Prof. Dr. Andreas Igl
TH Deggendorf

Auswirkungen der neuen EBA-Guidelines zum Third-Party Risk Management auf das Auslagerungsmanagement deutscher Kreditinstitute im Zusammenspiel mit DORA und MaRisk

Deggendorfer Notiz 2025/06 | Juli 2025

Einleitung

Die regulatorischen Anforderungen an das Management von Drittparteirisiken und Auslagerungen befinden sich derzeit im Umbruch. Die Veröffentlichung der Konsultationsfassung der neuen *Guidelines on the sound management of third-party risk* durch die Europäische Bankenaufsichtsbehörde (EBA) am 8. Juli 2025 markiert einen Wendepunkt in der europäischen Governance der Auslagerungen an Dritte. Diese neuen Leitlinien konkretisieren und ersetzen teilweise die bisherigen EBA-Guidelines zum Outsourcing aus dem Jahr 2019. Ihre Einbettung erfolgt im Rahmen der umfassenderen europäischen Regulierungsinitiative zur Stärkung der digitalen Resilienz des Finanzsektors, insbesondere durch die *Digital Operational Resilience Act (DORA)*-Verordnung (EU) 2022/2554.

Während DORA seit dem 17. Januar 2025 in vollem Umfang gilt und auf die Steuerung und Kontrolle von *IKT-Drittparteien* (IKT = Informations- und Kommunikationstechnologie) abzielt, fokussieren die neuen EBA-Guidelines nun explizit auf *nicht-IKT-bezogene Drittparteien*, insbesondere im Kontext der Erbringung kritischer oder wichtiger Funktionen. Dadurch wird eine strukturelle Zweiteilung des Third-Party-Risk-Managements (TPRM) etabliert: IKT-bezogene Dienstleistungen unterliegen den Anforderungen der DORA-Verordnung, nicht-IKT-Dienstleistungen hingegen der neu entstehenden Guideline-Welt der EBA.

Dieser Paradigmenwechsel hat erhebliche Auswirkungen auf die deutschen Institute, deren bisherige Auslagerungsstrukturen auf der Verwaltungsvorschrift MaRisk – hier insbesondere auf Abschnitt AT 9 – beruhen. Nachfolgend werden die neuen regulatorischen Rahmenbedingungen entlang zentraler Themenfelder analysiert und in zwei komparativen Perspektiven diskutiert:

1. Vergleich der neuen EBA-Guidelines für *non-ICT-Dienstleister* mit den bestehenden DORA-Anforderungen für *ICT-Dienstleister*.

2. Vergleich der neuen EBA-Guidelines mit dem bestehenden nationalen Rahmen des MaRisk AT 9 für Auslagerungen.

Einordnung: Fragmentierung der Regulierungslandschaft

Seit der Einführung von DORA und der nun vorliegenden Konsultationsfassung der EBA-Guidelines liegt die Verantwortung für das Drittparteirisikomanagement auf zwei Ebenen: einerseits auf der europäischen Ebene (DORA + EBA-Guideline) und andererseits auf der nationalen Ebene (MaRisk AT 9). **Eine entscheidende Zäsur bildet die erstmalige formelle Trennung zwischen IKT- und non-IKT-Dienstleistern**. Damit wird die erste Entscheidung im Auslagerungsprozess zukünftig die Klassifizierung der Dienstleistung nach ihrem IKT-Bezug sein. Diese Trennung ist keineswegs trivial, sondern erfordert eine robuste Governance-Struktur, welche diese Unterscheidung konsistent und risikoorientiert im gesamten Institut operationalisiert.

Dabei wird auch der bisherige Fokus vieler Häuser auf lediglich zeitkritische Prozesse hinterfragt. Denn im Zentrum steht **nunmehr die Identifikation *kritischer oder wichtiger Funktionen*** – unabhängig davon, ob diese in operativer, strategischer oder technischer Hinsicht kritisch sind. Die Definition solcher Funktionen entwickelt sich damit zu einer strategischen Aufgabe, vergleichbar mit der Bedeutung der Risikoinventur im Risikomanagement. Die Ableitung aus dem Geschäftsmodell wird somit zur zentralen Grundlage für das neue Third-Party-Risk-Management-Regime.

