Pragmatic GRC™
R-003 Risk Assessment Worksheet Guide

Risk Management Resource | Version 1.1 | Practical Implementation Guide

Document Information

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

Purpose

The Risk Assessment Worksheet gives you a structured way to identify, evaluate, and document risks before they are added to the Enterprise Risk Register (R-001). It keeps the analysis consistent and supports informed business decisions.

> 💡 **Tip:** Complete this worksheet before creating or updating an entry in the Enterprise Risk Register.

When to Use This Worksheet

Use this worksheet for new projects, technology purchases, vendor evaluations, process changes, annual reviews, security assessments, and whenever significant business changes occur.

Risk Assessment Process

1. Identify the asset or business process.
2. Identify potential threats and vulnerabilities.
3. Score likelihood and impact from 1 to 5.
4. Review existing controls.
5. Calculate inherent and residual scores (likelihood × impact).
6. Recommend a treatment strategy.
7. Escalate any score of 15 or more, then submit approved risks to the Enterprise Risk Register (R-001).

Recommended Worksheet Fields

Assessment ID, Date, Assessor, Asset or Process, Threat, Vulnerability, Existing Controls, Likelihood (1–5), Impact (1–5), Inherent Score and Rating, Recommended Treatment, Residual Likelihood and Impact, Residual Score and Rating, Risk Owner, Target Completion Date, 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 Treatment Strategies

Accept, Mitigate, Transfer, Avoid, or Monitor. Select the strategy that best fits the organization's objectives and risk appetite.

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

Best Practices

Use business language, involve the right business owner, record the evidence behind each score, and reference related assets and security documentation.

Common Mistakes

Scoring risks without evidence, confusing incidents with risks, failing to identify ownership, and leaving out planned treatment activities.

> ⚠️ **Warning:** Do not assign likelihood or impact values without a supporting rationale.

Example Assessment Workflow

1. Identify the asset or process
2. Identify threats and vulnerabilities
3. Score likelihood and impact (1–5 each)
4. Calculate the risk score (1–25)
5. Select a treatment strategy
6. Update the R-001 Enterprise Risk Register

Related Resources

F-001 Master Asset Register • F-002 Unified System Security Plan • R-001 Enterprise Risk Register • 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™	Replaced the 1–3 scale with the book's 1–5 likelihood and impact scale, 1–25 score bands, and the escalation threshold of 15