2 oder die Interne Revision der ZAM eG festgestellt wurden, der Prüfungsumfang der Internen Revision des Auftraggebers reduziert werden. Unberührt bleibt Abschnitt 3.2 des Auslagerungsvertrages (Hauptvertrag), insbesondere das Recht zu Ergänzungsprüfungen bei Zweifeln an der Funktionsfähigkeit der Innenrevision der ZAM eG. Im Regelfall können sich die Prüfungshandlungen der Internen Revision des Auftraggebers in diesen Bereichen auf die kritische Durchsicht folgender Unterlagen beschränken, ~~dabei unterstützt die ZAM eG über die separate Dienstleistungen „Unterstützung der internen Revision der Auftraggeber“ durch empfehlende Auslegungs- und Interpretationshinweise~~ hierbei erfolgt eine Unterstützung durch die ZAM eG:[1]

      a. Berichte zum Auslagerungsmanagement der ZAM eG,

      b. Muster-Risikoanalyse[2] der ZAM eG,

      c. Informationen über wesentliche Feststellungen aus dem IKS der ZAM eG,

[1] Hinweis: Das Ergebnis der Durchsicht ist zu dokumentieren.

[2] Hinweis: Die Muster-Risikoanalyse ist zu individualisieren und durch den Auftraggeber zu beschließen.

d. Bericht der Internen Revision der ZAM eG über wesentliche Mängel und

e. Bericht über die Prüfung des dienstleistungsbezogenen Internen Kontrollsystems und dessen Wirksamkeit des ausgelagerten Bereichs (Ordnungsmäßigkeit der Dienstleistungserbringung der ZAM eG).

5. Ausnahmen vom dargestellten Regelfall können sich insbesondere (aber nicht nur) bei Beanstandungen aus den vorgenannten Unterlagen ergeben.

6. Beziehen sich diese Mängel auf die Handhabung der Präventionsmaßnahmen bei der ZAM eG, müssen i. d. R. sowohl die Interne Revision des Auftraggebers als auch dessen Abschlussprüfer ergänzende Prüfungshandlungen anhand eigener Stichproben vornehmen, um eine ausreichende Prüfungssicherheit zu erhalten.

7. Sofern sich die Mängel auf die Dienstleistungserbringung der ZAM eG beziehen und diese nicht innerhalb ~~angemessener~~ einer angemessenen Zeit abgestellt werden oder Zweifel an der Funktionsfähigkeit der Internen Revision des Auftragnehmers entstehen, ergibt sich für die Interne Revision des Auftraggebers und/oder deren Abschlussprüfer in Anwendung von BT 2.1, Tz. 3 der MaRisk das Erfordernis zu eigenen Ergänzungsprüfungen. Sofern die Ergänzungsprüfungen auf Mängel im Internen Kontrollsystem (Angemessenheit und Funktionsfähigkeit/Wirksamkeit) der ZAM eG zurückzuführen sind, ist die ZAM eG berechtigt ~~anstelle~~, anstelle dessen und unter Zustimmung des Steuerungsgremiums der ZAM eG einen externen Prüfer mit der Ergänzungsprüfung zu beauftragen. Die ZAM eG trägt die Kosten dieser erforderlichen Ergänzungsprüfungen ihres Internen Kontrollsystems. Im Übrigen werden die Kosten durch den Auftraggeber getragen.

8. Eine detaillierte Darstellung der im Bereich des Auftraggebers (inkl. Interne Revision) verbleibenden Revisions- und Kontrollhandlungen ergibt sich aus der folgenden Schnittstellenbeschreibung.

9. Die nach dem IDW PS 951 zu erstellende Bericht über die Prüfung des dienstleistungsbezogenen internen Kontrollsystems (Bericht nach Typ 2) wird dem Auftraggeber zeitnah und unaufgefordert zur Verfügung gestellt. Der Abschlussprüfer des Auftraggebers wird im Rahmen seines risikoorientierten Ansatzes die Tätigkeit der Internen Revision und die Ergebnisse des Abschlussprüfers des Auftragnehmers nach IDW PS 951 (Bescheinigung nach Typ 2) verwenden. Nach pflichtgemäßem Ermessen wird der Abschlussprüfer des Auftraggebers über seine Prüfungshandlungen entscheiden. Soweit beim Auftraggeber bzw. beim Auftragnehmer keine Beanstandungen festgestellt wurden, kann der Abschlussprüfer des Auftraggebers nach pflichtgemäßem Ermessen eigenverantwortlich einen geringen Prüfungsumfang festlegen.

