

## SME Risk Maturity Self-Assessment

---

### About This Assessment

Effective risk management is not about bureaucracy — it is about enabling confident decision-making, protecting value and supporting sustainable growth.

This self-assessment tool is designed to help small and medium enterprises evaluate the maturity of their risk management approach, aligned to the internationally recognised ISO 31000 standard.

It translates the core principles, framework elements and processes of ISO 31000 into clear, practical guidance suitable for organisations where risk management is performed alongside broader operational responsibilities.

Whether you are a team leader, operations manager, finance manager or part-time risk owner, this assessment will help you:

- Understand what “good” risk management looks like in practice
  - Identify strengths and capability gaps
  - Prioritise improvement areas
  - Benchmark your organisation’s maturity
- 

### What This Assessment Covers

The diagnostic is structured across three core components of ISO 31000:

1. **Risk Management Principles** The foundations that underpin effective risk thinking and culture.
2. **Risk Management Framework** The governance structure that supports consistent risk oversight.
3. **Risk Management Process** The day-to-day activities used to identify, assess, treat and monitor risk.

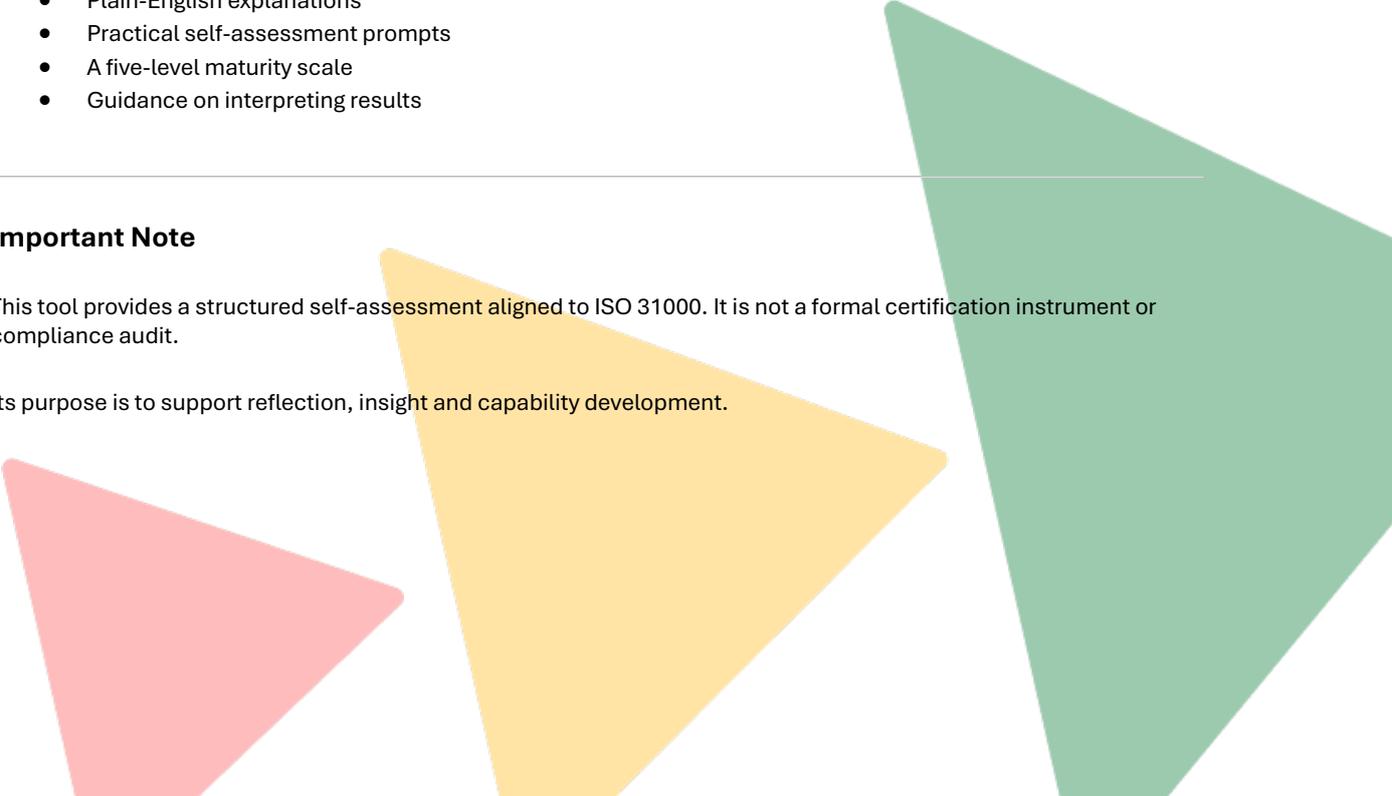
Each section includes:

