Zahlungsdiensteaufsichtliche Anforderungen an die IT (ZAIT)

Der neue Fokus der BaFin-Sicherheitsbestrebungen an die IT von Zahlungs- und E-Geld-Instituten

Am 16. August 2021 wurde das neue Rundschreiben ZAIT von der BaFin veröffentlicht, in dem die aufsichtsrechtlichen Anforderungen an eine ordnungsgemäße Geschäftsführung von Zahlungs- und E-Geld-Instituten in Bezug auf IT- und Cybersicherheit definiert sind.

Ein einheitlicher IT-Rahmen

Die in der ZAIT veröffentlichten Anforderungen, die weitestgehend den Inhalt und die Anforderungen der MaRisk und der BAIT übernehmen, erweitern bestehende Compliance-Anforderungen, um eine gezieltere Sicherheit für Zahlungs- und E-Geld-Institute zu gewährleisten.

Sie bieten einen Rahmen für Zahlungsinstitute im Umgang mit den Themenbereichen von der IT-Strategie über das Informationsrisikomanagement bis hin zum Informationssicherheitsmanagement. Die ZAIT finden seit der Veröffentlichung (16. August 2021) Anwendung.

Mit inhaltlichen Unterschieden zu den BAIT

Folgende Kapitel haben kleinere bis mittlere Veränderungen erfahren:

- Kapitel 1: IT-Strategie
- Kapitel 2: IT-Governance
- Kapitel 6: Identitäts- und Rechtemanagement
- Kapitel 7: IT-Projekte und Anwendungsentwicklung
- Kapitel 10: Notfallmanagement

Die größten Veränderungen sind in Kapitel 9 zu finden. Im Vergleich zu den BAIT befassen sich die ZAIT mit weiteren Konkretisierungen zu „Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen“.

Die ZAIT übernehmen hierbei auch die Regularien aus dem Allgemeinen Teil 9 MaRisk zum Thema „Auslagerung“, wobei die Konkretisierung der ZAIT sich hier mit der Auslagerung von IT-Prozessen und IT-Aktivitäten befasst. Hierdurch werden auch die Anforderungen aus § 26 ZAG sowie die EBA-Richtlinien weiter präzisiert.

> Die Anforderungen dieses Rundschreibens gelten für alle Institute im Sinne von § 1 Abs. 3 des Zahlungsdiensteaufsichtsgesetzes (ZAG), das heißt für Zahlungsinstitute und E-Geld-Institute […]. Sie gelten auch für die Zweigniederlassungen deutscher Institute im Ausland im Sinne von § 38 ZAG. Auf Zweigniederlassungen von Unternehmen mit Sitz in einem anderen Staat des Europäischen Wirtschaftsraums nach § 39 ZAG finden sie keine Anwendung.”
>
> Quelle: ZAIT, BaFin, Rundschreiben 11/2021 in der Fassung vom 16.08.2021

Die neuen ZAIT bilden damit gemeinsam mit den Anforderungen aus dem Digital Operational Resilience Act (DORA) – der am 17. Januar 2023 in Kraft getreten ist und ab dem 17. Januar 2025 gilt – die Grundlage für zukünftige Prüfungen der IT-Aufsicht.

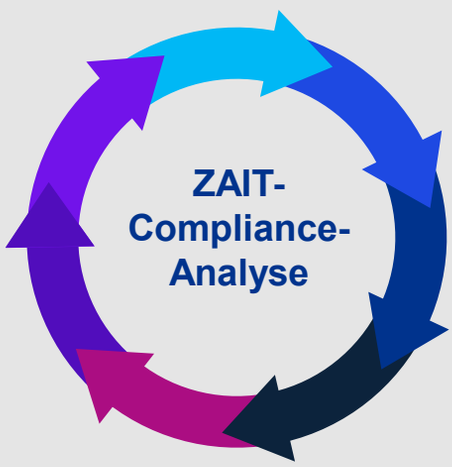
KPMG als Begleiter für Ihren ZAIT-Compliance-Check

KPMG hat umfassende Erfahrungen in den Themengebieten der BAIT, VAIT, KAIT und DORA. Gern begleitet KPMG Sie mit einer ZAIT-Compliance-Analyse und bei deren Umsetzung.

In der KPMG ZAIT-Compliance-Analyse werden sieben Schritte durchlaufen, die in der folgenden Abbildung beschrieben sind.

Mithilfe dieser Analyse werden potentielle Gaps und Risiken identifiziert, auf welche eine entsprechend angepasste - typischerweise risikoorientiert - Maßnahmenplanung konzipiert werden. KPMG kann Sie individuell nach dem Baukastenprinzip in jedem oder in einzelnen Schritten der Methodik unterstützen.

Genauere Informationen zu den ZAIT können Sie in folgendem Dokument finden: Rundschreiben 11/2021 (BA) in der Fassung vom 16.08.2021; Anforderungen an die IT von Zahlungs- und E-Geld-Instituten (ZAIT).



KPMG: Ihr Experte im Bereich Compliance

KPMG hat eine bewährte und vertrauenswürdige Methodik entwickelt, die unseren Kund:innen über Jahre hinweg erfolgreich bei IT-Aufsichtsprüfungen geholfen hat. Unser Team mit langjähriger Erfahrung freut sich darauf, Sie zu unterstützen.

01 Analyse des Status quo

Identifikation von Widersprüchen und nicht erfüllten Anforderungen bzw. Lücken zur Erreichung einer IT-Compliance

02 Unterstützung bei der Erhöhung des IT-Compliance-Reifegrades

- Definition von Maßnahmen zur Behebung identifizierter Widersprüche und Lücken
- Unterstützung der Projekte bei der Umsetzung der Maßnahmen (vor der Prüfung)

03 Organisatorische und prozessuale Vorbereitung

- Organisatorische Vorbereitung auf eine anstehende Aufsichtsprüfung
- Durchführung von Awareness-Maßnahmen
- Aufsetzen von Prozessen und Prüfungsoffice

04 Aktive Begleitung der Aufsichtsprüfung

Begleitung bei der Prüfung durch die Aufsicht – Organisation und Mitarbeit im Prüfungsoffice

05 Definition von Maßnahmen und Roadmaps

- Definition von Maßnahmen und Ambitionsniveaus
- Erarbeitung einer Roadmap inkl. Reporting-Termine

06 Fachliche Umsetzung der Maßnahmen

Bearbeitung der Maßnahmen zur Abmeldung von Feststellungen

07 Qualitätssicherung und Reporting

Qualitätssicherung von Ergebnisobjekten und regelmäßiges Reporting an die Aufsicht bis zu der Abmeldung

Einige oder alle der hier beschriebenen Leistungen sind möglicherweise für KPMG-Prüfungsmandanten und deren verbundene Unternehmen unzulässig.

Kontakt

Gerne unterstützt Sie unser Team.

KPMG AG
Wirtschaftsprüfungsgesellschaft
Klingelhöferstraße 18
10785 Berlin

Vaike Metzger (Muc)

Partnerin
Financial Services
T +49 89 9282-4816
M +49 172 2895793
vmetzger@kpmg.com

Nadine Schmitz (KOe)

Partnerin
Financial Services
T +49 221 2073-1403
M +49 174 3015954
nschmitz@kpmg.com

Peter Hertlein (Nbg)

Director
Financial Services
T +49 911 5973-3068
M +49 174 3060018
phertlein@kpmg.com

www.kpmg.de/sicher-und-compliant

www.kpmg.de

www.kpmg.de/socialmedia