Bundesanstalt für
Finanzdienstleistungsaufsicht

BaFin | Postfach 50 01 54 | 60391 Frankfurt

An die
Verbände der beaufsichtigten Finanzunternehmen

GZ: GIT 3-FR 1534/00007#00009 (Bitte stets angeben)

19.12.2024

**IT-Aufsicht/
Cybersicherheit**

Hausanschrift:
Bundesanstalt für
Finanzdienstleistungsaufsicht
Marie-Curie-Str. 24-28
60439 Frankfurt | Deutschland

Kontakt:
Hasselbach/Leitterstorf
Referat GIT 3
GIT3@bafin.de
www.bafin.de

Zentrale:
Fon +49 (0)2 28 41 08-0
Fax +49 (0)2 28 41 08-1550

53117 Bonn
Graurheindorfer Str. 108

53121 Bonn
Justus-von-Liebig-Straße 28

53175 Bonn
Dreizehnmorgenweg 13-15

60439 Frankfurt
Marie-Curie-Str. 24-28
Lurgiallee 10

Zugang für die rechtswirksame Übersendung qualifiziert elektronisch signierter Dokumente (§ 3a VwVfG) ausschließlich über:
qes-posteingang@bafin.de

Aufhebung der Aufsichtlichen Anforderungen an die IT

Anlagen: 1

Sehr geehrte Damen und Herren,

ein Paradigmenwechsel steht bevor: Ab dem 17.01.2025 findet die Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act, DORA) Anwendung. Sie führt europaweit harmonisierte Regeln für das Management von Risiken der Informations- und Kommunikationstechnologie (IKT) ein.

Zu diesen Regeln gehören Anforderungen an den „regulären IKT-Risikomanagementrahmen" und an die „Schlüsselprinzipien für ein solides Management des IKT-Drittparteienrisikos" einschließlich der entsprechenden Delegierten Verordnungen 2024/1774 und 2024/1773.[1] Diese Anforderungen decken im Wesentlichen die Aufsichtlichen Anforderungen der BaFin an die IT ab. Dazu gehören die Bankaufsichtlichen Anforderungen an die IT (BAIT), die Kapitalverwaltungsaufsichtlichen Anforderungen an die IT (KAIT), die Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) und die Zahlungsdiensteaufsichtlichen Anforderungen an die IT von Zahlungs- und E-Geld-Instituten (ZAIT).

[1] Zudem liegt ein Entwurf der Delegierten Verordnung zur Spezifizierung der Elemente, die ein Finanzunternehmen bestimmen und bewerten muss, wenn es IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen untervergeben hat (JC 2024 53), vor.

Um Doppelregulierung zu vermeiden und die Komplexität der regulatorischen Anforderungen zu verringern, werden daher die KAIT, VAIT und ZAIT vollständig zum 17.01.2025 und die BAIT schrittweise zum 31.12.2026 aufgehoben.

Beaufsichtigte Finanzunternehmen, die nicht unter den Anwendungsbereich der DORA fallen, sind auch verpflichtet, Maßnahmen zum angemessenen Umgang mit IKT-/ Cyberrisiken im Rahmen der ordnungsgemäßen Geschäftsorganisation zu treffen.

Schritte zur Aufhebung der BAIT

In einem ersten Schritt wird der Anwenderkreis der BAIT reduziert: Mit Ablauf des 16.01.2025 werden Institute, die ab dem 17.01.2025 ein IKT-Risikomanagement nach Art. 5-15 oder Art. 16 DORA betreiben müssen, aus dem Anwenderkreis der BAIT ausgenommen. Zudem wird Kapitel 11 der BAIT vollständig aufgehoben. Hierbei konnte von einem Konsultationsverfahren abgesehen werden, da sich die aufsichtlichen Anforderungen der BAIT nicht ändern, sondern lediglich der Anwenderkreis reduziert beziehungsweise eine Pflichtenreduktion vorgenommen wird.

Für die weiteren Unternehmen, die derzeit die BAIT anwenden müssen, aber ab dem 17.01.2025 nicht unter den unmittelbaren Anwendungsbereich der DORA fallen, bestehen die BAIT vorerst fort.

Gemäß § 1a Absatz 2 KWG, der durch das Gesetz über die Digitalisierung des Finanzmarktes (Finanzmarktdigitalisierungsgesetz - FinmaDiG) neu gefasst wurde, fallen ab dem 01.01.2027 weitere Institute in den Anwendungsbereich der DORA. Für diese Institute ist eine Übergangsfrist bis zum 31.12.2026 für die Anwendung der Anforderungen des IKT-Risikomanagements nach DORA vorgesehen. Durch das Fortbestehen der BAIT ist sichergestellt, dass während der Übergangszeit keine Regelungslücke entsteht. Die BAIT werden nach dem Ende der Übergangsfrist, d.h. mit Ablauf des 31.12.2026 vollständig aufgehoben.

Schlussbemerkungen

Die KAIT, VAIT und ZAIT treten mit Ablauf des 16.01.2025 außer Kraft.

Die neuen BAIT treten ab dem 17.01.2025 in Kraft. Gleichzeitig treten die bisherigen BAIT in der Fassung vom 16.08.2021 außer Kraft. Diesem Schreiben ist die Neufassung der BAIT mit reduziertem Anwenderkreis und dem aufgehobenen Kapitel 11 angefügt. Mit Ablauf des 31.12.2026 treten die BAIT vollständig außer Kraft.

Mit freundlichen Grüßen

Raimund Röseler

Dieses Schreiben wurde elektronisch erstellt und enthält daher keine Unterschrift.