D 7465

Zeitschrift für das gesamte
KREDITWESEN

78. Jahrgang · 1. Mai 2025

9-2025

Pflichtblatt der Frankfurter Wertpapierbörse
Fritz Knapp Verlag · ISSN 0341-4019

Digitaler Sonderdruck

Regulatorik und Bankenaufsicht

DORA: Vom Auslagerungsmanagement zum Drittparteienrisikomanagement

Kathrin Hellmich / Frank Mehlhorn / Olaf Rösener

Foto: pixabay.com

Kathrin Hellmich / Frank Mehlhorn / Olaf Rösener

DORA: Vom Auslagerungsmanagement zum Drittparteienrisikomanagement

Die Widerstandsfähigkeit des Finanzsektors im digitalen Betrieb zu erhöhen: Das ist das Ziel des Digital Operational Resilience Act – kurz DORA. Nach einer Vorbereitungszeit von knapp zwei Jahren ist die EU-Verordnung mit der formalen Bezeichnung 2022/2554 seit dem 17. Januar 2025 von einem Großteil der Institute in Europa anzuwenden.[1)]

Neben der Verordnung gibt es weitere Durchführungsstandards sowie gemeinsame Leitlinien (Level 2 und 3) der europäischen Aufsichtsbehörden, welche die Anforderungen unter anderem an das Drittparteienrisikomanagement weiter konkretisieren.

Eine große Neuerung von DORA besteht darin, die derzeitigen Schutzmechanismen der Finanzunternehmen und deren wesentliche IT-Drittanbieter in ein koordiniertes Sicherheitssystem einzubetten, das die digitale Betriebsstabilität im Finanzsektor erhöht.

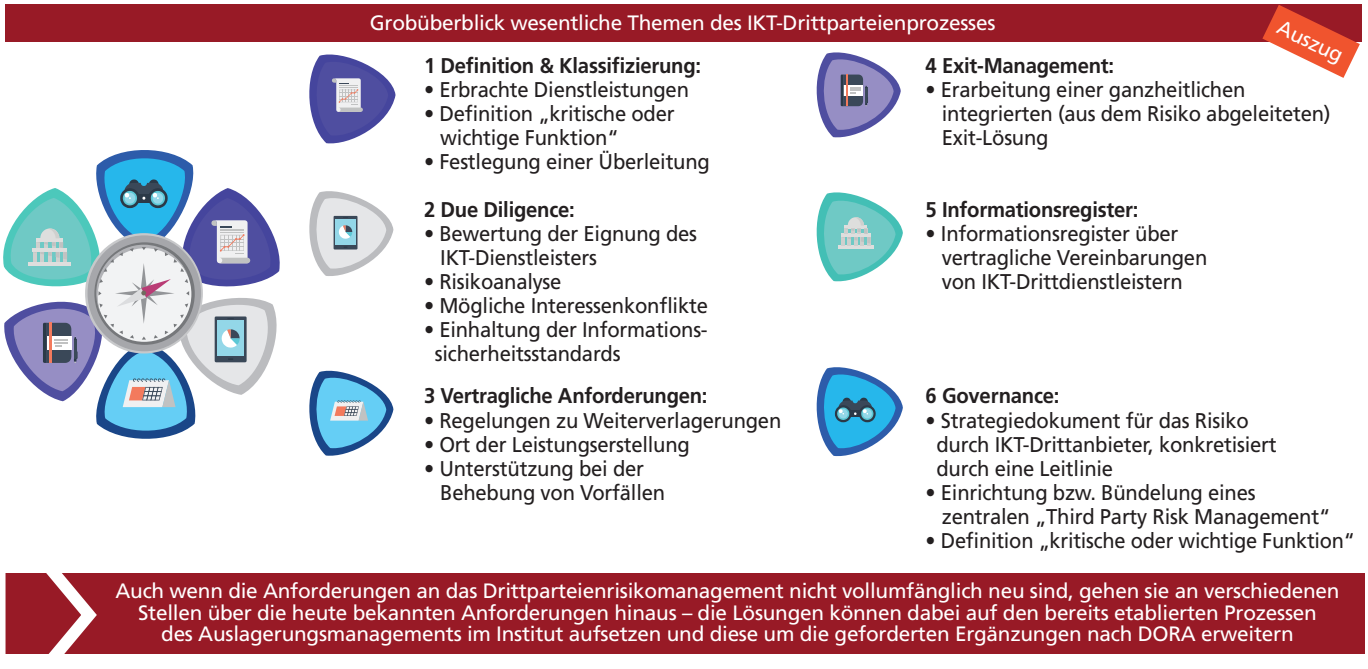
Denn Finanzunternehmen und ihre Dienstleister sind in der heutigen digitalen Welt so stark miteinander verflochten, dass Ausfälle auch über Unternehmensgrenzen hinweg Auswirkungen haben können. Der koordinierte Schutz soll unter anderem den erhöhten Anforderungen zum Schutz gegen Cyberangriffe genügen.