Vergleich 1: EBA-Guideline (non-ICT) vs. DORA (ICT)

Die EBA-Guidelines konzentrieren sich auf die Verwaltung von Drittparteirisiken bei nicht-IKT-Dienstleistungen, während DORA ein umfassendes Rahmenwerk für das IKT-Drittparteirisikomanagement bereitstellt. Beide Regelwerke verfolgen das Ziel, die Resilienz von Finanzinstituten zu stärken, unterscheiden sich jedoch in ihrer Spezifität und methodischen Ausgestaltung.

Die **Risikoanalyse** ist ein zentraler Bestandteil beider Regelwerke. DORA fordert eine detaillierte Bewertung der IKT-spezifischen Risiken, einschließlich Cyberrisiken, Abhängigkeiten von Drittanbietern und potenziellen Kaskadeneffekten innerhalb der Lieferkette. Die EBA-Guidelines hingegen legen den Schwerpunkt auf allgemeine Risiken, die mit der Auslagerung kritischer oder wichtiger Funktionen verbunden sind, und betonen die Notwendigkeit einer umfassenden Due-Diligence-Prüfung vor Vertragsabschluss. Während DORA spezifische Kriterien für die Klassifizierung von IKT-Dienstleistungen vorgibt, sind die EBA-Guidelines flexibler und orientieren sich am Proportionalitätsprinzip, was kleineren Instituten entgegenkommt.

Im Bereich der **Überwachung** fordert DORA eine kontinuierliche Kontrolle der IKT-Dienstleister, einschließlich der Nutzung standardisierter Berichtsformate und der Durchführung von Stresstests. Die EBA-Guidelines sehen ebenfalls eine fortlaufende Überwachung vor, jedoch mit einem stärkeren Fokus auf die vertragliche Sicherstellung von Leistungskennzahlen und regelmäßigen Audits. Ein wesentlicher Unterschied liegt in der Verpflichtung nach DORA, ein zentrales IKT-Drittparteienregister zu führen, das detaillierte Informationen über alle IKT-Dienstleister enthält, während die EBA-Guidelines ein solches Register nur für kritische nicht-IKT-Dienstleistungen empfehlen.

Die **Auslagerungsverträge** müssen nach beiden Regelwerken klare Regelungen zu Leistungsumfang, Haftung und Beendigungsrechten enthalten. DORA legt jedoch zusätzlichen Wert auf IKT-spezifische Klauseln, wie etwa den Schutz sensibler Daten und die Einhaltung von Datenschutzvorschriften. Die EBA-Guidelines hingegen priorisieren die Flexibilität der Verträge, um unterschiedliche Arten von nicht-IKT-Dienstleistungen abzudecken.

Im **Risikomanagement** zeigt sich ein weiterer Unterschied. DORA verlangt die Integration des IKT-Drittparteirisikomanagements in das unternehmensweite Risikomanagement, einschließlich spezifischer Szenarioanalysen für IKT-Risiken. Die EBA-Guidelines betonen hingegen die Notwendigkeit eines ganzheitlichen Ansatzes, der alle Risiken einer Auslagerung umfasst, ohne spezifische Szenarien detailliert vorzuschreiben. Dies führt zu einer höheren Spezifität bei DORA, während die EBA-Guidelines breiter gefasst sind.

Die **Notfallplanung** ist in beiden Regelwerken von hoher Relevanz. DORA fordert detaillierte Notfall- und Wiederherstellungspläne, die spezifisch auf IKT-Störungen ausgelegt sind, einschließlich klar definierter Wiederherstellungszeiten (RTOs). Die EBA-Guidelines hingegen verlangen ebenfalls Notfallpläne, lassen jedoch mehr Spielraum für die Ausgestaltung, insbesondere bei nicht-kritischen Dienstleistungen.