2-4 entfallen

2. ~~Hinweise zum Vertrag über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 und 29 DSGVO~~

~~Die ZAM eG erbringt im Rahmen des Vertrags über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 und 29 DSGVO – dort in seiner Funktion als Auftragsverarbeiter – für den Verantwortlichen Dienstleistungen entsprechend der jeweils geltenden aktuellen Verträge (inkl. dieser Schnittstellenbeschreibung sowie sämtlicher anderen Anlagen). Dazu ist es erforderlich, dass der Auftragsverarbeiter u.a. personenbezogene Daten verarbeitet, für die der Verantwortliche im Sinne des Datenschutzrechts verantwortlich ist. Es werden dabei einfache personenbezogene Daten verarbeitet; je nachdem welche Daten einschlägig sind, werden folgende Daten verarbeitet:~~

~~Name, Titel, akademischer Grad~~	~~Notes Username~~
~~Anschrift~~	~~Postfach für Notes Mail (optional)~~
~~Geburtsdatum~~	~~Rolle~~
~~Filiale~~	~~Straße (privat)*~~
~~Weitere Filialen~~	~~PLZ (privat)*~~
~~Abteilung~~	~~Ort (privat)*~~
~~Art der Stelle~~	~~Telefon (privat)*~~
~~Funktion/Tätigkeit~~	~~Mobil (privat)*~~
~~Vorgesetzter~~	~~Fax (privat)*~~
~~Telefon~~	~~Email (privat)*~~
~~Mobil~~	~~Eigenschaften (Hilfsdienste, Netzbetreiber, Technik, Versorger, Sonstige)~~
~~Fax~~	~~Ansprechpartner~~
~~Eintrittsdatum~~	~~Besonderheiten~~
~~Austrittsdatum~~	~~Hinweise~~
~~Personalnummer~~	~~Teilnehmernummer~~
~~GenoUserID bzw. BB3User ID~~	~~Verantwortlich für Geschäftsfeld~~
~~Bedienernummer (Fiducia)~~	~~Mitarbeiter von Geschäftsfeld~~
~~Beraternummer (Fiducia und Bankmitarbeiter)~~	~~Internet Mailadresse~~
~~Userstatus (Persönlicher User, Technischer User, Dummy User)~~	~~*= optional~~

5 Schnittstellenbeschreibung

			Zuordnung ZAM eG	Zuordnung Institut / Auftraggeber
1	**Rahmen zur Etablierung eines rechts-konformen Auslagerungsmanagements**	AT 9 TZ 6-8, AT9		
1.1			Entwurf Arbeitsanweisung / Regelungen zur Etablierung eines zentralen Auslagerungsmanagements durch die Zusammenarbeit der Bank mit der ZAM eG	Übernahme und Inkraftsetzung der Arbeitsanweisung und der Regelungen zur Etablierung eines zentralen Auslagerungsmanagements durch die Zusammenarbeit der Bank mit der ZAM eG sowie Ermächtigung der ZAM eG zur Entgegennahme der erforderlichen Informationen der F&G (inkl. Unternehmen in der Weiterverlagerung) und Anweisung der F&G zur Weitergabe der erforderlichen Informationen über den Abschluss des Auslagerungsvertrages. Ermächtigung der ZAM eG zur Interessenvertretung der Bank im Rahmen der Auslagerungssteuerung gegenüber der F&G und der Unternehmen in der Weiterverlagerung.
1.2			Erstellung einheitlicher Muster / Templates für ein stringentes Auslagerungsmanagement sofern keine Verbundhilfe vorhanden oder zu verwenden ist (Risikoanalyse, Berichtsauswertung, etc.)	Übernahme der Muster / Templates, verbindliche Nutzung des ~~Auslagerungsregisters~~ Auslagerungsmanagementsystem der ZAM eG
1.3	entfällt		~~Definition und Bereitstellung von Ausstiegsprozessen bei Beendigung der Auslagerung (Exit Strategie), sofern keine Verbunderleichterungen nach MaRisk AT 9 Tz. 5 Erläuterungen greifen~~	~~Akzeptanz der definierten und vorgehaltenen Ausstiegsprozesse bei Beendigung der Auslagerung (Exit Strategie)~~

