A. Normen- & Struktur-Kurzliste / Auditierbarkeit & Nachvollziehbarkeit von KI-Entscheidungen

I. EU AI Act (KI-VO) – zentrale Normanker

1. Art. 11 KI-VO – Technische Dokumentation

- Verpflichtung zur Dokumentation der Systemauslegung, Zweckbestimmung und Funktionsweise
- Ziel: **Nachvollziehbarkeit für Aufsicht und interne Prüfung**

Für den Mockup: Darstellung **wo** Dokumentation entstünde, **nicht** deren Inhalt.

2. Art. 12 KI-VO – Protokollierung (Logging)

- Hochrisiko-KI muss Ereignisse und Nutzung protokollieren
- Grundlage für Audits, Fehleranalyse und Haftungszuordnung

Für den Mockup: Konzeptionelle **Audit-Trail-Placeholder** (kein echtes Logging).

3. Art. 13 KI-VO – Transparenz & Informationspflichten

- Nachvollziehbarkeit der Systemlogik für Nutzer
- Grenzen, Zweck und Einsatzbedingungen müssen verständlich sein

Relevanz: Auditierbarkeit setzt **Transparenz über Funktionslogik** voraus.

4. Art. 14 KI-VO – Menschliche Aufsicht

- Sicherstellung, dass KI-Outputs:
    - überprüfbar,
    - übersteuerbar,
    - abbrechbar sind

Audit-Bezug: Ohne „human in the loop“ **keine revisionsfeste Verantwortlichkeit**.

5. Art. 26 KI-VO – Pflichten der Betreiber

- Überwachung des Betriebs
- Sicherstellung der Konformität
- Korrekturmaßnahmen bei Abweichungen

Für den Mockup: Darstellung von **Kontroll- und Eskalationspunkten**, nicht deren Vollzug.

II. Unternehmens- & Compliance-rechtliche Referenzen

1. Ordnungsgemäße Organisation / CMS (IDW PS 980)

- Dokumentation
- Kontrollen
- Überwachung
- Nachweisbarkeit

Auditierbarkeit = **Kernerwartung an Compliance-Systeme** (vgl. Integration der KI-VO in bestehende CMS-Strukturen).

2. Revisionsrechtliche Anforderungen

- Prüfpfade müssen:
  - eindeutig,
  - reproduzierbar,
  - personen- und zeitbezogen sein

KI-gestützte Prozesse ohne Audit-Trail = **Revisionsrisiko**.

III. Struktur-Bausteine für den Mockup

Die folgenden Elemente dürfen **rein konzeptionell** visualisiert werden:

1. **Audit-Trail-Logik** („Welche Schritte wären prüfbar?“)
2. **Rollen & Verantwortlichkeiten** (Nutzer – Legal – Compliance – Revision)
3. **Kontroll- & Freigabepunkte** (KI-Vorschlag ≠ Entscheidung)
4. **Eskalations- & Abbruchlogik** (Governance-Mechanismus, kein Technikdetail)
5. **Dokumentations-Touchpoints** (Zweck, Nutzung, Abweichung, Entscheidung)

IV. Explizite Abgrenzung (zwingend)

Der Mockup:

- erfüllt **keine** Auditpflichten
- erzeugt **keine** Protokolle
- ersetzt **keine** interne oder externe Prüfung
- begründet **keine** Konformität
- Aber: zeigt **anschlussfähige Governance-Strukturen**

V. 1-Satz-Leitlinie

„Der Mockup visualisiert Audit- und Nachvollziehbarkeitslogiken als Governance-Prinzip – nicht als erfüllte Prüf- oder Compliance-Pflichten.“

B. Hintergrundmemo & Mockup-Leitplanken (Legal / Compliance / Revision)

I. Ausgangspunkt: Mockup-Prämisse (rechtlich entscheidend)

Für die rechtliche Einordnung ist strikt festzuhalten: Der digitale Mockup **unterliegt selbst keinen Audit-, Protokollierungs- oder Nachweispflichten**, weder aus der KI-VO noch aus DSGVO, IT-Sicherheitsrecht oder Revisionsrecht.

ABER: Der Mockup bildet **einen später potenziell auditpflichtigen Zielprozess ab**. Er ist damit **antizipierende Governance-Visualisierung**, nicht Compliance-Pflichterfüllung. Diese Differenz ist zentral – und wird im Mockup **explizit markiert**.

1. Warum Auditierbarkeit trotzdem zentraler Mockup-Inhalt ist

Die von uns adressierten Use Cases (Legal / Compliance / Revision) liegen **typischerweise im Hochrisiko- oder jedenfalls sensiblen Bereich**, insbesondere:

- Risiko- und Rechtsbewertung
- Compliance-Vorprüfungen
- interne Kontrollmechanismen
- revisionsnahe Entscheidungsunterstützung

Die Fachliteratur ist hier eindeutig:

Auditierbarkeit ist der Dreh- und Angelpunkt rechtmäßiger KI-Governance, weil KI keine Rechtssubjekte sind, Verantwortung aber **voll beim Unternehmen verbleibt** .

