
Der Aufsichtsrat einer Bank

www.bankboard.de - kontakt@bankboard.de

13.07.2024

Der Aufsichtsrat einer Bank spielt eine zentrale Rolle bei der Überwachung und Sicherstellung einer ordnungsgemäßen Geschäftsführung sowie der Einhaltung vielfältiger regulatorischer Anforderungen. In einer zunehmend komplexen und regulierten Finanzwelt ist es unerlässlich, dass der Aufsichtsrat seine Pflichten und Aufgaben systematisch wahrnimmt. Dieser Artikel gibt einen detaillierten Überblick über die verschiedenen Aspekte der Aufsichtsratsarbeit, gestützt durch die relevanten gesetzlichen Grundlagen und Normen. Am Ende des Artikels sind sämtliche Quellen und ihre entsprechenden Internetlinks aufgeführt.

Überwachung der Geschäftsführung

Kreditwesengesetz (KWG)

Das Kreditwesengesetz (KWG) fordert in § 25d, dass der Aufsichtsrat aus sachkundigen Mitgliedern besteht, die in der Lage sind, die Geschäftsführung effektiv zu überwachen. Der Vorstand ist verpflichtet, den Aufsichtsrat regelmäßig über alle wesentlichen Angelegenheiten zu informieren (§ 25d Abs. 2 KWG).

Aktiengesetz (AktG)

Nach § 111 Abs. 1 AktG hat der Aufsichtsrat die Geschäftsführung der Gesellschaft zu überwachen. Diese Überwachung umfasst auch die Einhaltung aller relevanten gesetzlichen Vorschriften sowie interner Richtlinien, um sicherzustellen, dass die Gesellschaft ordnungsgemäß geführt wird.

Deutscher Corporate Governance Kodex (DCGK)

Abschnitt 5.1 des DCGK betont die Wichtigkeit einer aktiven und kritischen Überwachung der Geschäftsführung. Der Kodex verlangt, dass der Aufsichtsrat regelmäßig Berichte über die Geschäftsentwicklung erhält und bei Bedarf Maßnahmen ergreift, um eine ordnungsgemäße Unternehmensführung sicherzustellen.

Risikomanagement und interne Kontrollsysteme

Kreditwesengesetz (KWG)

Das KWG fordert in § 25a Abs. 1, dass die Geschäftsleiter geeignete Maßnahmen zur Risikokontrolle, -überwachung und -steuerung implementieren (MaRisk). Der Aufsichtsrat muss sicherstellen, dass diese Maßnahmen angemessen und effektiv sind. Dazu gehört auch die Überprüfung, ob die Geschäftsleiter über die erforderlichen Kenntnisse im Risikomanagement verfügen.

Capital Requirements Regulation (CRR)

Artikel 44 und 45 der CRR legen spezifische Anforderungen an das Risikomanagement fest, die auch die Verantwortlichkeiten des Aufsichtsrats umfassen. Der Aufsichtsrat muss die Strategien und Verfahren zur Risikosteuerung überwachen und sicherstellen, dass die Bank angemessen kapitalisiert ist, um ihre Risiken zu tragen.

MaRisk

Die Mindestanforderungen an das Risikomanagement (MaRisk) konkretisieren die Anforderungen an das Risikomanagement und die internen Kontrollsysteme von Banken. Der Aufsichtsrat ist für die Überwachung der Umsetzung und Einhaltung der MaRisk verantwortlich. Dies umfasst die regelmäßige Bewertung der Wirksamkeit der Risikomanagementsysteme und der internen Kontrollmechanismen.

Deutscher Corporate Governance Kodex (DCGK)

Abschnitt 5.3.2 des DCGK fordert, dass der Prüfungsausschuss des Aufsichtsrats die Wirksamkeit des internen Kontrollsystems, des Risikomanagementsystems und des internen Revisionssystems überwacht. Der Ausschuss soll sicherstellen, dass diese Systeme effizient arbeiten und die Risiken der Bank angemessen gesteuert werden.