- Plain-English explanations
  - Practical self-assessment prompts
  - A five-level maturity scale
  - Guidance on interpreting results
- 

### Important Note

This tool provides a structured self-assessment aligned to ISO 31000. It is not a formal certification instrument or compliance audit.

Its purpose is to support reflection, insight and capability development.

Three large, overlapping triangles in the bottom right corner: a pink one at the bottom left, a yellow one in the middle, and a green one at the top right.

# SECTION 1: RISK MANAGEMENT PRINCIPLES

---

## 1. Introduction – Why the Principles Matter

ISO 31000 sets out eight principles that underpin effective risk management. These principles are not about paperwork or compliance. They describe what “good” risk thinking looks like inside an organisation.

For SMEs — particularly those where risk is managed part-time alongside other responsibilities — the principles are especially important. They help ensure risk management is practical, proportionate and genuinely useful, rather than bureaucratic.

This section helps you assess how well these principles are reflected in how your organisation operates.

### How to Use This Section

- Allow around 20–30 minutes to complete.
- For each principle:
  - Read the plain-English explanation.
  - Reflect on the diagnostic prompts.
  - Select the maturity level that best reflects your current reality (not your intention).
- Don't overthink it. Go with what is consistently true in practice.

### Maturity Levels Explained

Level	Description
<b>1 – Reactive</b>	Risk is managed informally and only when issues arise.
<b>2 – Aware</b>	There is growing recognition of risk, but practices are inconsistent.
<b>3 – Structured</b>	Risk management is defined and applied in a consistent way.
<b>4 – Integrated</b>	Risk thinking is embedded into decision-making and leadership.
<b>5 – Leading</b>	Risk management is continuously improved and seen as a strategic advantage.

For many SMEs, **Level 3 (Structured)** represents a strong and appropriate level of maturity.

---

# The 8 Principles

## Principle 1: Integrated

### What This Means in Practice

Risk management is not a separate activity. It is part of how decisions are made, projects are run, and objectives are set.

### Self-Assessment Prompts

- Is risk considered when setting strategy or business plans?
- Are risks discussed during major decision-making?
- Are project risks identified before significant work begins?
- Is risk part of leadership or management meeting discussions?
- Is risk linked to performance or accountability?

### Maturity Guide

Level	Description	Result
1 – Reactive	Risk is only discussed after something goes wrong.	
2 – Aware	Risk is sometimes considered, but not systematically.	
3 – Structured	Risk is formally included in planning and key decisions.	
4 – Integrated	Risk is consistently embedded in management processes.	
5 – Leading	Risk thinking actively shapes strategic direction and opportunity selection.	

## Principle 2: Structured and Comprehensive

### What This Means in Practice

There is a clear and consistent approach to identifying, assessing and managing risks.

### Self-Assessment Prompts

- Do you have a documented risk register?
- Is there a defined method for assessing risk (e.g. likelihood and impact)?
- Are risk categories clearly defined?
- Is there consistency across teams in how risks are recorded?
- Are risks reviewed on a regular schedule?

### Maturity Guide

Level	Description	Result
1 – Reactive	No formal structure exists.	
2 – Aware	Some documentation exists but is inconsistent.	
3 – Structured	A defined process is used across the organisation.	
4 – Integrated	Risk processes are consistently applied and monitored.	
5 – Leading	Risk processes are refined using insights and data.	

## Principle 3: Customised

### What This Means in Practice

Risk management reflects your organisation's size, complexity, industry and objectives. It is not copied from a template without adaptation.

### Self-Assessment Prompts

- Is your risk framework proportionate to your organisation's size?
- Are risk categories tailored to your industry?
- Have you avoided unnecessary complexity?
- Do staff understand the process?
- Is the approach practical and usable?

