A. Normen- & Struktur-Kurzliste / Haftungs-, Revisions- und Dokumentationspflichten

I. Europäische Ebene

1. EU-KI-Verordnung (VO (EU) 2024/1689 – „AI Act“)

a. Art. 3 Nr. 1, 3, 4 (Begriffe: KI-System, Anbieter, Betreiber)
b. Art. 6, Anhang III (Hochrisiko-KI – KRITIS-Bezug)
c. Art. 8–15 (Pflichten Hochrisiko-KI: Risikomanagement, Daten-Governance, Dokumentation, Logging, Human Oversight)
d. Art. 11, 12 (Technische Dokumentation & Protokollierung)
e. Art. 26 (Pflichten der Betreiber)
f. Art. 73 ff. (Meldepflichten schwerwiegender Vorfälle)
g. Art. 99 ff. (Sanktionen)

2. Produkthaftungsrecht (EU-Ebene)

a. Neue **Produkthaftungs-VO / -RL**: Software & KI als Produkt
b. Beweislast-erleichterungen bei Intransparenz („Black Box“)

3. NIS-2-Richtlinie (RL (EU) 2022/2555)

a. Sicherheits-, Melde- und Nachweispflichten für KRITIS-nahe Akteure

II. Nationale Ebene (Deutschland)

1. BSI-Gesetz (BSIG)

a. § 2 Abs. 10 BSIG (KRITIS-Begriff – Übergang zur „kritischen Anlage“)
b. § 8a BSIG (ISMS, Stand-der-Technik-Pflicht, Nachweispflichten)
c. § 8b BSIG (Meldepflichten)

2. BGB

a. § 823 Abs. 1, Abs. 2 BGB (Verkehrssicherungspflichten)
b. Organisationsverschulden (ständige Rspr.)

3. Produkthaftungsgesetz (neu)

a. Zurechnung bei Software- und KI-Fehlern
b. Relevanz von Dokumentation für Haftungsentlastung

4. Handels- und Gesellschaftsrecht

a. § 91 Abs. 2 AktG analog (Risikofrüherkennung)
b. Compliance-Pflichten der Geschäftsleitung

III. Governance- & Soft-Law-Ebene

- ISO/IEC 23894 (AI Risk Management – in Entwicklung)

- ISO/IEC 27001 (ISMS)
- BSI-Grundschutz
- Interne Revisionsstandards (Three Lines of Defense)

B. Hintergrundmemo & Mockup-Leitplanken / Haftungs-, Revisions- und Dokumentationspflichten

I. Zentrale Klarstellung

Der im AI Case Sprint entwickelte digitale Mockup:

- ist **kein KI-System i.S.d. Art. 3 Nr. 1 KI-VO**,
- entfaltet **keine Entscheidungswirkung**,
- verarbeitet **keine Echt- oder personenbezogenen Daten**,
- ist **nicht produktiv**, **nicht angebunden**, **nicht automatisierend**.

Keine unmittelbaren Haftungs-, Revisions- oder Dokumentationspflichten werden ausgelöst.
Der Mockup ist **rechtlich inert** und dient ausschließlich der **Management- und Entscheidungsunterstützung**.

ABER (entscheidend):
Der Mockup **simuliert bewusst einen später potenziell hochregulierten Zielzustand**. Genau deshalb müssen **Haftungs-, Revisions- und Dokumentationslogiken konzeptionell mitgedacht werden**.

II. Haftungslogik – warum Dokumentation der Dreh- und Angelpunkt ist

Die Literatur ist hier eindeutig:

- KI-Systeme sind **keine Rechtssubjekte**,
- aber ihr **Autonomiegrad verschärft Organisations-, Überwachungs- und Dokumentationspflichten** der Unternehmen

Kernaussage für Trianel (Legal/Compliance):

Haftung entsteht nicht primär durch den KI-Fehler, sondern durch **fehlende Governance, fehlende Dokumentation und fehlende Kontrollierbarkeit**.

Besonders relevant:

- **Beweislastumkehr** bei unzureichender Dokumentation,
- **Verschuldensunabhängige Produkthaftung**, wenn KI später als Produkt qualifiziert wird,
- **Organisationsverschulden**, wenn kein belastbares KI-Governance-Framework existiert.

Der Mockup muss **sichtbar machen**,

- **wer** wofür verantwortlich ist,
- **wo** Entscheidungen entstehen,
- **wo** Menschen eingreifen,
- **wo** dokumentiert würde.

III. Revisionslogik – KI als Prüfobjekt

Aus Sicht von **Revision & Audit** ist KI kein Sonderfall, sondern ein **neuer Risikotreiber**.

Die Fachliteratur betont:

- KI muss **in bestehende Compliance-, Kontroll- und Revisionsstrukturen integriert** werden,
- nicht parallel oder isoliert

Zentrale Revisionsfragen (Mockup-relevant):

- Ist der Entscheidungsprozess **nachvollziehbar rekonstruierbar**?
- Gibt es **Audit-Trails**?
- Sind **Human-Oversight-Punkte** definiert?
- Existieren **Notfall- und Abschaltmechanismen** („Kill-Switch")?

Visualisiere **Audit-Einstiegspunkte**, nicht Technik:

- Protokoll-Symbolik,
- Freigabe-Checks,
- Eskalationspfade.

IV. Dokumentationspflichten

Die KI-VO macht Dokumentation zur **Compliance-Währung** schlechthin:

- Art. 11 KI-VO: technische Dokumentation,
- Art. 12 KI-VO: Logging & Nachvollziehbarkeit,
- Art. 9 KI-VO: Risikomanagementsystem,
- Art. 14 KI-VO: Human Oversight,
- Art. 15 KI-VO: Robustheit & Cybersicherheit

Dokumentation ist nicht Selbstzweck, sondern haftungsrechtliche Absicherung.

Fehlt sie:

- steigt Haftungsrisiko,
- greift Beweislastumkehr,
- drohen Bußgelder und Governance-Versagen.

Der Mockup muss **nicht dokumentieren**, aber **zeigen, was dokumentiert würde**:

- Datenquellen (hypothetisch),
- Entscheidungslogik,
- Kontrollpunkte,
- Rollen & Verantwortlichkeiten.

V. Besonderheit KRITIS / Energiewirtschaft

Für Energie-KRITIS gilt:

- **nicht jede KI ist automatisch Hochrisiko-KI**,
- aber KI als **Sicherheitsbauteil** in kritischen Anlagen regelmäßig schon

Besonders wichtig:

- KI für **Cybersicherheit** ist teilweise ausgenommen,
- KI zur **Steuerung oder Absicherung kritischer Prozesse** dagegen hochsensibel.

Deutlich machen:

- **Legal/Compliance-Use-Case ≠ operative Steuerung**,
- Fokus auf **Vorbereitung, Bewertung, Unterstützung**, nicht auf Eingriff.

Kurzfazit für das Sprint-Narrativ: Mockup **löst keine Haftung aus**, aber er **verhindert spätere Haftung**, indem er Governance-, Revisions- und Dokumentationsanforderungen **vorweg strukturiert**.