

---

# Checkliste für Aufsichtsräte

[www.bankboard.de](http://www.bankboard.de) - [kontakt@bankboard.de](mailto:kontakt@bankboard.de)

---

13.07.2024

**O**ft wird eine Aufsichtsratssitzung von spezifischen Themen der Bank überlagert. Daher ist es wichtig, die übrigen Aufgaben des Aufsichtsrats nicht aus den Augen zu verlieren. Eine Checkliste dient dazu, regelmäßig - z.B. vierteljährlich - möglichst alle Aspekte abzufragen. Bei Fragen, die nicht eindeutig mit einem "Ja" beantwortet werden können, sollte eine Auskunft beim Vorstand oder dem Wirtschaftsprüfer eingeholt werden.

## Überwachung der Geschäftsführung

1. Wird der Aufsichtsrat regelmäßig und umfassend über alle wesentlichen Angelegenheiten der Bank informiert? (§ 25d Abs. 2 KWG)
2. Überwacht der Aufsichtsrat die Rechtmäßigkeit, Zweckmäßigkeit und Wirtschaftlichkeit der Entscheidungen der Geschäftsführung? (§ 111 Abs. 1 AktG)
3. Erhält der Aufsichtsrat regelmäßig Berichte über die Geschäftsentwicklung? (DCGK Abschnitt 5.1)
4. Überprüft der Aufsichtsrat regelmäßig seine eigene Arbeitsweise und Effizienz? (DCGK Abschnitt 5.1)

## Risikomanagement und interne Kontrollsysteme

5. Sind die Risikomanagementsysteme der Bank implementiert und funktionieren sie angemessen? (§ 25a Abs. 1 KWG)
6. Überwacht der Aufsichtsrat die Risikostrategie und deren regelmäßige Aktualisierung? (Artikel 44, 45 CRR)
7. Überwacht der Aufsichtsrat die Einhaltung der MaRisk-Anforderungen? (MaRisk)

8. Überwacht der Prüfungsausschuss die Wirksamkeit des internen Kontrollsystems, des Risikomanagementsystems und des internen Revisionssystems? (DCGK Abschnitt 5.3.2)

## **Prüfung und Genehmigung von Jahresabschlüssen**

9. Hat der Aufsichtsrat den Jahresabschluss, den Lagebericht und den Vorschlag zur Verwendung des Bilanzgewinns geprüft? (§ 171 Abs. 1 AktG)
10. Wurde der geprüfte Jahresabschluss festgestellt und der Gewinnverwendungsvorschlag genehmigt? (§ 172 AktG)
11. Wurde der Jahresabschluss auf Ordnungsmäßigkeit, Wirtschaftlichkeit und die finanzielle Lage der Bank geprüft? (§ 170 HGB)

## **Ernennung und Überwachung der Geschäftsführung**

12. Sind die Mitglieder des Vorstands fachlich qualifiziert und persönlich geeignet? (§ 84 Abs. 1 AktG)
13. Überwacht der Aufsichtsrat kontinuierlich die Tätigkeiten der Geschäftsleiter? (§ 25d Abs. 5 KWG)

## **Compliance und regulatorische Konformität**

14. Verfügt die Bank über angemessene Verfahren und Regelungen zur Einhaltung der gesetzlichen und regulatorischen Anforderungen? (§ 25c Abs. 4a KWG)
15. Hat der Vorstand ein Überwachungssystem implementiert, das frühzeitig Risiken erkennt, die den Fortbestand der Gesellschaft gefährden könnten? (§ 91 Abs. 2 AktG)
16. Überwacht der Aufsichtsrat die Implementierung und Wirksamkeit des Überwachungssystems? (§ 91 Abs. 2 AktG)

## **BAIT (Bankenaufsichtliche Anforderungen an die IT)**

17. Ist die IT-Strategie der Bank mit der Geschäftsstrategie abgestimmt und wird sie vom Aufsichtsrat überwacht? (BAIT)
18. Gibt es eine klare IT-Governance-Struktur mit definierten Zuständigkeiten und Verantwortlichkeiten? (BAIT)
19. Überwacht der Aufsichtsrat die Identifikation, Bewertung und Steuerung von IT-bezogenen Risiken? (BAIT)
20. Sind angemessene Sicherheitsmaßnahmen zum Schutz der IT-Systeme und Daten implementiert und werden sie regelmäßig aktualisiert? (BAIT)
21. Überwacht der Aufsichtsrat die Planung und Durchführung von IT-Projekten sowie die Entwicklung neuer IT-Anwendungen? (BAIT)
22. Werden ausgelagerte IT-Dienstleistungen den BAIT-Anforderungen entsprechend überwacht? (BAIT)