II. Normativer Referenzrahmen (ohne Überdehnung)

1. EU AI Act (KI-VO)

Die KI-VO verankert Auditierbarkeit **als strukturelles Prinzip**, insbesondere bei Hochrisiko-KI:

- **Dokumentationspflichten** (Art. 11 KI-VO)
- **Protokollierung / Logging** (Art. 12 KI-VO)
- **Nachvollziehbarkeit der Funktionsweise** (Art. 13, 14 KI-VO)
- **menschliche Aufsicht („human in the loop“)**
- **Life-Cycle-Monitoring** (Art. 26 KI-VO)

Kernidee: Auditierbarkeit ist **keine punktuelle Kontrolle**, sondern **durchgängige Nachvollziehbarkeit über den gesamten Lebenszyklus** eines KI-Systems .

2. Compliance-Dogmatik (IDW PS 980 / Unternehmensrecht)

Aus Unternehmens- und Revisionssicht gilt:

- Auditierbarkeit ist **Teil ordnungsgemäßer Organisation**
- fehlende Nachvollziehbarkeit = **Organisationsverschulden**
- besonders relevant bei:
    - Compliance-Funktionen
    - internen Kontrollsystemen
    - risikorelevanten Entscheidungen

Die KI-VO lässt sich **bruchfrei in bestehende CMS integrieren**, insbesondere über:

- Risikoanalyse
- Dokumentation
- Überwachung
- kontinuierliche Verbesserung .

III. Was „Auditierbarkeit“ konkret bedeutet (inhaltlich)

Die Literatur differenziert klar zwischen vier Ebenen:

1. Entscheidungs-Nachvollziehbarkeit

- Warum kam die KI zu einem bestimmten Output?
- Welche Faktoren waren maßgeblich?
- Wo liegen Unsicherheiten / Bias-Risiken?

Wichtig: **Erklärbarkeit ≠ vollständige Transparenz des Modells**, sondern **nachvollziehbare Entscheidungslogik**.

2. Prozess-Auditierbarkeit

- Wer hat die KI genutzt?
- In welchem Kontext?
- Mit welcher Zielsetzung?
- Mit welchen Eingabedaten (hypothetisch)?

Zentral für Revision und Haftungsfragen .

3. Kontroll- & Interventionsfähigkeit

- Möglichkeit menschlichen Eingreifens
- Eskalationspfade
- Notfall-Mechanismen („Kill Switch“ als Governance-Symbol, nicht Technikdetail)

Kernelement wirksamer Aufsicht.

4. Dokumentation & Audit-Trail

- Protokollierung von Nutzung, Ergebnissen, Abweichungen
- Grundlage für:
    - interne Audits
    - externe Prüfungen
    - Haftungsabwehr

IV. Konsequenzen für den Mockup (entscheidend!)

Der Mockup darf und soll **keine echten Auditpflichten simulieren**, aber:

Er MUSS visualisieren:

- **wo Audit-Informationen entstehen würden**
- **wer Verantwortung trägt (Mensch, nicht KI!)**
- **wo Kontroll- und Freigabepunkte liegen**
- **wie Nachvollziehbarkeit gedacht ist**

Ziel: **Governance-Readiness sichtbar machen**, nicht Compliance vortäuschen.

Der Mockup SOLL zeigen:

- Rollen:
    - Fachanwender
    - Legal/Compliance
    - Revision
- Informationsflüsse:
    - Input → KI-Output → menschliche Bewertung → Entscheidung
- Dokumentationslogik:
    - „Was würde protokolliert werden, wenn produktiv?“

Der Mockup DARF NICHT:

- den Eindruck erwecken,
    - dass echte Logs existieren
    - dass Prüfungen erfolgen
    - dass rechtliche Pflichten erfüllt sind

-> Ein Expliziter Disclaimer auf Mockup-Ebene ist zwingend.

V. Mockup-Checkliste

Visual / Konzeptuell enthalten sein sollten:

- Kennzeichnung: „nicht produktiv / keine echte Auditspur“
- Menschliche Entscheidung als letzte Instanz
- Klar benannte Kontroll- und Freigabepunkte
- Darstellung hypothetischer Audit-Informationen
- Trennung: KI-Vorschlag ≠ Entscheidung
- Rollen & Verantwortlichkeiten sichtbar
- Eskalations- und Abbruchlogik (konzeptionell)

VI. Einordnung für Trianel (KRITIS-sensibel, aber korrekt)

Für Trianel als KRITIS-Unternehmen gilt:

- Auditierbarkeit ist **nicht optional**, sondern **erwarteter Standard**
- insbesondere bei:
    - rechtlichen Bewertungen
    - Compliance-Unterstützung
    - revisionsnahen Use Cases

Der Mockup zeigt:

dass Trianel Governance-, Kontroll- und Revisionsanforderungen von Anfang an mitdenkt,

ohne vorschnell regulatorische Pflichten auszulösen.

→ **Quintessenz: Auditierbarkeit ist kein technisches Feature, sondern ein Governance-Prinzip.** Der Mockup bildet dieses Prinzip sichtbar ab – ohne rechtliche Wirkungen zu entfalten.