			Zuordnung ZAM eG	Zuordnung Institut / Auftraggeber
1.4			Benennung zuständiger Mitarbeiter pro Institut	Benennung Ansprechpartner im Institut
1.5			Aufbau eines Registers zur Erstellung und Pflege einer vollständigen Dokumentation der Auslagerungen (einschließlich Weiterverlagerungen) und sonstigen Fremdbezüge	Installation und Nutzung des Registers in der Bank, Berechtigungs- und Lizenzverwaltung, Eingabe und Pflege institutsindividueller Parameter ~~(z.B. Mangelkategorien der Internen Revision, OpRisk-Matrix, Prozesse)~~
1.6			Weiterverlagerungskette der F&G erstellen (Feststellen / Einfordern welche Prozesse und Arbeitsschritte weiterverlagert werden)	ggf. vertragliche Grundlagen zur Beauskunftung des Dienstleisters gegenüber der ZAM eG schaffen (sofern im Auslagerungsvertrag nicht bereits geschehen)
1.7			Erstellung einer jährlichen Gesamtberichterstattung	Berichtsempfang, Weiterverarbeitung/Kommunikation innerhalb der Bank
1.8			Aufbau und Pflege eines kontinuierlichen Berichtsprozesses - Sicherstellung ad hoc Berichte	Berichtsempfang, Weiterverarbeitung/Kommunikation innerhalb der Bank; Meldung von Sachverhalten, die eine ad-hoc-Berichterstattung auslösen, sofern es sich nicht um einen flächendeckenden Vorfall handelt
2	**Identifikation Auslagerungssachverhalte**	AT 9 TZ 1,12,13	Ableitung der von der F&G zur Verfügung gestellten Datensätze und Informationen in Bezug auf die genutzten Dienstleistungen / Produkte pro Bank	Initiale Angabe der genutzten Produkte und laufende Aktualisierung bei Änderungen, sofern diese durch den Dienstleister nicht zur Verfügung gestellt werden (können) über das Auslagerungsregister
3	**Risikoanalyse- und -bewertung**	AT 9 TZ 2,3		

3.1			Entwurf einer institutsindividuellen Risikoanalyse	Überprüfung, Bearbeitung und Abschluss (insbesondere Beschluss) der institutsindividuellen Risikoanalyse auf Basis des vorgelegten Vorschlags, ggf. Anpassung im Auslagerungsregister.

			Zuordnung ZAM eG	**Zuordnung Institut / Auftraggeber**
3.2		MaRisk AT 9 TZ 2	anlassbezogene Analyse ggf. wg Schlechtleistung, Insolvenz, Feststellungen nach Berichtsauswertung etc.	Abschluss (insbesondere Beschluss) der institutsindividuellen Risikoanalyse auf Basis des vorgelegten Vorschlags, ggf. Anpassung
3.3		BAIT Modul 8	Risikobewertung zum sonstigen Fremdbezug erstellen	Abschluss (insbesondere Beschluss) der institutsindividuellen Risikoanalyse auf Basis des vorgelegten Vorschlags, ggf. Anpassung
3.4		BAIT Modul 8	anlassbezogene Bewertung ggf. wg. Schlechtleistung, Insolvenz, Feststellungen nach Berichtsauswertung (sonst. Fremdbezug)	Abschluss (insbesondere Beschluss) der institutsindividuellen Risikoanalyse auf Basis des vorgelegten Vorschlags, ggf. Anpassung
4	**Beurteilung der Leistungserbringung und Ableitung/ Durchführung Maßnahmen zur Risikosteuerung und -überwachung**	AT 9 TZ 9 bis 11		
4.1	Leistungsüberwachung gem. vertraglicher Vereinbarung		Aufnahme vertraglicher Leistungsparameter	Einlieferung Leistungsparameter, sofern diese durch den Dienstleister nicht zur Verfügung gestellt werden (können) ~~über das Auslagerungsregister~~
4.1.1.			Einfordern von Information über Entwicklungen, die die ordnungsgemäße Erledigung der ausgelagerten Aktivitäten	Hinweise zu möglichen Entwicklungen über das Auslagerungsregister~~s~~