DORA ist auch Bestandteil des EBA-Jahresarbeitsprogramms sowie der EZB-Prioritäten für 2025. In diesen werden die strategischen Schwerpunkte und Initiativen für das jeweilige Jahr festgelegt und unter anderem die Aufsichts- und Überwachungstätigkeiten zu DORA reflektiert.

Im Blickpunkt der nationalen Aufsicht

Darüber hinaus steht das Thema in diesem Jahr auch im Blickpunkt der nationalen Aufsicht. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat

Abbildung 1: Grobüberblick wesentliche Themen des IKT-Drittparteienprozesses



Quelle: KPMG

für 2025 sechs Hauptrisiken für den Finanzsektor identifiziert. Sie hat zu jedem Risiko ihre Gegenmaßnahmen dargelegt. Eines dieser Risiken ist das aus Konzentrationen bei der Auslagerung von IT-Dienstleistungen und eine Maßnahme besteht in der Analyse der durch die Institute erstmals einzureichenden Informationsregister. Diese Register sind von weniger bedeutenden Instituten (less significat institutions, im Folgenden LSI) bis zum 28. April 2025 bei der BaFin einzureichen und von bedeutenden Instituten (SIs) bis zum 30. April 2025 bei der Europäischen Zentralbank.

Gemäß der Aufsichtsmitteilung der BaFin[2] vom Mai 2024 ergänzt DORA die bestehenden Regelungen zu Auslagerungen (zum Beispiel EBA-Leitlinien zu Auslagerungen, MaRisk). Diese Auslagerungsanforderungen sind nach wie vor zu beachten. Somit besteht aktuell eine gewisse Form der Doppelregulierung und es gelten zudem in Teilen unterschiedliche aufsichtliche Anforderungen, da IKT-Drittdienstleistungen oft auch Auslagerungen sind.

LSI müssen beispielsweise weiterhin für Auslagerungen das Auslagerungsregister und bei IKT-Drittdienstleistungen zusätzlich das Informationsregister befüllen. Die international von der EZB beaufsichtigen SIs wurden Anfang des Jahres darüber informiert, dass die Meldung über die Datenerhebung zu Auslagerungsvereinbarungen an die Europäische Zentralbank aufgehoben wurde. Es ist davon auszugehen, dass die EZB künftig das Informationsregister um Auslagerungsvereinbarungen, bei denen es sich nicht um IKT-Drittdienstleistungen handelt, erweitern wird.

Wenngleich auch die gesamten DORA-Anforderungen bereits seit Mitte Januar 2025 anzuwenden sind, sieht auch die Aufsicht Herausforderungen, die neuen Anforderungen umzusetzen und das vor allem beim Management des IKT-Drittparteienrisikos.[3] Das entspricht auch der Marktwahrnehmung der Autoren, wonach sich Institute aktuell weiterhin in der abschließenden Umsetzung der IKT-Drittparteienrisikomanagementanforderungen befinden (zum Beispiel durch die Anforderungen an die Integration bestimmter Mindestinhalte in die vertraglichen Vereinbarungen). Es sollte für die möglicherweise noch ausstehenden Aktivitäten zur Herstellung der regulatorischen Konformität in jedem Falle ein sogenannter Abarbeitungsplan vorliegen, der klare Meilensteine unter Angabe von Terminen und Verantwortlichkeiten für noch laufende Aktivitäten fixiert.

Drittparteienrisikomanagement nach DORA

Im Folgenden werfen die Autoren einen Blick auf ausgewählte wichtige Anforderungen zum IKT-Drittparteienrisikomanagement nach DORA und mögliche Weiterentwicklungen des Auslagerungsmanagements. Die aufsichtsrechtliche Klassifizierung von Fremdbezügen von IKT-Drittparteien nach Risikogehalt spielt hierbei für die anzuwendenden Überwachungspflichten eine zentrale Rolle.

