

Enterprise risk and maturity self-assessment tool



WIPFLI

Use this worksheet to complete a risk and maturity self-assessment

This enterprise risk and maturity self-assessment tool offers a practical starting point for identifying priority risks and evaluating how prepared your organization is to manage them. Use it to get a clearer understanding of your current levels.*

How to complete this assessment

Complete the worksheet with a small cross-functional group rather than relying on one person’s perspective. Base ratings on observable evidence rather than intent. When evidence is mixed or a practice exists only in isolated areas, choose the lower rating.

- Identify and rate a small set of enterprise risks.
- Evaluate seven capabilities needed to manage risk consistently.
- Connect high-rated risks with the weakest relevant capabilities.
- Choose a first action, owner and target date for each priority.

Keep risk and maturity separate

A risk rating estimates the significance of a specific risk. A maturity rating evaluates the organization’s capability to identify, manage,

monitor and respond to risk. A high risk does not automatically mean low maturity — and a mature ERM program does not eliminate risk.

Question	What it measures	Output
How significant is this risk?	Likelihood and potential impact	Low, moderate or high risk
How capable are we of managing risk?	Governance, process, ownership, controls, information and adaptation	A 1–5 maturity profile by capability
What should we address first?	Risk significance considered alongside relevant capability gaps	Prioritized action

**This is a directional self-assessment, not a formal risk maturity model assessment, certification or substitute for a facilitated enterprise risk assessment. Use it to surface priorities and guide deeper discussion.*

Step 1 Identify and rate priority risks

Start with the objectives, operations or growth plans that matter most. Write each risk as a cause–event–impact statement:
Because [cause], [event] may occur, leading to [impact on the organization or objective].

Risk statement	Objective affected	Owner	Existing controls	L	I	Rating

Likelihood and impact criteria

Score	Likelihood	Impact
1	Unlikely: Not expected under normal conditions; limited history or warning signs.	Limited: Manageable within normal operations with minor effect on objectives.
2	Possible: Could occur; some history, indicators or plausible conditions exist.	Significant: Meaningful operational, financial, compliance or strategic disruption requiring management attention.
3	Likely: Expected, recurring or supported by strong indicators.	Severe: Threatens critical operations, financial stability, regulatory standing, reputation or a major strategic objective.

Risk-rating matrix

Likelihood ↓ / Impact →	1 — Limited	2 — Significant	3 — Severe
1 — Unlikely	Low	Low	Moderate
2 — Possible	Low	Moderate	High
3 — Likely	Moderate	High	High

Optional refinement: Rate the risk once before considering controls (inherent risk), then again after considering the design and effectiveness of existing controls (residual risk).

Step 2

Evaluate risk-management maturity

Score each indicator from 1 to 5. Consider three questions:

- 1. How consistently does the practice work?
- 2. Is it proactive or mostly reactive?
- 3. How broadly is it applied across functions and levels?

Record the evidence supporting each rating.

Score	Stage	What the stage looks like
1	Reactive	No consistent practice. Risk is generally addressed after a problem occurs and depends on individual effort.
2	Developing	Basic practices exist in some areas, but ownership, execution and documentation are inconsistent or siloed.
3	Defined	Core practices are documented, repeatable and used in important areas, although coverage or follow-through may vary.
4	Integrated	Practices are consistently applied across the organization and embedded in operations and decision-making.
5	Adaptive	Practices are measured, forward-looking and continually improved as objectives, conditions and risks change.

Scoring rule: For each capability, use the lower of its two indicator ratings as the capability score. Do not average all seven capabilities into one number; a single score can conceal a critical weakness.

Scoring sheet

Capability	Indicator	1–5	Evidence or gap
1. Leadership and governance	Leaders demonstrate active understanding of enterprise risk and reinforce its importance.		
	Roles, decision rights, oversight forums and escalation paths are clear.		
2. Risk identification and assessment	A consistent process captures enterprise, emerging and interconnected risks.		
	Likelihood, impact and control effectiveness are evaluated using defined criteria and evidence.		
3. Ownership, appetite and escalation	Named risk owners are accountable for monitoring risks and completing agreed actions.		
	Risk appetite, tolerance and escalation thresholds guide decisions and responses.		
4. Controls and response	Key controls are documented and periodically evaluated for both design and operating effectiveness.		
	Mitigation plans are prioritized, resourced, assigned and tracked through completion.		
5. Information, metrics and reporting	Metrics provide timely, meaningful and increasingly forward-looking insight into risk and control performance.		
	Reporting is tailored to management and board needs and explains significance, trends, residual risk and required decisions.		
6. Integration and decision use	Risk information informs strategy, budgeting, operations, projects, technology and third-party decisions.		
	ERM outputs inform audit, compliance, continuity planning and other assurance activities.		
7. Monitoring and resilience	Risks, controls and action plans are reassessed on a defined cadence and when material changes occur.		
	Scenario planning, disruption response and lessons learned strengthen readiness and continuous improvement.		

Your maturity profile

Capability	Score	Strongest evidence	Most important gap
Leadership and governance			
Risk identification and assessment			
Ownership, appetite and escalation			
Controls and response			
Information, metrics and reporting			
Integration and decision use			
Monitoring and resilience			

Interpretation: Scores of 1–2 signal foundational gaps. A score of 3 indicates a defined practice that may need broader or more consistent execution. Scores of 4–5 indicate stronger capability, but they should still be tested against evidence and changing conditions.

Step 3 Turn the results into priorities

Review each high- or moderate-rated risk and identify the capabilities most relevant to managing it. The goal is not to fix every gap at once. Focus first on high-risk, low-maturity areas.

Priority	Use when	Typical response
Act now	High risk + one or more relevant capability scores of 1–2.	Establish ownership, stabilize critical controls and define immediate mitigation.
Build the roadmap	High risk + relevant capability score of 3, or moderate risk + score of 1–2.	Set a target state, sequence improvements and assign resources and milestones.
Monitor	Low risk or moderate risk supported by relevant capability scores of 4–5 and within tolerance.	Track indicators, test controls and reassess when conditions change.



Get help mitigating your enterprise risk

Ask Wipfli's risk advisory team to do an enterprise risk assessment and help you mitigate financial, operational and reputational risk.

Let's manage your risk

ADVISORY & ACCOUNTING

WIPFLI

"Wipfli" is the brand name under which Wipfli LLP and Wipfli Advisory LLC and its respective subsidiary entities provide professional services. Wipfli LLP and Wipfli Advisory LLC (and its respective subsidiary entities) practice in an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable law, regulations, and professional standards. Wipfli LLP is a licensed independent CPA firm that provides attest services to its clients, and Wipfli Advisory LLC provides tax and business consulting services to its clients. Wipfli Advisory LLC and its subsidiary entities are not licensed CPA firms.