A. Normen-Kurzliste Mockup / KRITIS & IT-Sicherheit

I. Zentrale nationale Normen

- **§ 2 Abs. 10 BSIG** – Begriff der Kritischen Infrastruktur
  (Einrichtungen/Anlagen mit hoher Bedeutung für das Gemeinwesen; erhebliche Versorgungsengpässe oder Gefährdung der öffentlichen Sicherheit bei Ausfall)
  → Grunddefinition, anlagenbezogen, nicht unternehmensbezogen.
- **§§ 8 ff. BSIG** – Betreiberpflichten Kritischer Infrastrukturen
  (technische und organisatorische Maßnahmen, Stand der Technik, institutionelle Strukturen, Meldewege)
  → **Nur relevant bei späterer Produktivsetzung**, im Mockup rein konzeptionell.
- **BSI-Kritisverordnung (BSI-KritisV)**
  (Konkretisierung über Sektoren & Schwellenwerte)
  → Entscheidender Filter: **Ob** ein späterer KI-Use Case überhaupt in den KRITIS-Anwendungsbereich fällt.

II. Energiesektorspezifische Spezialregeln

- **Energierechtliche Spezialnormen (u.a. §§ 11 Ia ff. EnWG)**
  → Können **vorrangig** gegenüber dem allgemeinen BSIG greifen, wenn der Use Case operative Energie-IT berührt.
  → Für den Legal/Compliance-Use Case: **Prüfhinweis**, kein unmittelbarer Anwendungsfall.

III. Europäische Rahmensetzung (Kontext & Zukunft)

- **CER-Richtlinie (EU) 2022/2557** – Schutz kritischer Einrichtungen
  → Resilienz-Logik (cyber + physisch + organisatorisch).
- **NIS-Systematik (NIS-1 / NIS-2)**
  → Europäische Grundlage für die §§ 8 ff. BSIG; verschärfte Governance- und Nachweispflichten.

B. Hintergrundmemo

I. Ausgangspunkt: Trianel im KRITIS-Kontext

Der Energiesektor ist nach einhelliger Auffassung **klassischer KRITIS-Sektor**.
Energieinfrastrukturen bilden eine **systemische Lebensader** für nahezu alle weiteren kritischen Bereiche.

Digitalisierung und Vernetzung sind **Voraussetzung** für Energiewende und Marktintegration – erhöhen aber zugleich die **Verwundbarkeit**.

Für Trianel folgt daraus:

- KRITIS-Relevanz hängt **nicht** am Unternehmenslabel,
- sondern an **konkreten Anlagen, Diensten oder Funktionen**.

→ Legal-/Compliance-Funktionen sind **typischerweise nicht selbst KRITIS**, können aber **mittelbar KRITIS-relevant** sein, wenn sie Entscheidungen, Governance oder Absicherung kritischer Prozesse beeinflussen.

II. Begriff der Kritischen Infrastruktur – rechtliche Präzision

Der KRITIS-Begriff ist **historisch gewachsen** und **mehrschichtig**:

- Ursprünglich systemische Betrachtung von Verwundbarkeiten (US-Diskurs, PCCIP),
- Übertragung in deutsches Recht über AG KRITIS, BSIG, KRITIS-Strategien,
- heute: **anlagen- und funktionsbezogene Definition** (§ 2 Abs. 10 BSIG).

Wichtig für den Sprint:

- **Nicht jedes IT-System** in einem Energieunternehmen ist KRITIS.
- Entscheidend ist, ob der **Ausfall** zu erheblichen Versorgungsengpässen oder Sicherheitsgefährdungen führt.

Konsequenz für den Mockup: Der Use Case muss **explizit als „unterstützend / governance-bezogen“** gekennzeichnet werden – nicht als systemkritische Steuerung.

III. Schutzdimensionen: Cyber + physisch + organisatorisch

Moderne KRITIS-Regulierung beschränkt sich nicht mehr auf IT-Sicherheit:

- Cyberangriffe,
- physische Sabotage,
- hybride Bedrohungen,
- Kaskadeneffekte zwischen Sektoren.

Die CER-Richtlinie verstärkt diesen **Resilienz-Ansatz**.

Für Legal/Compliance-KI heißt das:

- Der Use Case selbst ist **kein Sicherheitsrisiko**,
- aber Teil der **organisatorischen Resilienz** (Dokumentation, Nachvollziehbarkeit, Kontrolle).

Mockup-Implikation: Visualisierung von **Kontroll-, Freigabe- und Eskalationspunkten** ist rechtlich sinnvoll – auch ohne operative Wirkung.

IV. Pflichtenlogik nach BSIG – nur antizipiert, nicht ausgelöst

Die §§ 8 ff. BSIG verpflichten **Betreiber kritischer Infrastrukturen** u.a. zu:

- technischen und organisatorischen Maßnahmen (Stand der Technik),
- institutionellen Strukturen (zentrale Meldestellen),
- Nachweis- und Meldepflichten.

Für den Sprint gilt:

- Der Mockup **löst diese Pflichten nicht aus**,
- darf sie aber **nicht ignorieren**, wenn er als Entscheidungsgrundlage dient.

Rechtsdogmatisch sauber ist daher:

- Darstellung einer **„anschlussfähigen Governance-Logik“**,
- ohne konkrete Implementierungszusagen.

V. Energierechtliche Spezialität

Die Literatur weist klar darauf hin:

Im Energiesektor existieren **spezialgesetzliche Sicherheitsregelungen**, die dem allgemeinen IT-Sicherheitsrecht **vorgehen können**.

Für Legal/Compliance-KI:

- regelmäßig **nur mittelbar relevant**,
- aber zwingend als **Prüfmarker** im Entscheidungsprozess.

VI. Klare Leitlinie für den Mockup (Zusammenfassung)

Der Mockup sollte für Feld 1 **sichtbar machen**, dass:

1. Der Use Case **nicht selbst KRITIS** ist,
2. aber **in einem KRITIS-sensiblen Umfeld** verortet ist,
3. spätere Umsetzung:
    a. BSIG / BSI-KritisV / Energierecht **prüfen muss**,
    b. Governance, Dokumentation und Eskalation voraussetzt,
4. Legal & Compliance eine **resilienzstärkende Rolle** spielen, keine operative Steuerungsrolle.