Abbildung 1 bringt die wesentlichen Themen des IKT-Drittparteienprozesses in den Überblick. Ergänzungen dazu liefert die Übersicht der Dokumentationsanforderungen auf der BaFin-Homepage zu DORA, die zusätzlich auch Schlüsselprinzipien für ein solides Management des IKT-Drittparteienrisikos aufführt.[4]

IKT-Drittdienstleistungen können zum Beispiel kritische oder wichtige Funktionen unterstützen. Welche das sind, muss gemäß der DORA-Vorgaben auf Institutsebene definiert werden. So ist davon auszugehen, dass in vielen Fällen der Zahlungsverkehrsprozess eine kritische oder wichtige Funktion bei den Kreditinstituten darstellt. Damit verbundene Drittdienstleistungen, die diesen Prozess umfänglich erbringen, dürften also als kritisch und wichtig einzustufen sein. Ferner kann es sich bei IKT-Drittdienstleistungen zusätzlich um eine nicht wesentliche oder wesentliche Auslagerung handeln. Institute müssen ihre Klassifizierungslogik anpassen, um zu bestimmen, ob es sich bei der durch einen Dritten erbrachten Leistung um einen sonstigen Fremdbezug ohne IT-Bezug (sFB), eine IKT-Drittdienstleistung mit oder ohne Unterstützung kritischer oder wichtiger Funktionen handelt und gegebenenfalls

Kathrin Hellmich

Senior Manager, KPMG AG Wirtschaftsprüfungsgesellschaft, Financial Services, Frankfurt am Main

Frank Mehlhorn

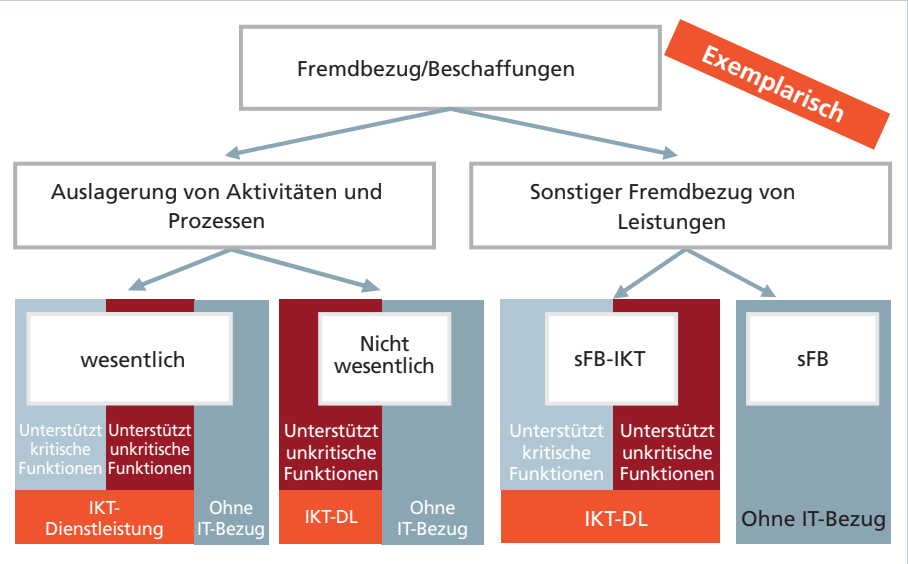
Director Bankenaufsicht, Bundesverband deutscher Banken e.V., Berlin

Olaf Rösener

Senior Manager, KPMG AG Wirtschaftsprüfungsgesellschaft, Financial Services, Essen

Der Digital Operational Resilience Act (DORA) verlangt nicht nur ein stringentes Drittparteienrisikomanagement, sondern hebt insbesondere die Anforderungen an IT-Dienstleister, Vertragsgestaltung, Governance und Überwachung auf ein neues Level. Für Banken bedeutet das: Doppelregulierung, neue Informationsregister, tiefgreifende Prozessanpassungen und deutliche Kapazitätssteigerungen – vor allem bei kritischen IKT-Drittdienstleistungen. Auch die BaFin und die Europäische Zentralbank nehmen 2025 verstärkt das Drittparteienrisiko in den Fokus – inklusive Meldepflichten und Governance-Anforderungen für Institute jeder Größenordnung. Die Umsetzung ist komplex, aber unverzichtbar. Warum sich gerade jetzt ein klarer Abarbeitungsplan, strategische Priorisierung und der Aufbau schlanker digitaler Steuerungslösungen auszahlen, zeigt der Beitrag im Detail. (Red.)