### Maturity Guide

Level	Description	Result
1 – Reactive	No formal approach exists.	
2 – Aware	Generic templates are used with minimal tailoring.	
3 – Structured	The approach reflects your organisational context.	
4 – Integrated	Risk processes evolve as the organisation grows.	
5 – Leading	Risk management is strategically designed to support competitive advantage.	

## Principle 4: Inclusive

### What This Means in Practice

Relevant stakeholders are involved in identifying and managing risks.

### Self-Assessment Prompts

- Are managers involved in identifying operational risks?
- Are subject matter experts consulted?
- Are frontline insights considered?
- Is the Board or governing body informed about key risks?
- Is risk ownership clearly assigned?

### Maturity Guide

Level	Description	Result
1 – Reactive	Risk decisions are made in isolation.	
2 – Aware	Some consultation occurs but not systematically.	
3 – Structured	Stakeholders are regularly engaged.	
4 – Integrated	Risk ownership and consultation are clear and consistent.	
5 – Leading	Risk culture encourages open dialogue and challenge.	

## Principle 5: Dynamic

### What This Means in Practice

Risk management responds to change — new regulations, growth, technology, market shifts.

### Self-Assessment Prompts

- Are emerging risks discussed regularly?
- Are risks updated when major changes occur?
- Is there a process for identifying new risks?
- Are external developments monitored?
- Do you revisit assumptions periodically?

### Maturity Guide

Level	Description	Result
1 – Reactive	Risks are rarely updated.	
2 – Aware	Risks are updated only when prompted.	
3 – Structured	Risks are reviewed periodically.	
4 – Integrated	Risk reviews are triggered by internal and external change.	
5 – Leading	The organisation anticipates emerging risks proactively.	

## Principle 6: Best Available Information

### What This Means in Practice

Risk decisions are based on relevant data, experience and informed judgement.

### Self-Assessment Prompts

- Are risk assessments supported by data where available?
- Do you consider both internal and external information?
- Are assumptions documented?
- Are limitations in information acknowledged?
- Do you use lessons learned from past events?

### Maturity Guide

Level	Description	Result
1 – Reactive	Decisions are largely intuitive.	
2 – Aware	Some information informs decisions.	
3 – Structured	Risk assessments use available and relevant information.	
4 – Integrated	Data and insights consistently inform risk evaluation.	
5 – Leading	Risk insights are supported by robust data analysis.	

## Principle 7: Human and Cultural Factors

### What This Means in Practice

Risk management recognises that behaviour, incentives and culture influence outcomes.

### Self-Assessment Prompts

- Are people encouraged to raise concerns?
- Are risk responsibilities clearly understood?
- Do incentives align with responsible behaviour?
- Is risk awareness part of onboarding or training?
- Is accountability clear?

### Maturity Guide

Level	Description	Result
1 – Reactive	Risk awareness is low and informal.	
2 – Aware	Some individuals champion risk thinking.	
3 – Structured	Roles and responsibilities are defined.	
4 – Integrated	Risk awareness is part of organisational culture.	
5 – Leading	Risk culture is actively measured and strengthened.	

## Principle 8: Continual Improvement

### What This Means in Practice

Risk management practices are reviewed and refined over time.

### Self-Assessment Prompts

- Are risk processes reviewed annually?
- Are lessons from incidents captured?
- Are audits or reviews used to improve the system?
- Are improvement actions tracked?
- Is feedback sought from users?

### Maturity Guide

Level	Description	Result
1 – Reactive	No review or improvement cycle exists.	
2 – Aware	Improvements occur after major issues.	
3 – Structured	Risk processes are reviewed periodically.	
4 – Integrated	Continuous improvement is built into governance cycles.	
5 – Leading	Risk maturity is regularly benchmarked and enhanced.	

## Principles Self-Assessment Summary

Principle	Your Score (1-5)	Comments
Integrated		
Structured & Comprehensive		
Customised		
Inclusive		
Dynamic		
Best Available Information		
Human & Cultural Factors		
Continual Improvement		

## Interpreting Your Results – Principles

### Average 1-2 (Reactive / Early Awareness)

Risk practices are inconsistent and informal.

