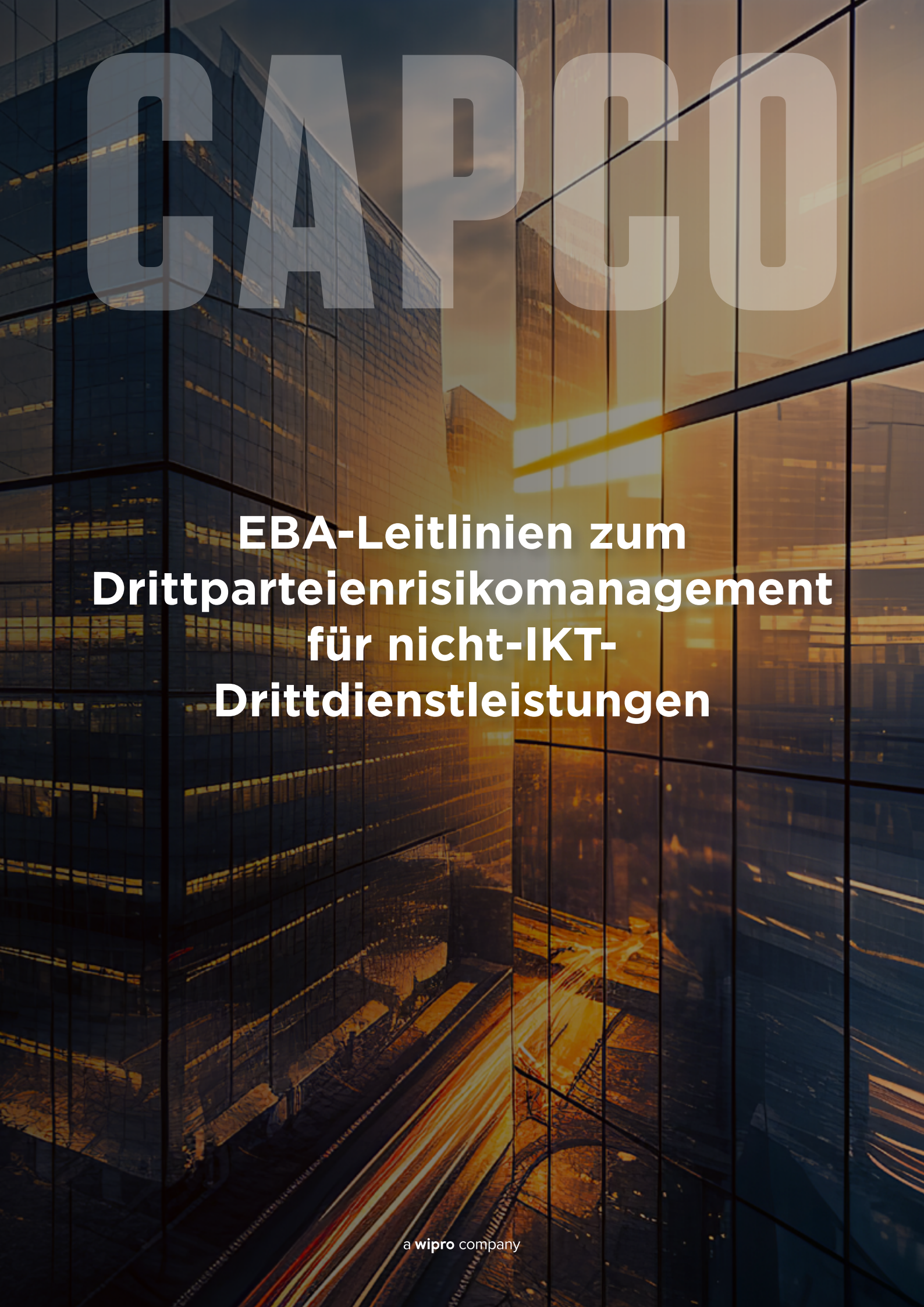

EBA-Leitlinien zum Drittparteienrisikomanagement für nicht-IKT-Drittdienstleistungen

a **wipro** company

Finanzunternehmen arbeiten zunehmend mit Drittanbietern zusammen, um Zugang zu spezialisiertem Fachwissen zu erhalten, Kosten zu senken sowie Skalierbarkeit und Effizienz zu erhöhen. Während dies eine stärkere Fokussierung auf die Kernaktivitäten ermöglicht, birgt die wachsende Abhängigkeit zu Drittanbietern zugleich erhebliche Risiken – sowohl für die Finanzunternehmen selbst als auch für deren Kunden und im Weiteren für das gesamte Finanzsystem.

