**LLM Risk Assessment Criteria & Prompt Template**

**1 Severity Scoring (ISO 31000‑style 5 × 5 matrix)**

| **Impact → / Likelihood ↓** | **1 Rare** | **2 Unlikely** | **3 Possible** | **4 Likely** | **5 Almost‑Certain** |
| --- | --- | --- | --- | --- | --- |
| **1 Negligible (C1)** | 1 | 2 | 3 | 4 | 5 |
| **2 Minor (C2)** | 2 | 4 | 6 | 8 | 10 |
| **3 Moderate (C3)** | 3 | 6 | 9 | 12 | 15 |
| **4 Major (C4)** | 4 | 8 | 12 | 16 | 20 |
| **5 Catastrophic (C5)** | 5 | 10 | 15 | 20 | 25 |

*Severity label* = **Critical (C5)** if score ≥ 20, **High (C4)** 15–19, **Medium (C3)** 8–14, **Low (C2)** 4–7, **Info (C1)** 1–3.

**2 Risk Type Taxonomy (pick one per risk)**

| **Code** | **Meaning** |
| --- | --- |
| **REQ\_NONFUNC** | Non‑functional requirement gap (performance, reliability, usability, etc.) |
| **SECURITY** | Security or privacy vulnerability |
| **PLANNING** | Impractical or unrealistic planning / scheduling / resourcing |
| **REDUNDANCY** | Redundant or duplicate effort/config/design |
| **PERFORMANCE** | Potential performance or scalability bottleneck |
| **QUALITY** | Insufficient test coverage / quality assurance risk |
| **DEPLOYMENT** | Release / infrastructure / IaC / configuration risk |
| **MAINTAINABILITY** | Long‑term maintenance or tech‑debt risk |
| **OTHER** | Anything not covered above (specify inside description) |

**3 Assessment Instructions (for the LLM)**

1. Read the supplied artefact in context of the declared **SDLC stage**.
2. Identify **as many distinct risks as you can** strongly supported by the artefact.
3. For each risk provide:
   * Risk\_ID – short slug (e.g. "DESIGN-SECURITY-01").
   * Severity – one of Critical, High, Medium, Low, Info (use table 1).
   * Likelihood (1–5) and Impact (1–5) that produced the severity.
   * Risk\_Type – code from §2.
   * Description – ≤ 40 words, actionable.
   * Rationale – ≤ 25 words citing evidence (line numbers, section titles, etc.).
4. **If no material risks exist, return an *empty JSON array*.**

**4 Output Format (strict)**

Return *only* a **single fenced code block** containing a **valid JSON array**. Example:

[

{

"Risk\_ID": "DESIGN-SECURITY-01",

"Severity": "High",

"Likelihood": 4,

"Impact": 4,

"Risk\_Type": "SECURITY",

"Description": "OAuth tokens are hard‑coded in API spec, exposing credentials.",

"Rationale": "Lines 120‑140 in spec show embedded tokens without encryption."

}

]

No commentary, markdown, or prose outside the code fence.