Prüfung und Genehmigung von Jahresabschlüssen

Aktiengesetz (AktG)

Gemäß § 171 Abs. 1 AktG ist der Aufsichtsrat verpflichtet, den Jahresabschluss, den Lagebericht und den Vorschlag zur Verwendung des Bilanzgewinns zu prüfen. Weiterhin fordert § 172 AktG, dass der Aufsichtsrat den geprüften Jahresabschluss feststellt und den Gewinnverwen-

dungsvorschlag genehmigt.

Handelsgesetzbuch (HGB)

§ 170 HGB legt fest, dass der Aufsichtsrat für die Prüfung des Jahresabschlusses verantwortlich ist. Dabei hat er die Ordnungsmäßigkeit der Geschäftsführung und die wirtschaftliche Lage der Bank zu berücksichtigen, um sicherzustellen, dass die Finanzberichte korrekt und vollständig sind.

Ernennung und Überwachung der Geschäftsführung

Aktiengesetz (AktG)

Das Aktiengesetz gibt dem Aufsichtsrat in § 84 Abs. 1 die Verantwortung, die Mitglieder des Vorstands zu bestellen und deren Tätigkeit zu überwachen. Der Aufsichtsrat muss sicherstellen, dass die Vorstandsmitglieder fachlich qualifiziert und persönlich geeignet sind.

Kreditwesengesetz (KWG)

Gemäß § 25d Abs. 5 KWG ist der Aufsichtsrat verpflichtet, die Eignung der Geschäftsleiter zu prüfen und deren Tätigkeiten zu überwachen. Diese Prüfung umfasst die fachliche Qualifikation und Zuverlässigkeit der Geschäftsleiter, um sicherzustellen, dass sie den Anforderungen des Unternehmens gerecht werden.

Compliance und regulatorische Konformität

Kreditwesengesetz (KWG)

Das Kreditwesengesetz verlangt in § 25c Abs. 4a, dass der Aufsichtsrat sicherstellt, dass die Bank über angemessene Verfahren und Regelungen zur Einhaltung der gesetzlichen und regulatorischen Anforderungen verfügt. Der Aufsichtsrat muss überprüfen, ob diese Verfahren effektiv sind und regelmäßig aktualisiert werden.

Aktiengesetz (AktG)

§ 91 Abs. 2 AktG verpflichtet den Vorstand, geeignete Maßnahmen zur Früherkennung von Entwicklungen zu treffen, die den Fortbestand der Gesellschaft gefährden könnten. Der Aufsichtsrat überwacht die Einhaltung dieser Pflichten und stellt sicher, dass ein funktionierendes Überwachungssystem eingerichtet ist.

BAIT (Bankenaufsichtliche Anforderungen an die IT)

IT-Strategie

Die Bank muss eine IT-Strategie entwickeln und umsetzen, die auf die Geschäftsstrategie abgestimmt ist. Der Aufsichtsrat überwacht die Implementierung und Weiterentwicklung dieser

IT-Strategie.

IT-Governance

Der Aufsichtsrat muss sicherstellen, dass eine effektive IT-Governance-Struktur vorhanden ist. Dies umfasst klare Zuständigkeiten und Verantwortlichkeiten für die IT und deren Kontrolle.

Informationsrisikomanagement

Der Aufsichtsrat überwacht die Identifikation, Bewertung und Steuerung von IT-bezogenen Risiken. Dazu gehört auch die regelmäßige Überprüfung der Sicherheitsmaßnahmen und Notfallpläne.

Informationssicherheit

Die BAIT fordert, dass angemessene Sicherheitsmaßnahmen zum Schutz der IT-Systeme und Daten der Bank implementiert werden. Der Aufsichtsrat muss sicherstellen, dass diese Maßnahmen den aktuellen Bedrohungen entsprechen und regelmäßig aktualisiert werden.

IT-Projekte und Anwendungsentwicklung

Der Aufsichtsrat überwacht die Planung und Durchführung von IT-Projekten sowie die Entwicklung und Implementierung neuer IT-Anwendungen. Dies schließt die Prüfung ein, ob diese Projekte und Anwendungen den regulatorischen Anforderungen entsprechen.