			und Prozesse beeinträchtigen können	
4.1.2			wesentliche Störungen, Störungshäufungen beobachten, Banken begleiten	Sicherstellung der Weitergabe der Störungsmeldungen an die Fachbereiche der Bank, Information an ZAM sofern nicht über F&G gemeldet

			Zuordnung ZAM eG	**Zuordnung Institut / Auftraggeber**
4.2.1			ad hoc Eskalation bei größeren oder schwerwiegende Störungen	ggf. Mitwirkung
4.2.2			wesentliche Störungen im operativen Betrieb der Bank aufnehmen und Bearbeitung durch den Dienstleister begleiten und im Berichtswesen verwerten	Information an ZAM bei wesentlichen Störungen sofern nicht über F&G gemeldet
4.3	**Allgemeine SLA-Überwachung**			
4.3.1			SLA-Überwachung Standardprodukte	ggf. Mitwirkung, insbesondere Meldung von Verstößen
4.3.2			SLA-Überwachung Individualprodukte	ggf. Mitwirkung, insbesondere Meldung von Verstößen
4.3.3			regelmäßige Beurteilung der Leistung des Auslagerungsunternehmens anhand vorzuhaltender Kriterien	ggf. Mitwirkung, insbesondere Meldung von Verstößen

4.3.4			regelmäßige Beurteilung der Leistung des Auslagerungsunternehmens anhand vorzuhaltender Kriterien	ggf. Mitwirkung, insbesondere Meldung von Verstößen

			Zuordnung ZAM eG	**Zuordnung Institut / Auftraggeber**
5	**Berichtsauswertung der Dienstleister**	AT 9 TZ 9 bis 11		
5.1		SOIT Ka. 6.3 und 6.4	Ableitung von Anforderungen an die ~~Fiducia & GAD~~ F&G auf Basis der Beurteilung der Leistungserbringung, Auswertung von Berichten und Prüfungen sowie der Identifizierung von Incidents	Priorisierung und Freigabe von Anforderungsvorschlägen zur Befassung des Steuerungsgremiums

5.2			Berichtstypen auswerten: Risikobericht, Revisionsberichte. Berichte zur Prüfung nach IDW PS 951 n. F., Berichte 24c KWG, Berichte zur Prüfung des Bankverfahrens nach IDW PS 880, Berichte zur Prüfung weiterer Softwarekomponenten nach IDW PS 880, Berichte des Abschlussprüfers der F&G (zur Beurteilung der Funktionsfähigkeit der Internen Revision des Auslagerungsunternehmens), Ad-hoc Berichte, Datenschutzbericht, sonstige Berichte	ggf. Mitwirkung, insbesondere Kommunikation in der Bank und Umsetzung abgeleiteter Maßnahmen

			Zuordnung ZAM eG	**Zuordnung Institut / Auftraggeber**
5.3			Zeitgerechten Eingang der Berichte überwachen, ggf. F&G zur Zusendung auffordern	ggf. Mitwirkung
5.4			Rückfragen zu Berichten der F&G bearbeiten (unklare Berichtsaussagen,	ggf. Mitwirkung

			fehlende Informationen, etc.)	
5.5			Einfordern und Verfolgen der Feststellungen und Maßnahmen bei F&D	ggf. Mitwirkung
5.6			ggf. Adressaten differenzieren: Geschäftsführung Revision Risikocontrolling-Funktion Informationssicherheitsbeauftragter ~~Auslagerungsbeauftragter~~ MaRisk-Compliance-Beauftragter, Schnittstellenbeauftragter, soweit vorhanden	ggf. Mitwirkung
5.7			ausgewertete~~n~~ Berichte aufbereiten und an Banken weiterleiten	Entgegennahme Bericht; Kommunikation in der Bank und Umsetzung abgeleiteter Maßnahmen
6.	**Aufbereitung Risikomanagement**	MaRisk AT 7.2, BAIT	mögliche~~n~~ Auswirkungen von Auslagerungsvereinbarungen auf operationelles Risiko beschreiben	Entgegennahme, eigenständige Bewertung und Einphasung in das Risikomanagement der Bank
6.1			ggf. zusätzliche Risiken aus Weiterverlagerung aufnehmen	Entgegennahme, eigenständige Bewertung und Einphasung in das Risikomanagement der Bank