Priority focus:

- Establish a basic risk register.
- Define risk ownership.
- Introduce quarterly risk discussions.

### Average ~3 (Structured)

Risk management is defined and functioning.

Priority focus:

- Improve integration into decision-making.
- Strengthen risk review triggers.
- Enhance stakeholder engagement.

### Average 4-5 (Integrated / Leading)

Risk thinking is embedded and proactive.

Priority focus:

- Benchmark maturity.
- Leverage risk insights strategically.
- Focus on continuous refinement and data quality.

## SECTION 2: RISK MANAGEMENT FRAMEWORK

### 1. Introduction – Why the Framework Matters

The risk management framework defines how risk is embedded into your organisation's governance, structure and operations.

While the principles describe what good risk management looks like, the framework describes how it is organised and sustained.

For SMEs, this is often where gaps appear. Many organisations identify risks informally, but lack:

- Clear accountability
- Defined governance cycles
- Regular review processes
- Alignment between risk and strategy

This section helps you assess whether risk management in your organisation is:

- Clearly structured
- Appropriately governed
- Actively maintained

Allow around 20–30 minutes to complete this section.

As before, score your organisation based on what is consistently happening in practice.

---

### Framework Maturity Levels

Level	Description
<b>1 – Reactive</b>	Risk management is informal and unstructured.
<b>2 – Aware</b>	Some structure exists but is inconsistent.
<b>3 – Structured</b>	Roles, processes and governance are clearly defined.
<b>4 – Integrated</b>	Risk management is embedded into organisational governance and planning.
<b>5 – Leading</b>	The framework is actively monitored, refined and aligned to strategy.

For most SMEs, **Level 3 (Structured)** represents a strong foundation.

---

# The 6 Framework Elements

## Element 1: Leadership and Commitment

### What This Means in Practice

Senior leaders visibly support and reinforce risk management. It is not delegated and forgotten.

### Self-Assessment Prompts

- Do leaders actively discuss risk in meetings?
- Is there a defined risk appetite or tolerance statement?
- Is risk included in strategic planning discussions?
- Do leaders model responsible decision-making?
- Is risk ownership clearly assigned at leadership level?

### Maturity Guide

Level	Description	Result
1 – Reactive	Leadership involvement is minimal or passive.	
2 – Aware	Leaders acknowledge risk but rarely engage formally.	
3 – Structured	Leadership roles in risk governance are defined and active.	
4 – Integrated	Risk oversight is embedded into executive and board governance.	
5 – Leading	Leadership uses risk insights to guide strategy and opportunity.	

## Element 2: Integration into Organisational Processes

### What This Means in Practice

Risk management is incorporated into key business activities — planning, budgeting, projects and performance management.

### Self-Assessment Prompts

- Is risk considered during annual planning and budgeting?
- Are risks assessed before major investments or initiatives?
- Are project risks documented and reviewed?
- Is risk included in performance or reporting cycles?
- Is risk considered during change initiatives?

### Maturity Guide

Level	Description	Result
1 – Reactive	Risk is rarely linked to operational processes.	
2 – Aware	Risk is occasionally included in projects or plans.	
3 – Structured	Risk assessment is formally embedded in key processes.	
4 – Integrated	Risk thinking is standard practice in decision workflows.	
5 – Leading	Risk analysis actively shapes organisational priorities.	

## Element 3: Design of the Framework

### What This Means in Practice

Your organisation has intentionally designed its risk framework to suit its size, complexity and regulatory environment.

### Self-Assessment Prompts

- Is your risk framework documented?
- Are roles and responsibilities clearly defined?
- Is the framework proportionate to your organisation?
- Is there clarity about how risks are escalated?
- Are reporting lines and governance structures clear?

### Maturity Guide

Level	Description	Result
1 – Reactive	No documented framework exists.	
2 – Aware	Some documentation exists but lacks clarity.	
3 – Structured	A documented framework defines governance and roles.	
4 – Integrated	The framework is well understood and consistently applied.	
5 – Leading	The framework evolves in line with organisational growth and complexity.	

## Element 4: Implementation

### What This Means in Practice

The risk framework is not just documented — it is actively applied across the organisation.