Die **Berichterstattung** unterscheidet sich in ihrer Frequenz und Tiefe. DORA sieht regelmäßige Berichte an Aufsichtsbehörden vor, die detaillierte Informationen über IKT-Drittparteien enthalten. Die EBA-Guidelines fordern Berichterstattung primär im Kontext interner Governance-Strukturen, wobei die Anforderungen an die Häufigkeit weniger streng sind.

Die **Prüfungsrechte** sind in beiden Regelwerken verankert, jedoch mit unterschiedlichen Schwerpunkten. DORA betont die Notwendigkeit von Audits bei IKT-Dienstleistern, einschließlich der Möglichkeit, Dritte wie Subunternehmer zu prüfen. Die EBA-Guidelines sehen ähnliche Rechte vor, legen jedoch mehr Gewicht auf die vertragliche Absicherung dieser Rechte.

Das **Proportionalitätsprinzip** wird in beiden Regelwerken berücksichtigt, wobei DORA strengere Anforderungen an größere Institute stellt, während die EBA-Guidelines eine

flexiblere Anwendung ermöglichen, die an die Größe und Komplexität des Instituts angepasst ist.

Zusammenfassung:

Themenfeld	EBA-Guideline (non-ICT)	DORA (ICT)
Anwendungsbereich	Gilt für non-ICT-Dienstleister und deren Subunternehmer im Rahmen kritischer oder wichtiger Funktionen	Gilt für alle IKT-Dienstleister, inkl. kritischer IKT-Dienstleister gemäß Art. 31 DORA
Kritikalität	Ableitung über Geschäftsmodell, Fokus auf *kritische oder wichtige Funktionen*	Fokus auf *kritische oder wesentliche IKT-Dienste*, ergänzt um Klassifizierungen nach EBA Q&A
Vertragsanforderungen	Umfassende Anforderungen an Inhalte von Auslagerungsverträgen (z. B. Kontrollrechte, Unterbeauftragung etc.)	Sehr spezifische Anforderungen an SLAs, Exit-Strategien, Risikoübertragungsgrenzen
Informationsregister	Vorgabe zur Pflege eines *Informationsregisters* über alle Drittparteien	Verpflichtendes Informationsregister gemäß Art. 28 DORA mit Meldepflichten an Aufsicht
Monitoring & Kontrolle	Fortlaufendes Monitoring, angepasst an Proportionalitätsprinzip	Risikobasierte Steuerung durch KPIs, Resilienztests, IKT-Audits
Risikobewertung	Initiale und regelmäßige Risikobewertung bei Kritikalitätsveränderung	Eingebettet in ICT-Risikomanagementsystem gem. Art. 5 DORA
Notfallplanung	Fokus auf Business Continuity, aber weniger formalisiert	Umfassende Anforderungen an BCM, Redundanz, Wiederherstellungszeiten (RTO/RPO)
Meldepflichten	Indirekte Anforderungen über interne Berichterstattung	Direkte aufsichtsrechtliche Meldepflichten bei Incidents gem. Art. 19 DORA

Vergleich 2: EBA-Guideline (non-ICT) vs. MaRisk AT 9

Die MaRisk AT 9 bildet seit Jahren die Grundlage für das Auslagerungsmanagement in Deutschland und fokussiert sich auf die Übertragung von Aktivitäten oder Funktionen an Dritte. Die neuen EBA-Guidelines bauen auf diesen Anforderungen auf, bringen jedoch eine europäische Harmonisierung und einen stärkeren Fokus auf nicht-IKT-Dienstleistungen.

In der **Risikoanalyse** fordert MaRisk AT 9 eine umfassende Bewertung der mit einer Auslagerung verbundenen Risiken, insbesondere bei wesentlichen Auslagerungen. Die EBA-Guidelines gehen weiter und verlangen eine detaillierte Analyse der Risiken kritischer

oder wichtiger Funktionen, unabhängig von ihrer Wesentlichkeit im Sinne der MaRisk. Dies führt zu einer stärkeren strategischen Ausrichtung der Risikoanalyse.

