

Musterstruktur: KI-Freigabebericht

Ein Freigabebericht ist eine Entscheidungsvorlage, kein Prosastück. Diese Struktur hat sich in Governance-Assessments bewährt und ist auf aufsichtliche Prüfungen ausgelegt. Sie ist als Arbeitsgrundlage und initiale Vorlage zu verstehen, die an System, Branche und Risikoprofil anzupassen ist: klares Soll, dokumentiertes Ist, bewertete Abweichung, codierte Maßnahmen und ein Verdikt, mit dem die Geschäftsleitung rechtssicher entscheiden kann.

Die Verdiktlogik: Drei definierte Ergebnisse

Freigabefähig: Alle Freigabekriterien erfüllt, Restrisiken dokumentiert und akzeptiert. Betrieb ohne Auflagen.

Bedingt freigabefähig: Betrieb zulässig unter benannten Auflagen mit Fristen. Der Normalfall gut geprüfter Systeme, kein Makel.

Nicht freigabefähig: Mindestens ein Ausschlusskriterium verletzt. Betrieb erst nach Nachbesserung und erneuter Prüfung.

Die zehn Gliederungspunkte

1. Deckblatt und Metadaten

Systemname und Version, Zweckbestimmung im Wortlaut, Anbieter und interne Verantwortliche (Owner, DSB, ISB), Berichtsversion, Prüfzeitraum, Verteiler. Ohne Versionierung ist der Bericht nicht prüffest.

2. Executive Summary mit Verdikt

Maximal eine Seite. Verdikt im ersten Satz, danach die drei wichtigsten Feststellungen und die Sofort-Maßnahmen. Die Geschäftsleitung liest oft nur diese Seite; sie muss allein tragfähig sein.

3. Prüfungsgrundlagen (das Soll)

Herangezogene Normen und Aufsichtsmaßstäbe mit Fundstelle (z. B. Art. 26 KI-VO, Art. 30, 35 DSGVO, § 30 BSIG, § 87 Abs. 1 Nr. 6 BetrVG, DSK-Orientierungshilfe KI), interne Richtlinien mit Version, Freigabekriterien und Ausschlusskriterien. Sauber trennen: Der Soll-Soll-Abgleich prüft, ob die interne Richtlinie die regulatorischen Anforderungen abbildet; der Soll-Ist-Abgleich prüft, ob das System der Richtlinie entspricht. Beide gehören in den Bericht. Dieses Kapitel entscheidet über die Prüfsicherheit des gesamten Berichts.

4. Systembeschreibung und Risikoklassifizierung

Funktionsweise in Klartext, Datenflüsse, Schnittstellen, Betriebsmodell (Cloud/On-Premises), Einstufung nach KI-VO (verboten / Hochrisiko / Transparenzpflicht / minimal) mit Begründung entlang Anhang III.

5. Feststellungen je Prüffeld

Getrennt nach Datenschutz, Informationssicherheit, KI-VO-Pflichten, Urheber- und Lizenzrecht (Trainings- und Ausgabedaten), Gleichbehandlung und Bias (AGG), Arbeitsrecht und Mitbestimmung sowie Vertragslage. Die Prüftiefe je Feld richtet sich nach der Lebenszyklusphase des Systems: Vor der Freigabe stehen Transparenz, menschliche Aufsicht und Bias-Korrektur im Vordergrund, mit Blick auf die Betriebsphase zusätzlich Logging (Art. 12 KI-VO) und Post-Market-Monitoring (Art. 72 KI-VO). Jede Feststellung mit Beleg (Dokument, Protokoll, Screenshot mit Datum) und Soll-Bezug.

6. Abweichungsbewertung

Jede Abweichung erhält Risikobewertung (Eintritt x Auswirkung), Normbezug und Einstufung als Auflage (verhindert Freigabe nicht) oder Ausschlusskriterium (verhindert Freigabe).

7. Maßnahmenkatalog

Codiert nach Horizont (Sofort / P1 vor Go-live / P2 / P3) und Aufwand, mit Owner und Frist. Nur Maßnahmen, die realistisch umsetzbar sind; ein Katalog, den niemand abarbeiten kann, erhöht das Haftungsrisiko erheblich.

8. Verdikt und Auflagen

Das Verdikt mit vollständiger Auflagenliste, Fristen und der Regelung, was bei Fristversäumnis gilt (automatischer Betriebsstopp oder Neubewertung).

9. Follow-up und Wirksamkeitsnachweis

Wer prüft wann die Umsetzung, mit welchem Beleg. Eine erledigte Maßnahme ohne Wirksamkeitsnachweis ist in der Prüfung wertlos.

10. Anlagen

Prüfprotokolle, Datenflussdiagramm, DSFA oder Schwellenwertanalyse, Vertragsauszüge, Betriebsvereinbarung oder Stand der Verhandlung.

Qualitätskontrolle: Fünf Fragen vor Versand

- Steht das Verdikt im ersten Satz der Zusammenfassung, und ist es eines der drei definierten?
- Hat jede Feststellung einen Beleg mit Datum und einen ausdrücklichen Soll-Bezug?
- Ist jede Maßnahme mit Owner, Frist und Horizont codiert, und ist der Katalog realistisch abarbeitbar?
- Ist geregelt, was bei Fristversäumnis einer Auflage automatisch gilt?
- Könnte eine externe Prüferin den Bericht ohne mündliche Erläuterung nachvollziehen?

Typische Fehler, die Berichte entwerfen

Beobachtung statt Feststellung

Eine UI-Analyse ohne dokumentiertes Soll produziert Beobachtungen. Erst der Abgleich mit einem definierten Maßstab macht daraus eine Feststellung.

Verdikt in Prosa

Formulierungen wie „sollte beobachtet werden“ verlagern die Entscheidung zurück zum Leser und nehmen dem Bericht seinen Zweck.

Maßnahmen ohne Konsequenzregel

Auflagen ohne definierte Folge bei Nichterfüllung sind Empfehlungen. Prüfer erkennen den Unterschied sofort.

Nächster Schritt

Wir erstellen Freigabeberichte nach dieser Struktur oder bauen sie mit Ihrer Revision als Standard auf, inklusive Soll-Dokumentation je KI-System.

Kontakt: governance-first.de · Questax Systems GmbH, Heidelberg

Wichtiger Hinweis zur Nutzung dieses Dokuments. Dieses Dokument dient der ersten Orientierung und als initiale Vorabprüfung. Es stellt weder eine abschließende Bewertung noch eine Rechtsberatung im Sinne des Rechtsdienstleistungsgesetzes (RDG) dar und ersetzt keine einzelfallbezogene Prüfung durch qualifizierte Fachanwälte oder zertifizierte Compliance-Expertinnen und -Experten. Gesetzliche Fristen und Pflichten sind nach bestem Wissen zum angegebenen Stand wiedergegeben; maßgeblich sind stets die amtlichen Rechtstexte und die aktuelle Verwaltungspraxis der zuständigen Aufsichtsbehörden. Trotz sorgfältiger Erstellung wird keine Gewähr für Vollständigkeit, Richtigkeit und Aktualität übernommen. Eine Haftung der Questax Systems GmbH für Entscheidungen, die allein auf Grundlage dieses Dokuments getroffen werden, ist ausgeschlossen.