### Self-Assessment Prompts

- Is there an active and maintained risk register?
- Are risk reviews conducted on a defined schedule?
- Are risk owners aware of their responsibilities?
- Are treatment plans documented and monitored?
- Is risk reporting provided to leadership or the board?

### Maturity Guide

Level	Description	Result
1 – Reactive	Risk processes are rarely followed.	
2 – Aware	Some implementation occurs but inconsistently.	
3 – Structured	Risk processes are applied consistently.	
4 – Integrated	Risk management is routinely embedded in management practice.	
5 – Leading	Risk implementation is monitored, measured and optimised.	

## Element 5: Evaluation

### What This Means in Practice

The organisation evaluates whether its risk framework is effective and fit-for-purpose.

### Self-Assessment Prompts

- Is the risk framework reviewed annually?
- Are internal audits or reviews conducted?
- Are performance indicators used to measure effectiveness?
- Are lessons from incidents incorporated into improvements?
- Is feedback sought from stakeholders?

### Maturity Guide

Level	Description	Result
1 – Reactive	No formal evaluation occurs.	
2 – Aware	Reviews occur occasionally or after incidents.	
3 – Structured	The framework is periodically evaluated.	
4 – Integrated	Evaluation is part of governance cycles.	
5 – Leading	The framework is benchmarked and continuously improved.	

## Element 6: Improvement

### What This Means in Practice

The organisation takes deliberate action to improve risk capability over time.

### Self-Assessment Prompts

- Are improvement actions tracked and monitored?
- Are framework gaps identified and prioritised?
- Is risk capability training provided?
- Are systems or tools reviewed for effectiveness?
- Does leadership support capability uplift?

### Maturity Guide

Level	Description	Result
1 – Reactive	Improvements occur only after major issues.	
2 – Aware	Some improvement efforts occur but are unstructured.	
3 – Structured	Improvement actions are identified and followed through.	
4 – Integrated	Risk capability uplift is part of strategic planning.	
5 – Leading	Continuous improvement is embedded and data-driven.	

## Framework Self-Assessment Summary

Framework Element	Your Score (1-5)	Comments
Leadership & Commitment		
Integration into Processes		
Design of Framework		
Implementation		
Evaluation		
Improvement		

## Interpreting Your Results – Framework

### Average 1-2 (Reactive / Early Awareness)

Risk governance lacks structure.

Priority actions:

- Define leadership accountability.
- Document a minimum viable risk framework.
- Establish a quarterly risk review cycle.
- Assign clear risk ownership.

### Average ~3 (Structured)

A functioning framework exists but may not be fully embedded.

Priority actions:

- Improve integration into decision-making workflows.
- Strengthen risk reporting to leadership.
- Formalise evaluation mechanisms.
- Track improvement actions systematically.

### Average 4-5 (Integrated / Leading)

Risk governance is embedded and effective.

Priority actions:

- Benchmark against peers.
- Refine data quality and reporting.
- Align risk insights more closely with strategic planning.
- Invest in capability uplift and optimisation.

# SECTION 3: RISK MANAGEMENT PROCESS

---

## 1. Introduction – Why the Process Matters

The risk management process describes how risks are:

- Identified
- Analysed
- Evaluated
- Treated
- Monitored and reviewed
- Communicated

For SMEs, the process needs to be simple, repeatable and proportionate.

Over-engineering creates fatigue.

Under-structuring creates blind spots.

This section helps you assess whether your organisation has a clear and usable process — one that supports informed decision-making without creating unnecessary burden.

Allow approximately 20–30 minutes to complete this section.

As with previous sections, select the maturity level that reflects what consistently happens in practice.

---

### Process Maturity Levels

Level	Description
<b>1 – Reactive</b>	Risk activities occur informally or after issues arise.
<b>2 – Aware</b>	Basic process steps exist but are inconsistent.
<b>3 – Structured</b>	A defined and repeatable risk process is in place.
<b>4 – Integrated</b>	The process is embedded in projects and operations.
<b>5 – Leading</b>	The process is refined, data-informed and proactive.

For most SMEs, **Level 3 (Structured)** is strong and appropriate.

---

# The 6 Process Elements

## Element 1: Communication and Consultation

### What This Means in Practice

Risk information is shared appropriately, and relevant stakeholders are involved in discussions.