Abbildung 2: Einstufung beziehungsweise Klassifizierung von Fremdbezügen



sFB = sonstiger Fremdbezug

Quelle: KPMG

zusätzlich um eine IT-Auslagerung oder eine Auslagerung ohne IT-Bezug.

Diese Einstufung beziehungsweise Klassifizierung von Fremdbezügen wird durch die beispielhafte Abbildung 2 veranschaulicht.

Es sei jedoch darauf hingewiesen, dass Definitionen von „kritischen oder wichtigen Funktionen" und der „Wesentlichkeit" voneinander abweichen, da sich die anzulegenden Kriterien unterscheiden. Daher kann nach Veröffentlichungen der BaFin nicht pauschal von einer Kategorie in die andere übergeleitet werden.[5)]

In Abhängigkeit von der vorgenommenen Klassifizierung sowie der anschließenden Risikoanalyse sind entsprechende regulatorische Mindestanforderungen unter anderem an die Überwachung und Vertragsgestaltung zu erfüllen.

Due Diligence mit Blick auf IKT weiterentwickeln

Während in den Mindestanforderungen an das Risikomanagement (MaRisk) bei Auslagerungen Due-Diligence-Anforderungen nicht explizit genannt sind, sondern in die Durchführung der Risikoanalyse eingehen, muss bei dem jeweiligen IKT-Drittdienstleister, wie auch in den aktuellen EBA-Leitlinien zu Auslagerungsvereinbarungen genannt, vor dem Abschluss einer vertraglichen Vereinbarung dessen Eignung sichergestellt werden. Für SI sollten bereits etablierte Due-Diligence-Prozesse vorhanden sein, die gegebenenfalls mit Blick auf IKT weiterzuentwickeln sind. Für LSI könnte dahingehend ein Handlungserfordernis bestehen, entsprechende Prozesse neu einzurichten oder weiterzuentwickeln.

Da es sich bei IKT-Drittdienstleistungen in den bisherigen Regulierungen in Teilen nicht um IT-Auslagerungen, sondern um „sonstigen Fremdbezug von IT-Dienstleistungen" handelt, dürfte diese formale Due-Diligence-Anforderung für alle Institute in der Regel ein zu überprüfender oder anzupassender Prozessschritt darstellen.

Bis zu ihrer Aufhebung im Januar 2025 waren die Anforderungen zum sonstigen Fremdbezug von IT-Dienstleistungen in den BAIT geregelt. Und auch nach DORA müssen weiterhin Risikobewertungen/-analysen für IKT-Drittdienstleistungen durchgeführt werden. Formal gesehen gab es laut BAIT bislang keine Mindestanforderungen zu Risikofaktoren. Hingegen beinhalten die EBA-Leitlinien zu Auslagerungsvereinbarungen und MaRisk jeweils Mindestanforderungen an Risikofaktoren, welche im Zusammenhang mit einer Risikoanalyse zu betrachten sind (zum Beispiel politische Risiken, Schutzbedarf). Das hat zur Folge, dass Institute ihre bisherige Risikobewertung nach BAIT oder ihre Risikoanalyse für Auslagerungen entsprechend der neuen DORA-Vorgaben etwa um das Konzentrationsrisiko und Weiterverlagerungsrisiko überprüft und, falls nötig, erweitert haben.

Für kritische oder wichtige IKT-Drittdienstleistungen müssen nach Maßgabe von DORA auch Geschäftsfortführungspläne (Exit-Management) definiert werden. Die bisherige in den MaRisk genannte Erleichterung, wonach ein Verzicht von Ausstiegsprozessen bei gruppeninternen Auslagerungen möglich ist, entfällt. Laut den BaFin-FAQs zu DORA sind jedoch insofern Erleichterungen im Rahmen der Proportionalität möglich, wenn das Risiko in diesen Konstellationen verringert ist, etwa durch umfassendere Durchgriffs- oder Kontrollmöglichkeiten für die Institute. In den EBA-Leitlinien zu Auslagerungsvereinbarungen gibt es diese Erleichterung, bei gruppeninternen Auslagerungen nicht.

