A. Normen- & Struktur-Kurzliste / Vermeidung von Vendor-Lock-in & Schatten-IT

I. Europäische Ebene

1. EU-KI-Verordnung

a. Art. 4 KI-VO – *AI Literacy*
→ Schulungspflicht als Governance-Instrument gegen unkontrollierte KI-Nutzung
b. Art. 9, 10, 11 KI-VO – Risikomanagement, Daten-Governance, Dokumentation
→ Nur beherrschbare Systeme sind audit- und wechsel-fähig
c. Art. 26 KI-VO – Pflichten der Betreiber
→ organisatorische Kontrolle, kein „Blindflug" bei Drittanbietern

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

a. Lieferketten- und Supply-Chain-Security
b. Resilienz- und Abhängigkeitskontrolle bei kritischen Dienstleistern

3. EU Data Act (VO (EU) 2023/2854)

a. Recht auf Anbieterwechsel
b. Interoperabilität & Portabilität von Daten
c. Verbot übermäßiger Wechselhindernisse („Lock-in-Barrieren")

4. EU-Cyber-Resilience-Logik (CRA-Kontext)

a. Erwartung robuster, kontrollierbarer digitaler Lieferketten

II. Nationale Ebene (Deutschland)

1. BSI-Gesetz (BSIG)

a. § 2 Abs. 10 BSIG – KRITIS-Bezug
b. § 8a BSIG – Stand-der-Technik-Pflicht, ISMS, Nachweispflichten
→ Schatten-IT = strukturelle Sicherheitslücke

2. DSGVO

a. Art. 5, 24, 32 DSGVO – Rechenschaft, Sicherheit, TOMs
b. Datenabfluss durch nicht autorisierte KI-Tools = Compliance-Verstoß

3. Gesellschafts- & Organhaftungsrecht

a. § 93 AktG / § 43 GmbHG – Organisationsverschulden
b. fehlende KI-Governance = haftungsrelevant

III. Governance- & Revisionsstandards

- IDW PS 980 (CMS)
- Three Lines of Defense
- ISO/IEC 27001 (ISMS)
- BSI-Grundschutz

B. Hintergrundmemo & Mockup-Leitplanken / Vermeidung von Vendor-Lock-in & Schatten-IT

I. Ausgangspunkt

Die Fachliteratur ist eindeutig: **Vendor-Lock-in und Schatten-IT sind keine bloßen IT-Probleme, sondern Governance- und Haftungsrisiken.**

Gerade im **KRITIS-Umfeld** wirken sie als **systemische Schwachstellen**, weil sie:

- Kontrollverlust erzeugen,
- Auditierbarkeit unterlaufen,
- Resilienz und Reaktionsfähigkeit beeinträchtigen,
- Haftungs- und Organisationsverschulden begründen.

Legal/Compliance ist hier Schlüsselstelle, nicht Technik.

II. Schatten-IT: rechtliche Einordnung

1. Begriff & Risiko

Schatten-IT liegt vor, wenn:

- Mitarbeiter **nicht freigegebene KI-Tools** nutzen,
- außerhalb definierter Prozesse,
- ohne Dokumentation, Kontrolle oder Vertrag.

Im KI-Kontext besonders gefährlich:

- öffentliche LLMs,
- Cloud-basierte Tools mit unbekannter Datenverwendung.

2. Rechtliche Bewertung

a) BSIG / NIS-2

- Unkontrollierte KI-Nutzung widerspricht:
    - ISMS-Pflichten,
    - Nachweisanforderungen,
    - Stand-der-Technik-Gebot.

Für KRITIS: **struktureller Verstoß**, nicht Bagatelle.

b) DSGVO

- Weitergabe personenbezogener oder vertraulicher Daten an externe KI-Dienste:
    - Verletzung Art. 5, 24, 32 DSGVO,
    - Bußgeld- und Haftungsrisiken.

c) KI-VO (Art. 4 – AI Literacy)

- Fehlende Schulung fördert Schatten-IT.
- AI Literacy wird zum **präventiven Compliance-Werkzeug**.

d) Organhaftung

- Keine Richtlinien, keine Schulung, keine Kontrolle
  ⇒ **Organisationsverschulden** der Geschäftsleitung.

3. Mockup-Leitplanken (Schatten-IT)

Mockup soll **Governance sichtbar machen**:

Visualisierung:

- genehmigter KI-Einsatzpfad
- klare „No-Go-Zonen“
- Zuständigkeit Legal/Compliance

Konzeptionelle Artefakte:

- KI-Policy-Verweis
- Schulungs-/Freigabe-Logik
- Hinweis „nicht freigegebene Tools unzulässig“

Keine Darstellung:

- freier Tool-Auswahl,
- „Bring-your-own-AI“.

III. Vendor-Lock-in: rechtliche Einordnung

1. Begriff & Risiko

Vendor-Lock-in liegt vor, wenn:

- KI-Modelle, Daten oder Schnittstellen **nicht portabel** sind,
- Wechsel technisch oder wirtschaftlich faktisch unmöglich ist.

Im KRITIS-Kontext besonders kritisch:

- Abhängigkeit von einzelnen Cloud-/KI-Providern,
- geopolitische, wirtschaftliche oder technische Ausfallrisiken.

2. Rechtliche Bewertung

a) NIS-2 / KRITIS-Resilienz

- Lieferketten-Resilienz ist **rechtliche Pflicht**.
- Ein Lock-in, der den Betrieb gefährdet, widerspricht dem Schutzzweck.

b) EU Data Act

- Gesetzgeberisches Ziel: **Abbau von Lock-in-Effekten**
- Recht auf Wechsel, Interoperabilität, Portabilität.

c) Haftungs- & Revisionssicht

- Kein Exit-Konzept =
    - fehlende Notfallvorsorge,
    - Revisionsmangel,
    - haftungsrelevant.

3. Der Mockup sollte **konzeptionell zeigen**:

Prinzipien:

- Provider-Neutralität
- modulare Architektur (gedanklich)
- Daten- & Modell-Portabilität

Governance-Artefakte:

- Exit-Strategie-Hinweis
- Multi-Provider-Option
- Vertrags-/Compliance-Check-Touchpoint

Keine Darstellung:

- exklusiver Anbieterbindung
- proprietärer „One-Way-Architekturen“.

IV. Revision & Dokumentation (verbindendes Element)

Sowohl Schatten-IT als auch Vendor-Lock-in sind **nur beherrschbar durch Dokumentation**:

- KI-Inventar (was ist erlaubt?)
- Richtlinien (was ist verboten?)
- Verträge (wer haftet?)
- Exit-Konzepte (was passiert im Notfall?)

Revision prüft nicht KI – sondern Governance.

Mockup:

- löst **keine Pflichten aus**,
- zeigt aber, **wie Trianel Governance-Risiken strukturiert adressiert**,
- und verhindert genau jene Risiken, die Aufsicht, Revision und Gerichte später sanktionieren.