### Self-Assessment Prompts

- Are risks communicated to leadership or the board?
- Are risk owners consulted when risks are identified or assessed?
- Are key stakeholders informed of significant risks?
- Is there a clear channel for escalating emerging risks?
- Are risk discussions documented?

### Maturity Guide

Level	Description	Result
1 – Reactive	Risk communication is informal and inconsistent.	
2 – Aware	Risk is sometimes shared but not systematically.	
3 – Structured	Risk communication is defined and occurs regularly.	
4 – Integrated	Risk consultation is embedded in governance and operations.	
5 – Leading	Risk dialogue is proactive, transparent and culturally embedded.	

## Element 2: Establishing the Context

### What This Means in Practice

Before assessing risks, your organisation clearly defines objectives, scope, stakeholders and external influences.

### Self-Assessment Prompts

- Are objectives clearly defined before risk assessment begins?
- Are internal and external factors considered?
- Is scope documented for projects or initiatives?
- Are stakeholder expectations understood?
- Is risk appetite or tolerance considered?

### Maturity Guide

Level	Description	Result
1 – Reactive	Risks are assessed without clearly defining context.	
2 – Aware	Context is considered informally.	
3 – Structured	Context-setting is part of formal risk assessment.	
4 – Integrated	Context analysis informs strategic and operational planning.	
5 – Leading	Context is regularly reviewed and aligned with strategy.	

## Element 3: Risk Identification

### What This Means in Practice

Your organisation systematically identifies risks that could impact objectives.

### Self-Assessment Prompts

- Is there a structured approach to identifying risks?
- Are workshops or discussions used to identify risks?
- Are operational, financial, strategic and compliance risks considered?
- Are emerging and external risks identified?
- Are identified risks recorded in a central register?

### Maturity Guide

Level	Description	Result
1 – Reactive	Risks are identified only after incidents occur.	
2 – Aware	Some risks are documented but inconsistently.	
3 – Structured	Risk identification is systematic and documented.	
4 – Integrated	Risk identification occurs across teams and projects.	
5 – Leading	Risk identification includes forward-looking and scenario analysis.	

## Element 4: Risk Analysis and Evaluation

### What This Means in Practice

Risks are assessed consistently to determine their likelihood, impact and priority.

### Self-Assessment Prompts

- Is there a defined method for scoring likelihood and impact?
- Are risk ratings documented and explained?
- Are inherent and residual risks considered?
- Are risk criteria or thresholds defined?
- Are high risks escalated appropriately?

### Maturity Guide

Level	Description	Result
1 – Reactive	Risk severity is judged informally.	
2 – Aware	Basic scoring occurs but lacks consistency.	
3 – Structured	A defined methodology is used consistently.	
4 – Integrated	Risk analysis informs decision-making and prioritisation.	
5 – Leading	Risk analysis is data-informed and regularly refined.	

## Element 5: Risk Treatment

### What This Means in Practice

Actions are defined to manage, reduce, transfer or accept risks.

### Self-Assessment Prompts

- Are treatment plans documented?
- Are responsibilities for treatments assigned?
- Are timeframes defined?
- Are treatments tracked to completion?
- Are control effectiveness reviews conducted?

### Maturity Guide

Level	Description	Result
1 – Reactive	Risk treatments are informal or undocumented.	
2 – Aware	Some actions are defined but not tracked.	
3 – Structured	Treatment plans are documented and monitored.	
4 – Integrated	Treatments are embedded into operational workflows.	
5 – Leading	Treatment effectiveness is measured and optimised.	

## Element 6: Monitoring and Review

### What This Means in Practice

Risks and controls are regularly reviewed to ensure they remain current and effective.

### Self-Assessment Prompts

- Is the risk register reviewed on a defined schedule?
- Are changes in risk levels monitored?
- Are risk dashboards or reports used?
- Are risk incidents analysed for lessons learned?
- Are risk owners held accountable for updates?

### Maturity Guide

Level	Description	Result
1 – Reactive	Risks are rarely reviewed.	
2 – Aware	Reviews occur occasionally or after incidents.	
3 – Structured	Risk reviews occur on a defined schedule.	
4 – Integrated	Monitoring is embedded into governance cycles.	
5 – Leading	Monitoring uses data and trend analysis to anticipate change.	