In Teilen Anpassungsbedarf bei Kreditinstituten

Des Weiteren unterscheiden sich die Anforderungen an ein Testing von Exit-Plänen, gemäß der EBA-Leitlinien zu Auslagerungen und den MaRisk: Während die EBA-Leitlinien ein erforderliches Testing adressieren, gehen die MaRisk an dieser Stelle nicht explizit darauf ein. Institute, die das Testing bereits in ihren Arbeitsprozessen integriert haben, können diese Prozesse gemäß DORA-Anforderungen nutzen. Institute, die im Schwerpunkt auf die MaRisk abgestellt haben, müssen weitergehende Prozessschritte etablieren. Beobachtungen[6)] zeigen, dass Kreditinstitute in Teilen Anpassungsbedarf in der Umsetzung von Exit-Management-Anforderungen besitzen.

Ein weiterer wesentlicher neuer Aspekt umfasst die DORA-Anforderungen an die

Vertragsgestaltung und das Vertragsmanagement. Diese bewirken einen erheblichen Umsetzungsaufwand, nicht zuletzt auch deshalb, da die DORA-Anforderungen oft dazu führen, neue Verträge mit den jeweilig bestehenden IKT-Dienstleistern zu schließen. Insbesondere führten die bisherigen bankaufsichtlichen Vorgaben in der Regel nicht zu so detaillierten vertraglichen Anforderungen, um den IT-Fremdbezug oder nicht wesentliche IT-Auslagerungen zu regeln.

Die in der Organisationsstruktur überwiegend verankerte dezentrale Steuerung und die dazugehörige Dokumentation der IKT-Dienstleistungen erfolgt auch nach DORA weiter risikobasiert. Wie bei wesentlichen Auslagerungen müssen bei kritischen oder wichtigen IKT-Drittdienstleistungen beispielsweise auch Leistungsindikatoren (Key Performance Indikatoren, KPIs) sowie Maßnahmen bei Schlechtleistung definiert werden. Gemäß Marktbeobachtung ist der Aufwand bei einer kritischen oder wichtigen IKT-Dienstleistung grundsätzlich mit dem Überwachungsaufwand einer wesentlichen Auslagerung vergleichbar.

Ferner ist das Informationsregister nach DORA hinsichtlich der inhaltlichen DORA-Anforderungen deutlich umfangreicher, als das weiterhin für LSI relevante Auslagerungsregister nach MaRisk. Es umfasst rund 110 Datenfelder (im Vergleich zu 70 Datenfeldern des Auslagerungsregisters). Dabei sollten Institute Prozesse einrichten, die gewährleisten, dass die Daten zum Drittparteienrisiko vollständig und aktuell sind. Damit verbunden ist auch das Einrichten von Prozessen, welche die Einreichungs- und Anzeigepflichten sicherstellen.

Abbildung 3 zeigt Gemeinsamkeiten und Unterschiede des Auslagerungs- und Informationsregisters auf.

Hinsichtlich der Governance zum Drittparteienrisikomanagement lässt sich feststellen, dass die Anforderungen gemäß DORA weiter zunehmen. So fällt insbesondere der Geschäftsleitung eine noch stärkere (aktive) Verantwortung im Hinblick auf die Überprüfung der Risiken von IKT-Drittdienstleistungen, auf Basis einer Bewertung des Gesamtrisikoprofils, des Umfangs und der Komplexität der Unternehmensdienstleistungen, zu. Damit die Leitungsorgane ihrer Verantwortung nachkommen können, sind bisherige Meldekanäle[7)] an die Geschäftsleitung neu auszurichten und mindestens um IKT-relevante Informationen zu erweitern. Beispielsweise sind Vereinbarungen über die Nutzung von IKT-Drittdienstleistungen in die Berichtspflicht an die Geschäftsleitung zu inkludieren.

Gestiegene Anforderungen an die Governance

Ein weiterer Aspekt, der die gestiegenen Anforderungen an die Governance reflektiert, ist die erforderliche Genehmigung und Überprüfung der bankinternen Leitlinie für die Nutzung von IKT-Drittdienstleistern durch die Geschäftsleitung. Diese Anforderung ist zwar bereits Bestandteil der EBA-Leitlinien zur Auslagerung, gelangt aber durch DORA als Level-1- und Level-2-Vorgaben eine erhöhte Bedeutung. Ergänzend sei darauf verwiesen, dass die BaFin in ihren Aufsichtsprioritäten für 2025 erneut das Themenfeld Governance adressiert hat. Während es für Auslagerungen bereits die Anforderung gibt, Auslagerungsziele in einer Auslagerungsstrategie festzulegen, müssen die Institute ihre vorhandenen Auslagerungsstrategien um das IKT-Drittparteienrisiko ergänzen. Es ist zu beobachten, dass einige Institute auch eine separate IKT-Drittparteienrisiko-Strategie erstellen oder in der DOR-Strategie entsprechende Ergänzungen vorgenommen haben.

