This checklist is designed to bridge the communication gap between the **Technical (CISO)** and the **Legal/HR** departments. In 2026, most standard German D&O policies still contain "Cyber Exclusions" that can leave you personally exposed.

Hand this document to your Legal Counsel or Insurance Broker to perform a "Gap Audit."

2026 CISO D&O Policy Audit Checklist (NIS2 Germany)

Section 1: The "Insured Person" Definition

- [ ] **CISO Role Specificity:** Is the role of "Chief Information Security Officer" (or your specific job title) explicitly listed as an **"Insured Person"** (*versicherte Person*)?
    - *Why:* Many German policies only cover formal "Management Bodies" (Board/MDs). As a non-board CISO, you need a specific endorsement.
- [ ] **Non-Officer Coverage:** Does the policy cover "employees acting in a managerial capacity"?
- [ ] **Past, Present, and Future:** Does the coverage extend to former CISOs? (Crucial for NIS2, as lawsuits often surface 18–24 months after a breach).

Section 2: Scope of Claims & Recourse Protection

- [ ] **Internal Recourse (*Regressanspruch*):** Does the policy explicitly cover claims brought by the **Company against the CISO**?
    - *Why:* Under §38 BSIG, the company is often *legally forced* to sue you to recover fines. Standard D&O often excludes "Insured vs. Insured" claims. You need a **"Cyber Recourse Extension."**
- [ ] **Administrative Fines:** Does the policy cover **"Defense Costs"** for regulatory proceedings by the BSI?
    - *Note:* In Germany, insurance cannot pay the *fine* itself, but it **can and should** pay the legal fees to fight it.
- [ ] **Gross Negligence (*Grobe Fahrlässigkeit*):** Is there a "Severability" clause ensuring that the "Gross Negligence" of the CEO doesn't void *your* coverage?

Section 3: Removal of Cyber Exclusions

- [ ] **The "Data Breach" Carve-Back:** Check for an exclusion titled "Cyber & Data." You must ensure there is a **"Carve-back"** for *Management Liability* (i.e., the policy doesn't

pay for the data loss, but it *does* pay for the CISO's defense against mismanagement charges).

- [ ] **"Confidential Information" Exclusion:** Ensure that a breach of NIS2 reporting obligations isn't excluded under "unauthorized disclosure of information."

Section 4: Defense Costs & Limits

- [ ] **Dedicated CISO Sub-Limit:** Does the CISO have a **separate, dedicated limit** for legal defense?
    - *Why:* In a major crisis, the CEO and CFO will hire the most expensive lawyers and can exhaust a €10M limit in months. A dedicated €1M–€2M sub-limit for the CISO is a 2026 industry standard.
- [ ] **Side A "Difference in Conditions" (DIC):** If the company becomes insolvent or refuses to indemnify you (common after a scandal), does the policy switch to **Side A (Individual) coverage** immediately?

Section 5: 2026 Regulatory Specifics

- [ ] **Mandatory Training Defense:** If a claim arises, will the insurer provide coverage even if the "Mandatory Management Training" (§38 BSIG) was delayed or incomplete?
- [ ] **BSI Reporting Windows:** Does the policy trigger coverage for legal advice *before* a formal claim is filed (e.g., during the 24-hour notification window)?