## Process Self-Assessment Summary

Process Element	Your Score (1–5)	Comments
Communication & Consultation		
Establishing the Context		
Risk Identification		
Risk Analysis & Evaluation		
Risk Treatment		
Monitoring & Review		

## Interpreting Your Results – Process

### Average 1–2 (Reactive / Early Awareness)

Risk activities are informal and inconsistent.

Priority actions:

- Establish a central risk register.
- Define a simple risk scoring method.
- Assign risk ownership.
- Introduce quarterly risk review meetings.

### Average ~3 (Structured)

A functioning process exists but may lack consistency or integration.

Priority actions:

- Improve documentation and tracking.
- Embed risk assessments into projects.
- Strengthen monitoring and reporting cycles.
- Formalise escalation pathways.

### Average 4–5 (Integrated / Leading)

Risk processes are embedded and proactive.

Priority actions:

- Enhance data quality and reporting.
- Improve control testing and effectiveness review.
- Introduce trend analysis and forward-looking risk assessment.
- Benchmark maturity against peers.

## Next Steps: Turning Insight into Action

Completing this assessment is a strong first step. The real value now comes from translating your results into a practical maturity uplift plan.

For most SMEs, improvement does not require complexity — it requires clarity, prioritisation and consistency.

---

### Step 1: Identify Your Priority Gaps

Review your results across:

- Principles
- Framework
- Process

Look for:

- Areas scoring 1–2 (foundational gaps)
- Large inconsistencies between sections (e.g. strong governance but weak monitoring)
- Repeated themes in your comments

Focus on no more than **3–5 priority areas** for the next 6–12 months.

Trying to improve everything at once creates fatigue and stalls progress.

---

### Step 2: Define Practical Uplift Actions

For each priority area, define:

- **What needs to improve?** (e.g. Risk treatments are not consistently tracked)
- **What does “good enough” look like?** (e.g. All high risks have documented owners and due dates)
- **What is the simplest action that moves us forward?** (e.g. Introduce quarterly risk review meetings and update the central register)

Keep actions proportionate to your organisation’s size and resources.

Progression from Reactive to Structured often requires:

- A centralised risk register
  - Clear ownership
  - Defined review cycles
  - Basic reporting discipline
-

### **Step 3: Assign Ownership and Timeframes**

Improvement plans fail when accountability is vague.

For each action:

- Assign a named owner
- Set a realistic timeframe
- Define what completion looks like

Where risk is managed part-time, ensure uplift actions are achievable within existing capacity.

Small, consistent improvements are more sustainable than large transformation programs.

---

### **Step 4: Establish a 90-Day Forward Plan**

Rather than building a multi-year roadmap, focus on a rolling 90-day improvement plan.

A simple structure:

#### **Next 30 Days**

- Address foundational gaps
- Clarify roles and responsibilities
- Update or consolidate the risk register

#### **Next 60 Days**

- Embed structured review cycles
- Improve documentation and scoring consistency

#### **Next 90 Days**

- Strengthen reporting and monitoring
- Refine treatment tracking
- Engage leadership in maturity discussions

Reassess maturity annually to track progress.

---

## When to Seek Additional Support

Many organisations find that while the intent to improve is clear, practical challenges emerge, including:

- Limited internal capacity
- Inconsistent risk tracking
- Difficulty embedding risk into decision-making
- Lack of clear reporting for leadership or boards
- Growing regulatory or stakeholder expectations

In these cases, a structured uplift approach can accelerate progress and reduce effort.

---

## How StartRisk Can Help

StartRisk supports SMEs and not-for-profit organisations to:

- Design proportionate, ISO-aligned risk frameworks
- Facilitate risk maturity uplift planning
- Embed practical governance structures
- Implement structured risk tracking and reporting
- Improve visibility of risk treatments and controls

Whether you require a facilitated maturity workshop, targeted consulting support, or a structured risk management platform, support can be tailored to your organisation's size and capability.

If you would like to discuss your assessment results or explore next steps:

**Contact StartRisk for a confidential maturity review discussion. [Book now.](#)**