



# Neue BaFin-Richtlinie (Konsultation) verschärft Fit-and-Proper-Anforderungen an IT-Kompetenzen für das Leitungsorgan in Banken

Deggendorfer Notiz 2025/05 | Mai 2025

## Einleitung

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat den Entwurf eines neuen Rundschreibens „zu den Mitgliedern der Geschäftsleitung sowie von Verwaltungs- und Aufsichtsorganen gemäß KWG“ (im Folgenden: FAP-Rundschreiben) zur Konsultation gestellt, das zwei bestehende Merkblätter ablösen soll: das Merkblatt zu den Geschäftsleitern gemäß KWG, ZAG und KAGB sowie das Merkblatt zu den Mitgliedern von Verwaltungs- und Aufsichtsorganen gemäß KWG und KAGB. Diese Konsolidierung zielt darauf ab, die Anforderungen an die fachliche Eignung und Zuverlässigkeit von Führungskräften und Aufsichtsorganmitgliedern in Kreditinstituten zu harmonisieren und an aktuelle gesetzliche sowie europäische Vorgaben anzupassen. Im Folgenden werden die drei Dokumente hinsichtlich ihrer fachlichen Anforderungen an IT, Digitalisierung, IKT-Risiko (Informations- und Kommunikationstechnologie-Risiko) und Informationssicherheit verglichen, um die Entwicklung und Verschärfung der regulatorischen Erwartungen in diesen Bereichen zu analysieren.

---

Das **bestehende Merkblatt zu den Geschäftsleitern**<sup>1</sup> gemäß KWG, ZAG und KAGB legt die Anforderungen an die fachliche Eignung von Geschäftsleitern fest, wobei der Fokus auf einer umfassenden Sachkunde liegt, die die Leitung eines Kreditinstituts ermöglicht. In Bezug auf IT und Digitalisierung werden keine spezifischen Anforderungen an technische Kenntnisse oder IKT-Risikomanagement explizit formuliert. Stattdessen wird erwartet, dass Geschäftsleiter über ein generelles Verständnis der Geschäftsprozesse und Risiken verfügen, zu denen implizit auch IT-bezogene Risiken zählen. Informationssicherheit wird zwar als Teil der allgemeinen Risikosteuerung erwähnt, jedoch ohne detaillierte Vorgaben zu spezifischen Kompetenzen in diesem Bereich. Die Anforderungen bleiben somit vergleichsweise allgemein und lassen Spielraum für Interpretation, was den IT-Fachhintergrund angeht.

---

<sup>1</sup> [https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb\\_geschaeftsleiter\\_KWG\\_ZAG\\_KAGB.html](https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_geschaeftsleiter_KWG_ZAG_KAGB.html)



Das **Merkblatt zu den Mitgliedern von Verwaltungs- und Aufsichtsorganen**<sup>2</sup> gemäß KWG und KAGB betont die kollektive Eignung des Gremiums, wobei einzelne Mitglieder nicht zwingend über vertiefte Fachkenntnisse in allen Bereichen verfügen müssen. In Bezug auf IT und Digitalisierung wird die Notwendigkeit eines grundlegenden Verständnisses der technologischen Entwicklungen und deren Auswirkungen auf das Geschäftsmodell angesprochen. IKT-Risiken werden als Teil des Risikomanagements betrachtet, jedoch ohne spezifische Anforderungen an technische Expertise. Informationssicherheit wird in diesem Kontext als ein Aspekt der Überwachungspflichten genannt, wobei die Verantwortung primär bei der Geschäftsleitung liegt und das Aufsichtsorgan lediglich eine kontrollierende Funktion wahrnimmt. Auch hier bleibt der Fokus auf einem allgemeinen, nicht technisch detaillierten Verständnis.