Auslagerung von IT-Dienstleistungen

Wenn IT-Dienstleistungen ausgelagert werden, muss der Aufsichtsrat sicherstellen, dass die ausgelagerten Tätigkeiten ebenfalls den BAIT-Anforderungen entsprechen und dass die Risiken der Auslagerung angemessen gesteuert werden.

Wirtschaftliche Aspekte

Strategie und Geschäftsmodell

Das KWG (§ 25d) und der DCGK (Abschnitt 4.1) verlangen, dass die Unternehmensstrategie regelmäßig überprüft und an veränderte Marktbedingungen angepasst wird. Der Aufsichtsrat überwacht die Umsetzung der Unternehmensstrategie und der Geschäftsmodelle (DCGK Abschnitt 4.2).

Ertragslage und Wirtschaftlichkeit

Die Ertragslage der Bank muss gemäß § 25a Abs. 1 KWG regelmäßig analysiert und berichtet werden. Maßnahmen zur Verbesserung der Wirtschaftlichkeit der Bank müssen implementiert und überwacht werden (DCGK Abschnitt 7.1).

Kreditrisiko

§ 25a Abs. 1 KWG und die MaRisk verlangen, dass die Kreditrisiken der Bank regelmäßig bewertet und gesteuert werden. Effektive Verfahren zur Überwachung und Steuerung von Ausfallrisiken bei Krediten müssen vorhanden sein (MaRisk AT 4.3).

Revision und interne Prüfungen

Die interne Revision muss gemäß § 25a Abs. 1 KWG und MaRisk AT 4.4 unabhängig und umfassend durchgeführt werden. Der Aufsichtsrat überwacht die Umsetzung der Empfehlungen der internen Revision (DCGK Abschnitt 5.3.2). Auch die Ergebnisse externer Prüfungen werden regelmäßig geprüft und Maßnahmen ergriffen (§ 29 Abs. 1 KWG).

Projekte und Investitionen

Der Aufsichtsrat muss große Projekte und Investitionen überwachen und genehmigen (DCGK Abschnitt 5.3.1). Mechanismen zur Überwachung des Fortschritts und der Wirtschaftlichkeit von Projekten müssen implementiert sein (MaRisk AT 4.2).

Bankbuch und Barwertsteuerung

Das KWG (§ 25a Abs. 1) fordert, dass das Bankbuch regelmäßig auf Risiken und Wertveränderungen überprüft wird. Effektive Methoden zur Steuerung des Barwerts und zur Bewertung von Zinsänderungsrisiken müssen vorhanden sein (MaRisk AT 2.2).

Finanzielle Stabilität und Kapitalplanung

Artikel 92 CRR und § 25a Abs. 1 KWG verlangen, dass der Aufsichtsrat die finanzielle Stabilität der Bank und die Einhaltung der Kapitalanforderungen überwacht. Eine vorausschauende Kapitalplanung, die regelmäßig überprüft und angepasst wird, muss existieren.

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

Kreditwesengesetz (KWG)

§ 25a Abs. 1 KWG fordert, dass Kreditinstitute Nachhaltigkeitsrisiken, die sich aus ESG-Faktoren ergeben, identifizieren, bewerten und steuern. Der Aufsichtsrat muss sicherstellen, dass diese Risiken in das Risikomanagement integriert sind.

Deutsche Nachhaltigkeitsstrategie

Der Aufsichtsrat überwacht die Umsetzung der Nachhaltigkeitsstrategie der Bank, die auf nationalen und internationalen Nachhaltigkeitszielen basiert.

EU-Taxonomie-Verordnung

Der Aufsichtsrat stellt sicher, dass die Bank ihre Tätigkeiten gemäß der EU-Taxonomie klassifi-

ziert und berichtet, um Transparenz über nachhaltige Investitionen zu gewährleisten.