Abbildung 3: Grundlegende Anforderungen des Informationsregisters – Vergleich zum Auslagerungsregister

	Auslagerungsregister	Informationsregister
Umfang	Übersicht aller Auslagerungssachverhalte	Übersicht aller IKT-Dienstleistungen (sFB-IT sowie Auslagerungen)
Anzahl der Datenfelder und Inhalt der Register	70 Datenfelder Primär Informationen zum Dienstleister	102 (+19 Definitions-)Datenfelder Information des Dienstleisters + Interne Informationen des Instituts
Grob -Überblick regulatotorische Anforderugen	EBA/GL/2019/02 – Kapitel 11 - Nr. 52-60 AT 9 Tz.14 MaRisk § 24 Abs. 1 Nr. 19 KWG § 3 AnzV	Art. 28 Nr. 3 DORA JC 2023 85 – ITS on Register of Information
Pflicht zur Vorlage	Jährlicher Turnus	
Einreichungsart der Meldungen	Jährlich: Meldung erfolgt für LSIs an die BaFin (MVP-Portal), für SIs an die EZB (Casper Portal) Ad hoc: Meldung erfolgt für LSIs an die BaFin (MVP-Portal), für SIs an die EZB (IMAS-Portal)	

Quelle: KPMG

Darüber hinaus haben Kreditinstitute bereits begonnen, die Organisationsrichtlinien zu erweitern und das Management von IKT-Drittparteien entlang des gesamten Lebenszyklus zu etablieren: von der Klassifizierung, der Due Diligence, der Risikoanalyse und -bewertung über die Vertragserstellung, dezentrale Kontrollaktivitäten, zentrale Überwachungsaktivitäten, Geschäftsfortführungspläne, Informationsregister und Anzeigepflichten bis hin zur Beendigung von Verträgen, einschließlich dem Vorhalten von Dokumenten und Informationen zu den Verträgen für eine eventuelle spätere aufsichtliche Prüfung.

Ähnlich wie die Einrichtung eines zentralen Auslagerungsbeauftragten oder eines zentralen Auslagerungsmanagements müssen Institute eine Funktion zur Überwachung der IKT-Dienstleistungen einrichten. Die Autoren beobachten, dass ein Großteil der Institute plant, diese Second-Line-of-Defense-(2LoD)-Funktion zur Überwachung des IKT-Drittparteienrisikos dem zentralen Auslagerungsbeauftragten oder dem zentralen Auslagerungsmanagement zuzuordnen.

Überwachungsaktivitäten innerhalb der Kreditinstitute nehmen zu

Die Autoren stellen auch fest, dass Kreditinstitute weiter die Möglichkeit nutzen, den risikobasierten Ansatz bei der Überwachung von IKT-Drittdienstleistern, den auch DORA gewährt, anzuwenden. Gleichwohl nehmen aufgrund von DORA die Überwachungsaktivitäten innerhalb der Kreditinstitute insbesondere für jene IKT-Dienstleistungen zu, die bisher keine Auslagerungen waren. Denn es hat beispielweise eine regelmäßige Pflege und Qualitätssicherung des Informationsregisters zu erfolgen. Eine Konsequenz daraus ist, dass Institute, in Abhängigkeit der identifizierten wichtigen oder kritischen IKT-Drittdienstleistungen, die zuvor keine wesentlichen Auslagerungen waren, in Teilen die Mitarbeiterkapazität signifikant erhöhen oder das zumindest planen.

Folgende Aspekte beeinflussen die Aufgaben und unter Umständen auch die Kapazitäten, um die Anforderungen an die Einhaltung sicherzustellen sowie eine erforderliche Überwachung zu gewährleisten:

- Abgrenzung von Aktivitäten, Aufgaben und Arbeitsschritten zwischen zentraler Funktion und dezentral Verantwortlichen,
- Komplexität der Prozesse und der Organisation, beim Bezug von Dienstleistungen und Produkten,
- Automatisierungsgrad des Kreditinstituts und des Vertragspartners,
- Reifegrad der IT-Landschaft, bestehenden aus Netzwerk, Applikationen, Tools und entsprechenden Zugriffsrechten,
- Synergien innerhalb einer Institutsgruppe oder unter Nutzung von Verbünden mit anderen Instituten.