---

Im Gegensatz dazu legt das **neue FAP-Rundschreiben**<sup>3</sup> (Konsultation) einen stärkeren Fokus auf die spezifischen Herausforderungen der Digitalisierung und der damit verbundenen Risiken. Es berücksichtigt explizit die gestiegene Bedeutung von IT-Systemen und IKT-Risiken im Finanzsektor, die durch die fortschreitende Digitalisierung und die zunehmende Abhängigkeit von Technologien bedingt sind. Das Rundschreiben fordert, dass Geschäftsleiter über ausreichende Kenntnisse verfügen, um IT-Strategien und deren Auswirkungen auf das Geschäftsmodell zu beurteilen. Dies schließt ein vertieftes Verständnis von IKT-Risiken ein, insbesondere im Hinblick auf Cyberbedrohungen, Datenintegrität und Systemstabilität. Für Mitglieder von Verwaltungs- und Aufsichtsorganen wird ebenfalls ein kollektives Wissen über IT-Risiken und Informationssicherheit erwartet, wobei mindestens einzelne Mitglieder über spezifische Kenntnisse in diesen Bereichen verfügen sollten, um eine effektive Überwachung zu gewährleisten. Das Rundschreiben betont zudem die Bedeutung von Informationssicherheit als integralen Bestandteil des Risikomanagements und verweist auf die Notwendigkeit, aktuelle regulatorische Vorgaben, wie etwa die des Risikoreduzierungsgesetzes und künftige Anpassungen durch die CRD VI, zu berücksichtigen.

Ein wesentlicher Unterschied zwischen dem neuen Rundschreiben und den bisherigen Merkblättern liegt in der Präzisierung und Verschärfung der Anforderungen an den IT-Fachhintergrund. Während die Merkblätter IT und Digitalisierung eher als Teil eines allgemeinen Risikomanagements betrachten, stellt das FAP-Rundschreiben klar, dass ein fundiertes Verständnis dieser Themen für die Erfüllung der Aufgaben von Geschäftsleitern und Aufsichtsorganen unerlässlich ist. Insbesondere die explizite Erwähnung von IKT-Risiken und die Erwartung, dass zumindest Teile des Aufsichtsorgans über spezifische IT-

---

<sup>2</sup> [https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb\\_verwaltungs-aufsichtsorgane\\_KWG\\_KAGB.html](https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_verwaltungs-aufsichtsorgane_KWG_KAGB.html)

<sup>3</sup> [https://www.bafin.de/SharedDocs/Downloads/DE/Konsultation/2025/dl\\_kon\\_11\\_2025\\_FAP\\_RS.pdf](https://www.bafin.de/SharedDocs/Downloads/DE/Konsultation/2025/dl_kon_11_2025_FAP_RS.pdf)



Kenntnisse verfügen, markieren einen Paradigmenwechsel hin zu einer stärker technologieorientierten Governance. Diese Entwicklung spiegelt die zunehmende Bedeutung von Technologie im Finanzsektor wider und steht im Einklang mit europäischen Vorgaben, die eine robuste Steuerung von IT-Risiken fordern.

---

## Ausblick

Zusammenfassend lässt sich feststellen, dass das neue FAP-Rundschreiben im Vergleich zu den bisherigen Merkblättern deutlich höhere Anforderungen an den IT-Fachhintergrund, die Digitalisierungskompetenz, das IKT-Risikomanagement und die Informationssicherheit stellt. Während die Merkblätter diese Themen nur implizit oder allgemein behandeln, fordert das Rundschreiben explizite Kenntnisse und eine aktive Auseinandersetzung mit technologischen Risiken. Diese Verschärfung ist ein Indikator für die wachsende Relevanz von IT und Digitalisierung in der Finanzbranche und unterstreicht die Notwendigkeit, dass Führungskräfte und Aufsichtsorgane über entsprechende Kompetenzen verfügen, um den aktuellen und zukünftigen Herausforderungen gerecht zu werden.



### **Prof. Dr. Andreas Igl**

BDO-Stiftungsprofessor an der TH Deggendorf  
Lehrbeauftragter an der Hochschule der Deutschen Bundesbank

[andreas.igl@th-deg.de](mailto:andreas.igl@th-deg.de)

(Mobil): 0151 2301 8610

(LinkedIn): [Link](#)



### **Axel Gürntke**

Akademie Deutscher Genossenschaften e.V.  
Leiter Management Programme

[axel.guerntke@adg-campus.de](mailto:axel.guerntke@adg-campus.de)

(Telefon): +49 2602 14 170

(LinkedIn): [Link](#)