Die **Überwachung** nach MaRisk AT 9 sieht eine kontinuierliche Kontrolle der ausgelagerten Aktivitäten vor, die durch interne Kontrollverfahren unterstützt wird. Die EBA-Guidelines ergänzen dies durch die Einführung von standardisierten Leistungskennzahlen und regelmäßigen Audits, die eine einheitlichere Überwachung auf europäischer Ebene ermöglichen.

Die **Auslagerungsverträge** nach MaRisk AT 9 müssen klare Regelungen zu Leistungsumfang, Haftung und Prüfungsrechten enthalten. Die EBA-Guidelines spezifizieren diese Anforderungen weiter, indem sie zusätzliche Klauseln zur Sicherstellung der Dienstleistungsqualität und zur Flexibilität der Verträge vorschreiben.

Im **Risikomanagement** fordert MaRisk AT 9 die Einbindung der Auslagerungsrisiken in das unternehmensweite Risikomanagement, ohne jedoch spezifische Szenarien detailliert vorzugeben. Die EBA-Guidelines betonen die Notwendigkeit eines ganzheitlichen Ansatzes, der alle Risiken einer Auslagerung umfasst, und legen mehr Gewicht auf die strategische Bedeutung der Risikobewertung.

Die **Notfallplanung** ist nach MaRisk AT 9 ebenfalls vorgeschrieben, mit einem Fokus auf die Sicherstellung der Geschäftskontinuität bei Störungen. Die EBA-Guidelines ergänzen dies durch detailliertere Anforderungen an die Ausgestaltung von Notfallplänen, insbesondere bei kritischen Dienstleistungen.

Die **Berichterstattung** nach MaRisk AT 9 umfasst regelmäßige Berichte über den Status und die Risiken der Auslagerung, die primär intern genutzt werden. Die EBA-Guidelines fordern eine strukturiertere Berichterstattung, die auch für aufsichtsrechtliche Zwecke genutzt werden kann.

Die **Prüfungsrechte** sind in beiden Regelwerken verankert, wobei die EBA-Guidelines eine stärkere Betonung auf die vertragliche Absicherung und die Durchführung von Audits bei Subunternehmern legen.

Das **Proportionalitätsprinzip** wird sowohl in der MaRisk als auch in den EBA-Guidelines berücksichtigt, wobei die EBA-Guidelines eine flexiblere Anwendung ermöglichen, die besser an die Vielfalt europäischer Institute angepasst ist.

Zusammenfassung:

Themenfeld	EBA-Guideline (non-ICT)	MaRisk AT 9 (bestehende Version)
Funktionale Ausrichtung	Ableitung aus kritischen/wichtigen Funktionen; organisatorische Trennung von ICT/non-ICT	Fokus auf "Auslagerung" als Begriff; differenziert weniger stark nach IKT-Bezug
Begriffsdefinitionen	Neue Definitionen für „third-party arrangements“, inklusive Subdienstleister	Begriff der "Auslagerung" mit teilweise enger Auslegung
Auslagerungsverantwortung	Klare Verantwortlichkeiten für jede Drittparteienbeziehung	Zentraler Auslagerungsverantwortlicher, meist im Bereich Organisation oder Risikomanagement
Kontrollverfahren	Risikobasierte Kontrollsysteme, gestützt durch Kontinuitätsplanung und Due Diligence	Kontrollen vorgeschrieben, aber weniger formalisierte Verfahren
Vertragliche Anforderungen	Konkrete Inhalte, insbesondere zu Auditrechten, KPIs und Steuerungsbefugnissen	Vorgaben vorhanden, aber Auslegungsspielräume bestehen (z. B. bei Prüfungsrechten)
Registerführung	*Informationsregister* über alle Drittparteien verpflichtend	*Auslagerungsregister* als Mindestanforderung, jedoch geringer Umfang
Berichtspflichten	Umfassende interne Berichterstattung über Status, Risiken und Maßnahmen	Regelmäßige Berichterstattung vorgesehen, jedoch ohne Vorgabe zur Tiefe der Inhalte
Proportionalitätsprinzip	Ausgeprägt, abgestuft nach Art der Funktion, Risiko und Vertragsstruktur	Grundsätzlich enthalten, aber selten konkret operationalisiert
Notfallplanung	Fokus auf Kontinuitätsfähigkeit auch bei non-ICT-Dienstleistern	Notfallplanung vor allem bei kritischen Auslagerungen, IKT-spezifische Aspekte fehlen