			Zuordnung ZAM eG	Zuordnung Institut / Auftraggeber
6.2			ggf. zusätzliche Risiken aus Berichtsfeststellungen aufnehmen	Entgegennahme, eigenständige Bewertung und Einphasung in das Risikomanagement der Bank
6.3			ggf. zusätzliche Risiken aus Schlechtleistung aufnehmen	Entgegennahme, eigenständige Bewertung und Einphasung in das Risikomanagement der Bank Meldung von Schadensfällen über Auslagerungsregister
6.4			OpRisk-Beschreibung als Vorschlag für indiv. Einwertung im Risikomanagement der Bank	Entgegennahme, eigenständige Bewertung und Einphasung in das Risikomanagement der Bank
6.5.			Risikoeinwertung überprüfen	
7	**Notfallmanagement**	MaRisk AT 7.3, AT 9 TZ. 6	Konzeptionelle Unterstützung bei der Methodik für Einbindung/ Berücksichtigung Dienstleister im Notfallkonzept auf Verbundebene, keine bankindividuelle Beurteilung	gegebenenfalls Mitwirkung, Verantwortung für das Notfallmanagement verbleibt in der Bank

			Zuordnung ZAM eG	Zuordnung Institut / Auftraggeber
8	**Interne Revision**	MaRisk BT 2.1 TZ 3, BT 2.3 bis 2.5, AT 9 TZ 2	Unterstützung der internen Revision der Banken	Ansprechpartner in der Internen Revision benennen

8.1			Unabhängige Berichtsauswertung der Berichtstypen F&G zur Unterstützung der IR der Banken. Folgende Berichte sind aus Revisionsgesichtspunkten auszuwerten: Berichte zur Prüfung nach IDW PS 951 n. F., Berichte 24c KWG, Berichte zur Prüfung des Bankverfahrens nach IDW PS 880, Berichte zur Prüfung weiterer Softwarekomponenten nach IDW PS 880, Berichte des Abschlussprüfers des Auslagerungsunternehmens (zur Beurteilung der Funktionsfähigkeit der Internen Revision des Auslagerungsunternehmens), Ad-hoc Berichte, Dienstleisterbericht, Datenschutzbericht, weitere Berichte	Entgegennahme und Verwertung der Berichtsauswertungen
8.2			Zeitgerechten Eingang der Berichte überwachen, ggf. F&G zur Zusendung auffordern	

			Zuordnung ZAM eG	**Zuordnung Institut / Auftraggeber**

8.3			Rückfragen zu Berichten der F&G bearbeiten (unklare Berichtsaussagen, fehlende Informationen, etc.)	
8.4			Einfordern und Verfolgen der Feststellungen und Maßnahmen bei F&G	Integration der Ergebnisse in das Follow-Up der Internen Revision
8.5			Feststellungen verfolgen, ggf. Adressaten differenzieren: Geschäftsführung Interne Revision Risikocontrolling-Funktion Informationssicherheitsbeauftragter ~~Auslagerungsbeauftragter~~ MaRisk-Compliance, Schnittstellenbeauftragter, soweit vorhanden	
8.6			ausgewertete~~n~~ Berichte aufbereiten und an Banken weiterleiten	Entgegennahme und Verwertung der Berichtsauswertungen
8.7			Ergänzungsprüfungen bei Bedarf planen und durchführen	ggf. Mitwirkung
9.	**Informationssicherheits- und -risikomanagement**	AT 7.2 i.V.m. BAIT	konzeptionelle Unterstützung bei Methodik für Schutzbedarfsanalyse und Soll-Ist Abgleich	verantwortlich für das Informationssicherheits- und –risikomanagement