Als Reaktion darauf eröffnete die Europäische Bankenaufsichtsbehörde (EBA) am 8. Juli 2025 eine Konsultation zu den Entwurfsleitlinien für das solide Management von Drittanbieterrisiken (die „Leitlinien"), die am 8. Oktober 2025 endete. Die Leitlinien sollen die EBA-Outsourcing-Richtlinien von 2019 ersetzen und einen harmonisierten EU-Rahmen für das Third-Party-Risikomanagement außerhalb des Informations- und Kommunikationstechnologie-Bereichs (Nicht-IKT) schaffen. Die Umsetzung soll innerhalb von zwei Jahren nach dem Prinzip „Comply or Explain" erfolgen. 1

Ziel der Leitlinien ist es, konsistente, effiziente und wirksame Aufsichtspraktiken zu fördern und gleichzeitig eine einheitliche Anwendung der EU-Vorschriften im gesamten Finanzsektor sicherzustellen. Sie ergänzen bestehende Rahmenwerke wie die Kapitaladäquanzrichtlinie (CRD) und die Richtlinie über die Sanierung und Abwicklung von Banken (BRRD). Insbesondere sind die Leitlinien mit dem Digital Operational Resilience Act (DORA) abgestimmt, der sich auf IKT-Drittparteirisiken konzentriert. Die Leitlinien harmonisieren Begriffe und Methoden, sodass Unternehmen Drittparteirisiken über den IKT-Bereich hinaus ganzheitlich steuern können. Sie spiegeln darüber hinaus internationale Standards des Financial Stability Board (FSB) sowie des Basler Ausschusses für Bankenaufsicht (BCBS) wider und tragen so zu globaler Konsistenz bei.

Die Leitlinien erweitern den Anwendungsbereich der EBA-Outsourcing-Richtlinien von 2019 deutlich: Betroffen sind nicht nur Kreditinstitute und Wertpapierfirmen, sondern auch Zahlungsverkehrs- und E-Money-Institute, Emittenten von Asset-Referenced Tokens sowie Hypothekengläubiger. Ausgenommen bleiben jedoch Kreditvermittler und Kontoinformationsdienstleister, die lediglich unter PSD2 (Anhang I, Dienst 8) registriert sind.

Die EBA-Leitlinien wurden so gestaltet, dass sie in Einklang mit DORA stehen, das den Fokus auf IKT-Drittparteirisiken legt und Terminologie sowie Praktiken harmonisiert. Damit Finanzunternehmen Drittanbieterrisiken auch jenseits des IKT-Bereichs ganzheitlich steuern können.

Marija Devic
Executive Director

1. https://www.eba.europa.eu/publications-and-media/press-releases/eba-launches-consultation-its-draft-guidelines-third-party-risk-management-regard-non-ict-related

Auswirkungen auf Unternehmen

Die Leitlinien erweitern die aufsichtliche Perspektive auf Drittanbieter erheblich. Unternehmen müssen ihre bestehenden Informationsregister erweitern, um alle Drittanbietervereinbarungen abzudecken – einschließlich solcher, die nicht im IKT-Bereich liegen und bisher meist nicht unter regulatorische Anforderungen fielen. Diese erweiterten Register sollen mit den DORA-Informationsregistern konsistent sein und ein vollständiges Inventar aller nicht-IKT-bezogenen Drittanbieterbeziehungen enthalten, inklusive:

- Dienstleistungsbeschreibung
- Kritikalität der Funktion
- Risikobewertung
- Abhängigkeiten von Subunternehmern

Die Bewertung der Verhältnismäßigkeit erfolgt parallel zur Identifizierung kritischer oder wichtiger Funktionen (Critical or Important Functions – CIFs). Damit wird sichergestellt, dass der Umfang der Aufsicht nicht nur die Bedeutung des Dienstes widerspiegelt, sondern auch dessen Komplexität, Austauschbarkeit und potenziellen Einfluss auf den Markt.

Finanzunternehmen müssen ihre Due-Diligence- und Onboarding-Prozesse stärken, um ein breiteres Spektrum an Risiken abzudecken. Neben operativen, rechtlichen und Continuity-Risiken müssen künftig auch Kredit-, Markt-, ESG- sowie Geldwäsche- und Terrorismusfinanzierungsrisiken berücksichtigt werden. Verträge mit nicht-IKT-Dienstleistern müssen überprüft und gegebenenfalls erweitert werden, um sicherzustellen, dass angemessene risikomindernde Klauseln enthalten sind – insbesondere bei Vereinbarungen, die CIFs unterstützen.

Ein besonderer Schwerpunkt der Leitlinien liegt auf der Überwachung von Konzentrationsrisiken, darunter:

- Abhängigkeit von einem schwer ersetzbaren Einzelanbieter oder Subunternehmer
- Parallele Verträge mit demselben oder eng verbundenen Anbieter/Subunternehmer

Betroffene Unternehmen müssen Ausstiegs- und Übergangsszenarien für kritische Dienstleister erstellen, testen und sicherstellen, dass Notfallmaßnahmen realistisch und umsetzbar sind.

Insgesamt markieren die Leitlinien einen Wandel hin zu einem ganzheitlicheren, prinzipienorientierten und risikosensiblen Ansatz, der Third Party-Risiken fest in dem Governance- und Resilienzrahmen von Unternehmen verankert.

