Strategic Risk Ingestion Generative AI Prompt

A Generative AI prompt that turns your completed Enterprise Risk Register into a prioritized, business-focused action plan.

One of the greatest challenges facing SMBs is not identifying risks—it is deciding which risks deserve immediate attention. Most organizations operate with limited budgets, small teams, and competing business priorities, making it difficult to address every vulnerability at once. Unfortunately, many organizations either react to the loudest problem of the day or focus exclusively on technical severity scores that fail to account for the broader impact on business operations.

The Pragmatic GRC Methodology™ takes a different approach. Effective risk management is not about eliminating every risk; it is about making informed decisions that protect the organization's ability to operate, generate revenue, and achieve its strategic objectives. Risks should be prioritized based on their potential impact to the business, the likelihood of occurrence, existing controls, and the resources required to implement practical mitigations.

The Strategic Risk Ingestion Generative AI Prompt accelerates this analysis by transforming your completed Enterprise Risk Register into a business-focused action plan. Rather than simply ranking technical vulnerabilities, it evaluates each risk through the lens of operational resilience, financial impact, regulatory obligations, customer trust, and organizational capacity. The result is a prioritized roadmap that helps leadership focus limited resources where they can reduce business risk the most.

Before You Run the Prompt

Gather these inputs:

- Enterprise Risk Register
- Known vulnerabilities
- Existing security controls
- Business criticality
- Revenue-generating systems
- Regulatory obligations
- Estimated likelihood
- Existing mitigations

Attach or paste the relevant input materials listed above, including the Enterprise Risk Register, known vulnerabilities, existing controls, business-critical systems, regulatory obligations, and any documented mitigations. Redact sensitive details first: describe vulnerabilities by category rather than by system name, IP address, or exploit detail.

Safe AI Use — read before you paste

- **Use an approved account.** Only paste business information into an AI tool your organization has actually vetted — not a personal or free-tier account with unclear data-handling terms.
- **Redact before you paste.** Strip out personally identifiable information, protected health information, and anything a client would expect to stay confidential before it ever reaches the AI tool.
- **Never paste secrets.** Passwords, API keys, access tokens, and login credentials should never appear in a prompt, regardless of which tool you're using.
- **Verify every output.** Treat AI-generated content as a draft, not a final answer — review it against your own knowledge of the business before you rely on it.
- **Require human approval before action.** If your AI tool can take actions — sending messages, modifying systems, writing to a database — a person must approve before it executes.

The Prompt

Copy everything inside the box into your approved AI tool, then attach or paste your inputs.

You are an experienced Governance, Risk, and Compliance (GRC) consultant specializing in small and medium-sized businesses (SMBs). Your objective is to analyze the organization's Enterprise Risk Register and produce a practical, business-focused risk prioritization that supports executive decision-making (use attachments).

For each identified risk:

- Assess the potential impact on:
  - Revenue and cash flow
  - Business operations
  - Customer trust and reputation
  - Regulatory or contractual compliance
  - Confidentiality, integrity, and availability of information
- Estimate:
  - Likelihood (Low, Medium, High)
  - Business Impact (Low, Medium, High)
  - Overall Risk Rating (Low, Medium, High, Critical)
- Recommend an appropriate response:
  - Mitigate
  - Transfer
  - Accept
  - Avoid
- Recommend:
  - Primary risk owner
  - Suggested mitigation activities
  - Recommended implementation timeframe:
    - Immediate (0–30 days)

    - Near Term (30–90 days)
    - Long Term (90+ days)
- Identify:
    - Quick wins that require minimal effort but significantly reduce risk
    - High-cost initiatives that should be planned strategically
    - Risks that may be accepted based on organizational tolerance
- Highlight:
    - Risks affecting multiple business functions
    - Risks dependent on third-party vendors
    - Single points of failure
    - Regulatory or legal concerns

Produce your results in a table with the following columns:

- Risk
- Business Impact
- Likelihood
- Overall Risk Rating
- Recommended Response
- Priority
- Suggested Owner
- Recommended Timeline
- Recommended Actions
- Executive Notes

Do not assume every risk requires immediate remediation. Balance risk reduction with cost, operational impact, and available resources. Recommend practical, right-sized solutions rather than enterprise-scale controls. If the Enterprise Risk Register already includes 1 to 5 likelihood and impact scores, use them, treating 1–2 as Low, 3 as Medium, and 4–5 as High.

Practical Guidance

Like every Generative AI tool included in this methodology, this prompt is intended to assist, not replace, executive judgment. Leadership remains responsible for determining the organization's risk tolerance, approving mitigation strategies, and accepting any residual risk. Think of this prompt as an experienced GRC advisor that rapidly organizes complex information, allowing your leadership team to spend less time analyzing spreadsheets and more time making informed business decisions.