Zentrale Auswirkungen für Institute

Aus der Gegenüberstellung der Anforderungen ergibt sich für deutsche Kreditinstitute eine Reihe strategischer Implikationen:

1. **Veränderung der MaRisk AT 9 in naher Zukunft:** Es ist davon auszugehen, dass mit einer nächsten Novellierung der MaRisk die Anforderungen aus den EBA-Guidelines übernommen und angepasst werden. Damit verbunden ist eine stärkere Angleichung an europäische Vorgaben, was das bisherige Verständnis von "Auslagerung" erheblich erweitern wird.
2. **Initialentscheidung: ICT oder non-ICT:** Die zentrale Unterscheidung zwischen ICT- und non-ICT-Dienstleistern wird zur Weichenstellung im gesamten

Risikomanagement. Die DORA-Vorgaben bringen dabei klare Definitionen und Kriterien mit sich, die aufbauend auf EBA-Q&A zunehmend Anwendung in der Praxis finden.

3. **Fokus auf kritische/wichtige Funktionen:** Die neue Logik stellt nicht den Dienstleister oder Vertrag, sondern die durch ihn unterstützte Funktion in den Mittelpunkt. Diese wird entlang des Geschäftsmodells identifiziert und nicht – wie bisher häufig – nur anhand operativer oder zeitlicher Kritikalität. Die Definition solcher Funktionen muss daher auf Vorstandsebene verantwortet und dokumentiert werden.
4. **Risikoorientierung statt Rechtskategorie:** Die Einteilung der Auslagerung in zulassungspflichtige oder nicht-zulassungspflichtige Bereiche tritt in den Hintergrund. Entscheidend ist künftig die Risikobewertung der Funktion, unabhängig von der rechtlichen Einordnung.
5. **Professionalisierung der Steuerung und Berichterstattung:** Die bestehende Steuerung über Excel-basierte Dienstleisterverzeichnisse und sporadische Berichte genügt den neuen Anforderungen nicht mehr. Gefordert sind kontinuierliche Performance-Überwachung, strukturierte Risikoberichte und belastbare Exit-Strategien.

Fazit

Die neue EBA-Guideline in Verbindung mit DORA läutet eine neue Ära im Third-Party-Risk-Management europäischer Finanzinstitute ein. Sie führt zu einer tiefgreifenden Reorganisation der bestehenden Auslagerungsgovernance. Für deutsche Institute ergibt sich daraus nicht nur Anpassungsbedarf in den Prozessen und Systemen, sondern auch ein grundsätzlicher Wandel in der strategischen Risikosteuerung.

Insbesondere die klare Differenzierung zwischen IKT- und non-IKT-Dienstleistern sowie die auf Funktionen statt auf Verträge bezogene Risikobewertung erfordern eine neue Governance-Architektur. Die MaRisk AT 9 wird in dieser neuen Welt ihre Struktur und Ausrichtung verändern müssen. Für die Institute bedeutet dies, dass die bisherige, eher reaktiv-organisatorische Herangehensweise einem integrativen, risikoorientierten und strategisch verankerten Third-Party-Risk-Management weichen muss.

Prof. Dr. Andreas Igl
BDO-Stiftungsprofessor an der TH Deggendorf
Lehrbeauftragter an der Hochschule der Deutschen Bundesbank

andreas.igl@th-deg.de
(Mobil): 0151 2301 8610
(LinkedIn): Link