## Wirtschaftliche Aspekte

23. Wird die Unternehmensstrategie regelmäßig überprüft und an veränderte Marktbedingungen angepasst? (§ 25d KWG, DCGK Abschnitt 4.1)
24. Überwacht der Aufsichtsrat die Umsetzung der Unternehmensstrategie und der Geschäftsmodelle? (DCGK Abschnitt 4.2)
25. Wird die Ertragslage der Bank regelmäßig analysiert und berichtet? (§ 25a Abs. 1 KWG)
26. Sind Maßnahmen zur Verbesserung der Wirtschaftlichkeit der Bank implementiert und überwacht? (DCGK Abschnitt 7.1)
27. Werden die Kreditrisiken der Bank regelmäßig bewertet und gesteuert? (§ 25a Abs. 1 KWG, MaRisk)
28. Existieren effektive Verfahren zur Überwachung und Steuerung von Ausfallrisiken bei Krediten? (MaRisk AT 4.3)
29. Wird die interne Revision unabhängig und umfassend durchgeführt? (§ 25a Abs. 1 KWG, MaRisk AT 4.4)
30. Überwacht der Aufsichtsrat die Umsetzung der Empfehlungen der internen Revision? (DCGK Abschnitt 5.3.2)
31. Werden die Ergebnisse externer Prüfungen regelmäßig geprüft und Maßnahmen ergriffen? (§ 29 Abs. 1 KWG)
32. Werden große Projekte und Investitionen vom Aufsichtsrat überwacht und genehmigt? (DCGK Abschnitt 5.3.1)
33. Sind Mechanismen zur Überwachung des Fortschritts und der Wirtschaftlichkeit von Projekten implementiert? (MaRisk AT 4.2)
34. Wird das Bankbuch regelmäßig auf Risiken und Wertveränderungen überprüft? (§ 25a Abs. 1 KWG)
35. Sind effektive Methoden zur Steuerung des Barwerts und zur Bewertung von Zinsänderungsrisiken vorhanden? (MaRisk AT 2.2)
36. Überwacht der Aufsichtsrat die finanzielle Stabilität der Bank und die Einhaltung der Kapitalanforderungen? (Artikel 92 CRR, § 25a Abs. 1 KWG)
37. Existiert eine vorausschauende Kapitalplanung, die regelmäßig überprüft und angepasst wird? (§ 25a Abs. 1 KWG, MaRisk)

## Umwelt-, Sozial- und Governance-Themen (ESG)

38. Sind Nachhaltigkeitsrisiken in das Risikomanagement der Bank integriert und werden sie regelmäßig bewertet? (§ 25a Abs. 1 KWG)
39. Kommt die Bank ihren Berichtspflichten zu ESG-Faktoren nach? (Deutsche Nachhaltigkeitsstrategie)
40. Werden die Tätigkeiten der Bank gemäß der EU-Taxonomie klassifiziert und berichtet? (EU-Taxonomie-Verordnung)

## **Bekämpfung von Geldwäsche und Terrorismusfinanzierung (AML/CFT)**

41. Verfügt die Bank über wirksame Verfahren und Systeme zur Verhinderung von Geldwäsche und Terrorismusfinanzierung? (§ 25h KWG, GwG)
42. Wurde ein Geldwäschebeauftragter bestellt, der regelmäßig an den Aufsichtsrat berichtet? (§ 7 GwG)
43. Werden die Risikobewertungen hinsichtlich Geldwäsche und Terrorismusfinanzierung regelmäßig durchgeführt und aktualisiert? (§ 5 GwG)
44. Entsprechen die internen Kontrollsysteme der Bank den Anforderungen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung? (§ 25c Abs. 4a KWG)

## **Datenschutz und IT-Sicherheit**

45. Hält die Bank alle Vorgaben der DSGVO ein, einschließlich der Implementierung eines Datenschutzmanagementsystems? (DSGVO Art. 24, 25)
46. Wurde ein Datenschutzbeauftragter bestellt und überwacht der Aufsichtsrat die Einhaltung der Datenschutzrichtlinien? (DSGVO Art. 37)
47. Werden die BAIT-Vorgaben hinsichtlich der IT-Sicherheit und des Datenschutzes eingehalten und regelmäßig überprüft? (BAIT)

## **Vergütungssysteme**

48. Entsprechen die Vergütungssysteme der Bank den Anforderungen der Institutsvergütungsverordnung (InstVV), einschließlich der Berücksichtigung von Nachhaltigkeits- und Risikokriterien? (§ 25a Abs. 5 KWG, InstVV)
49. Überwacht der Aufsichtsrat die Implementierung und Einhaltung der Vergütungspolitik? (InstVV)

## **Ethik und Unternehmensverantwortung**

50. Fördert der Aufsichtsrat eine Kultur der Ethik und Integrität innerhalb der Bank? (DCGK)
51. Werden die entsprechenden Verhaltenskodizes und Unternehmensrichtlinien eingehalten? (DCGK)