Um die in den Leitlinien definierten Erwartungen zu erfüllen, müssen betroffene Unternehmen einen strukturierten und harmonisierten Ansatz für Drittparteirisiken verfolgen, der IKT- und nicht-IKT-Bereiche miteinander verzahnt.

Dr. Mahir Alman
Managing Principal

Strategische Vorteile für Finanzunternehmen

Über die bloße Einhaltung regulatorischer Anforderungen hinaus bietet der vorgeschlagene Rahmen strategische Mehrwerte. Er stärkt Governance- und Risikomanagementpraktiken für Outsourcing und Drittbeziehungen und ermöglicht den betroffenen Unternehmen eine verbesserte Kontrolle und Transparenz über kritische Funktionen. Dies fördert ein tieferes Verständnis der mit Drittanbietern verbundenen Risiken.

Verbesserte Notfall- und Szenarioplanungen bieten zudem mehr Klarheit über Handlungsoptionen bei Störungen und unterstützen eine wirksamere Reaktion und Wiederherstellung. In Summe fördern die Leitlinien ein widerstandsfähigeres und transparenteres Betriebsmodell und befähigen Finanznternehmen, Abhängigkeiten von Drittparteien agiler und sicherer zu steuern.

Wie Capco helfen kann

Um die Vorgaben innerhalb des zweijährigen Übergangszeitraums zu erfüllen, müssen betroffenen Unternehmen einen strukturierten und harmonisierten Ansatz für Third Party-Risiken verfolgen.
Ein zentraler erster Schritt ist eine Gap-Analyse des Reifegrade des bestehenden Third Party-Rahmenwerks im Abgleich mit den Leitlinien sowie gängigen Branchenstandards um bestehende eLücken und Bereiche zu identifizieren, in denen Governance und Dokumentation zwischen IKT und Nicht-IKT abgestimmt werden müssen.

Capco unterstützt Finanzunternehmen bei der Durchführung dieser Assessments, gewährleistet dabei eine konsistente Bewertung und Klassifizierung von Drittanbietervereinbarungen und stellt eine transparente Anwendung des Materialitätsprinzips sicher.

Die Überarbeitung bestehender nicht-IKT-bezogener Verträge ist essentiell um Lücken zu schließen und die vertragliche Anforderungen zu stärken. Capco begleitet die Bereinigung von Verträgen, unterstützt bei der Identifikation und em Umgang mit Subunternehmer- und Konzentrationsrisiken sowie beim Aufbau belastbarer Ausstiegsstrategien. Darüber hinaus hilft Capco durch die Integration der Proportionalität in Onboarding, Risikoanalysen, Due Diligence und laufende Überwachung die Kontrollumgebungen zu verbessern.

Durch den Einsatz von Technologie und KI-gestützten Lösungen unterstützt Capco zudem beim Aufbau und der Automatisierung von Third Party-Risikoframeworks und -Workflows. Dies steigert Effizienz, Effektivität und Prüfbarkeit. Finanznternehmen erreichen dadurch nicht nur Compliance mit den Anforderungen, sondern auch einen zukunftsorientierten, widerstandsfähigen Ansatz für Governance und Kontrolle im Drittparteimanagement.

Autoren

Marija Devic, Executive Director
Dr. Mahir Alman, Managing Principal
Todd Woodhart, Senior Consultant

Kontakt

Christian Dierssen
Partner
christian.dierssen@capco.com

Über Capco

Capco, ein Unternehmen der Wipro-Gruppe, ist ein globales Management- und Technologieberatungsunternehmen, das sich auf die Transformationsumsetzung in der Finanzdienstleistungsbranche und Energie spezialisiert hat. Capco agiert an der Schnittstelle von Wirtschaft und Technologie und kombiniert zukunftsorientierte Denkweisen mit ausgewiesener Branchenkenntnis. In seinen Beratungsaktivitäten treibt Capco digitale Initiativen für Banken und Zahlungsverkehr, Kapitalmärkte, Wealth- und Asset-Management, Versicherungen und den Energiesektor voran. Capcos Innovationskraft wird durch seine preisgekrönte Be Yourself At Work-Kultur und die Vielfalt seiner Talente zum Leben erweckt.

Um mehr zu erfahren, besuchen Sie **www.capco.com** oder folgen Sie uns auf LinkedIn, Instagram, Facebook, YouTube, und Xing.

Globale Standorte

APAC
Bengaluru – Electronic City
Bengaluru – Sarjapur Road
Bangkok
Chennai
Gurgaon
Hong Kong
Hyderabad
Kuala Lumpur
Mumbai
Pune
Singapore

NAHER OSTEN
Dubai

EUROPA
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
Glasgow
London
Milan
Paris
Vienna
Warsaw
Zurich

NORD AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto

SÜD AMERICA
Rio de Janeiro
São Paulo

capco.com

CAPCO
a wipro company

JN_7390