Pragmatic GRC™
R-001 Enterprise Risk Register Guide

Risk Management Resource | Version 1.1 | Practical Implementation Guide

Document Information

Resource ID	R-001
Resource Family	Risk Management
Version	1.1
Status	Approved
Related Chapters	1, 2, 4, 6, 7, 8
Related Resources	F-001, F-002, G-002, R-003, R-005

Purpose

The Enterprise Risk Register is the authoritative record of the organization's identified risks. It is one of the Three Living Documents. It enables leadership to evaluate, prioritize, assign ownership, and monitor risks using a consistent method.

> 💡 **Tip:** Describe risks in business language that leadership understands.

Why This Resource Matters

Organizations face strategic, operational, financial, cybersecurity, legal, and compliance risks every day. A central register keeps risks visible, discussed, and managed instead of discovered during a crisis.

When to Use This Resource

Use the register during initial GRC implementation, project planning, vendor reviews, technology changes, security assessments, audit preparation, and the Monthly GRC Heartbeat™. Give it a full review once a year in Q2 of the annual Living Document cycle.

Risk Categories

Recommended categories include Strategic, Operational, Cybersecurity, Compliance, Financial, Third-Party, Human, Physical, and Reputational risks.

Recommended Risk Register Fields

Risk ID, Risk Description, Category, Risk Owner, Likelihood (1–5), Impact (1–5), Inherent Score and Rating, Existing Controls, Residual Likelihood, Residual Impact, Residual Score and Rating, Treatment Strategy, Status, Target or Closed Date, Last Review Date, related Asset ID (F-001), SSP Section (F-002), Assessment ID (R-003), Treatment Plan (R-005), and Notes.

Scoring Scale (Likelihood 1–5 × Impact 1–5)

Score likelihood and impact from 1 to 5 and multiply them. The score runs from 1 to 25. Score each risk twice: inherent (before controls) and residual (after the controls that are actually in place).

Rating	Likelihood	Impact
1	Rare: not expected to occur; less than once every five years	Minimal: negligible disruption; no meaningful financial, operational, or reputational effect
2	Unlikely: could occur, but not expected within the next three years	Minor: limited disruption; minimal financial, operational, or reputational effect
3	Possible: could occur, or has occurred within the last one to three years	Moderate: noticeable disruption requiring management attention and recovery effort
4	Likely: expected to occur, or has occurred within the last year	Major: significant disruption, major loss, or regulatory exposure
5	Almost certain: expected more than once a year, or happening now	Severe: business-threatening disruption, reportable breach, or lasting reputational harm

Score	Rating	Expected Response
1–4	Low	Accept or monitor; review at the annual risk register review.
5–9	Medium	Assign an owner and a treatment; review at least quarterly.
10–14	High	Treat with a target date; review at every Monthly GRC Heartbeat™.
15–25	Critical	Escalate to the Executive Sponsor; build a Risk Treatment Plan (R-005).

⚠️ **Escalation Threshold:** Any risk scoring 15 or higher is Critical and is escalated to executive leadership (book Chapter 8, Section 8.4; Template 2A).

Risk Scoring Examples

Likelihood	Impact	Score	Rating
4 Likely	5 Severe	20	Critical: escalate; treatment plan required
3 Possible	4 Major	12	High: treat with a target date
2 Unlikely	3 Moderate	6	Medium: assign an owner and treatment
1 Rare	2 Minor	2	Low: accept or monitor

Risk Treatment Options

Accept, Mitigate, Transfer, Avoid, or Monitor each risk based on business objectives and risk tolerance.

✔ **Best Practice:** Every identified risk should have a documented treatment decision.

Best Practices

Assign one accountable owner to every risk, review High and Critical risks at every Monthly GRC Heartbeat™, link risks to the Master Asset Register (F-001), and document treatment decisions.

Common Mistakes

Keeping a list of problems instead of risks, failing to assign ownership, never updating risk status, and documenting risks without planned treatments.

⚠️ **Warning:** Do not confuse vulnerabilities, issues, or incidents with risks.

Risk Management Lifecycle

1. Identify the risk
2. Assess it in R-003 (likelihood × impact)
3. Prioritize by score
4. Treat it (R-005 for Critical risks)
5. Monitor it
6. Review it at the Monthly GRC Heartbeat™
7. Improve continually

Related Resources

F-001 Master Asset Register • F-002 Unified System Security Plan • R-003 Risk Assessment Worksheet • R-005 Risk Treatment Plan • G-002 Monthly GRC Heartbeat™ Checklist

Revision History

Version	Date	Author	Description
1.0	August 2026	Pragmatic GRC™	Initial publication
1.1	November 2026	Pragmatic GRC™	Aligned to the book's 1–5 likelihood and impact scale, the 1–25 score bands, and the escalation threshold of 15