Die dargestellten Faktoren haben Auswirkungen auf das Drittparteienrisikomanagement und somit auf den Arbeitsaufwand und möglichen zusätzlichen Bedarf an Mitarbeitenden – neben der reinen Anzahl und Komplexität der Auslagerungen sowie der Anzahl und Art der IKT-Drittdienstleistungen.

Nach der Beobachtung der Autoren liegt die Bandbreite des zusätzlichen Bedarfs an Fachkräften, im zentralen Auslagerungsmanagement und der Überwachungsfunktion nach DORA, bei bis zu 100 Prozent. Die Bandbreite bezieht sich hierbei auf sehr kleine Institute, mit sehr wenigen Auslagerungen, mittelgroße Institute sowie auf sehr große Institute, die sowohl ein Nearshoring als auch ein Offshoring betreiben.

Steigender prozessualer Aufwand

Die Autoren gehen davon aus, dass der prozessuale Aufwand im Rahmen der Steuerung und Überwachung durch die DORA-Einführung im Drittparteienrisikomanagement deutlich steigen wird – unabhängig vom Grad der Digitalisierung etwa durch digitale Workflow-Lösungen. Dies zeigt sich gemäß Marktbeobachtungen einerseits im Personalaufbau der Überwachungsfunktionen zum Drittparteienrisikomanagement sowie andererseits im gestiegenen Bedarf der Kreditinstitute und Dienstleister, Fachwissen aufzubauen.

Es ist zu erwarten, dass die DORA-Anforderungen zu Anpassungen an den EBA-Leitlinien zu Auslagerungen führen werden. Diese sollen zudem in EBA-Leitlinien zum Drittparteienrisiko umbenannt werden. Die Konsultation des Entwurfs erfolgt voraussichtlich Ende Juni 2025. Für alle LSI ist die Anpassung an den MaRisk und somit die Transformation in die nationale Verwaltungspraxis abzuwarten.

Das Management von IKT-Risiken steht klar im Blickpunkt der Aufsicht. So werden auch Entwicklungen wie verstärkt auftretende Cyberangriffe und der fortschreitende Einsatz von künstlicher Intelligenz (KI) die Institute veranlassen, das IKT-Drittparteirisikomanagement angemessen und wirksam umzusetzen sowie fortlaufend weiterzuentwickeln. Das wird zur Folge haben, dass die Institute eine effiziente digitale Workflow-Lösung zum Drittparteienrisikomanagement benötigen.

In einem nächsten Artikel sollen die wesentlichen Anforderungen und Herausforderungen der neuen beziehungsweise geänderten EBA-Leitlinien zum Drittparteienrisiko vorgestellt werden.

Fußnoten

1) Für einige Finanzdienstleister, zum Beispiel Finanzierungsleasing- und Factoringinstitute und Kryptowertpapierregisterführer sowie Zweigstellen nach § 53 KWG, gibt es eine Übergangsfrist. Sie müssen DORA erst vom 1. Januar 2027 an vollständig anwenden.
2) Aufsichtsmitteilung „Umsetzungshinweise zur DORA-Implementierung“, BaFin, Mai 2024
3) Siehe BaFin-Homepage zu DORA, Fachartikel Vorbereitung auf DORA: Zacken zugelegt“, Frage zu „Sind denn jetzt alle Unternehmen wirklich startklar?“ an Herrn Obermöller, Gruppenleiter der BaFin-IT-Aufsicht vom 17.01.2025
4) Link: BaFin - News & Maßnahmen - Dokumentationsanforderungen nach DORA leicht(er) gemacht
5) Siehe Fragen und Antworten zum Management des IKT-Drittparteienrisiko auf der BaFin-Homepage zu der Frage „Sind kritische oder wichtige Funktionen i.S.d. Art. 3 Nr. 22 DORA immer auch wesentliche Auslagerungen und umgekehrt?“
6) Marktbeobachtungen ergeben sich aus Experteninterviews des Bankenverbandes mit seinen Mitgliedern und Projekterfahrungen der KPMG.
7) Siehe Governance und Organisation, Art. 5 Abs. 2i) DORA