Bekämpfung von Geldwäsche und Terrorismusfinanzierung (AML/CFT)

Geldwäschegesetz (GwG)

Das GwG und § 25h KWG verlangen, dass die Bank über wirksame Verfahren und Systeme zur Verhinderung von Geldwäsche und Terrorismusfinanzierung verfügt. Der Aufsichtsrat ist verantwortlich für die Bestellung eines Geldwäschebeauftragten, der die Einhaltung der gesetzlichen Vorgaben überwacht und regelmäßig an den Aufsichtsrat berichtet (§ 7 GwG). Der Aufsichtsrat überwacht die Durchführung und regelmäßige Aktualisierung der Risikobewertungen im Hinblick auf Geldwäsche und Terrorismusfinanzierung (§ 5 GwG).

Datenschutz und IT-Sicherheit

Datenschutz-Grundverordnung (DSGVO)

Artikel 24 und 25 DSGVO verpflichten den Aufsichtsrat sicherzustellen, dass die Bank alle Vorgaben der DSGVO einhält, einschließlich der Implementierung eines Datenschutzmanagementsystems. Ein Datenschutzbeauftragter muss bestellt werden, und der Aufsichtsrat überwacht die Einhaltung der Datenschutzrichtlinien (Artikel 37 DSGVO).

BAIT (Bankenaufsichtliche Anforderungen an die IT)

Der Aufsichtsrat überwacht die Einhaltung der BAIT-Vorgaben hinsichtlich der IT-Sicherheit und des Datenschutzes, einschließlich der regelmäßigen Überprüfung und Aktualisierung der Sicherheitsmaßnahmen.

Vergütungssysteme

Institutsvergütungsverordnung (InstVV)

Die Institutsvergütungsverordnung (InstVV) und § 25a Abs. 5 KWG verlangen, dass die Vergütungssysteme der Bank den Anforderungen entsprechen, einschließlich der Berücksichtigung von Nachhaltigkeits- und Risikokriterien. Der Aufsichtsrat überwacht die Implementierung und Einhaltung der Vergütungspolitik.

Ethik und Unternehmensverantwortung

Deutscher Corporate Governance Kodex (DCGK)

Der DCGK fördert eine Kultur der Ethik und Integrität innerhalb der Bank. Der Aufsichtsrat überwacht die Einhaltung entsprechender Verhaltenskodizes und Unternehmensrichtlinien.

Fazit

Die vielfältigen Aufgaben und Pflichten des Aufsichtsrats einer Bank sind entscheidend für die Sicherstellung einer ordnungsgemäßen und gesetzeskonformen Geschäftsführung sowie für das Risikomanagement und die langfristige Stabilität der Finanzinstitute. Der Aufsichtsrat spielt eine zentrale Rolle bei der Überwachung und Sicherstellung, dass alle relevanten gesetzlichen und regulatorischen Anforderungen eingehalten werden, einschließlich der Aspekte ESG, Datenschutz, IT-Sicherheit und der Bekämpfung von Geldwäsche und Terrorismusfinanzierung.

Anhang: Internet-Quellen

- **Kreditwesengesetz (KWG)**
 - § 25a KWG
 - § 25c KWG
 - § 25d KWG
 - § 25h KWG
- **Aktiengesetz (AktG)**
 - § 84 AktG
 - § 91 AktG
 - § 111 AktG
 - § 171 AktG
 - § 172 AktG
- **Handelsgesetzbuch (HGB)**
 - § 170 HGB
- **Geldwäschegesetz (GwG)**
 - GwG
- **Datenschutz-Grundverordnung (DSGVO)**
 - DSGVO
- **Capital Requirements Regulation (CRR)**
 - CRR
- **Deutscher Corporate Governance Kodex (DCGK)**
 - DCGK
- **Mindestanforderungen an das Risikomanagement (MaRisk)**
 - MaRisk
- **Bankenaufsichtliche Anforderungen an die IT (BAIT)**
 - BAIT
- **Institutsvergütungsverordnung (InstVV)**
 - InstVV

- **Deutsche Nachhaltigkeitsstrategie**
 - Deutsche Nachhaltigkeitsstrategie
- **EU-Taxonomie-Verordnung**
 - EU-Taxonomie-Verordnung