



The ISO Risk Assessment Guide

When to write one, what it must contain, and how to score severity against likelihood.

Melissa Brewer Consulting & Compliance

Guiding Compliance. Building Confidence.

832-928-5175 | mbcc.iso@gmail.com

When to Write a Risk Assessment

Risk assessments should be created for any area or action in operations where one of these four triggers applies:

Operations don't clearly match ISO 9001 requirements

Any area or action in your operation that does not clearly line up with a requirement of the standard deserves a documented risk assessment.

Processes change frequently

Where changes in processes occur with sufficient frequency, yesterday's controls may not cover today's reality.

Existing procedures are incomplete

When standard operating procedures in place are found to be incomplete, a risk assessment closes the gap until the SOP catches up.

Non-conformance is observed

Non-conformance identified through walkthroughs or internal audits is a direct trigger — assess the risk before deciding on corrective action.

The Ten Components of a Complete Assessment

- 1. Introduction** — The stated purpose and intention of the risk assessment.
- 2. Reference (optional)** — The applicable ISO 9001 clause or other quality certification scheme clauses, if applicable.
- 3. Definitions** — Key concepts, terms, or acronyms that help the reader understand how the risk assessment is applied.
- 4. Responsibility** — The employees or third-party entities who oversee completion and are authorized to change the assessment as conditions in operations change.
- 5. Hazards To Be Considered** — Identified hazards that belong in the hazard analysis where risk, severity, or likelihood is great enough that injury or death could result from the unchecked action.
- 6. Severity Definition** — The graduating scale of harm that may be caused by the risk — from Minor to Critical.
- 7. Likelihood Definition** — The graduating scale of possibility that the risk will occur during normal operations — from Unlikely to Very Likely.
- 8. Severity / Probability Chart** — The grid of numerical values at each level of operation, color-coded by control status.
- 9. Safety Assessment** — Identification of the operational steps or areas associated with the risk — with hazards, assessments, controls and preventive measures, severity, likelihood, and risk

level at each step.

10. Outcome — The up-to-date summary as of the effective date. Reviewed at least annually to verify the assessment is accurate for current operations.

The Severity × Probability Chart

Each risk lands on the grid where its severity row meets its probability column. The number — and its color — tells you how the risk must be controlled. All risks must have a corresponding reasoning or action for control.

Severity ↓ / Probability →	Unlikely	Possible	Probable	Very Likely
Minor	1	1	1	2
Serious	1	2	3	3
Major	2	3	3	4
Critical	3	4	4	4

What the Colors Mean

	Green — Level 1 A risk that is inherently controlled or mitigated through process design and/or pre-requisite programs.
	Yellow — Level 2 A risk controlled through pre-requisite programs and defined monitoring records.
	Orange — Level 3 The presence of a risk where lack of control has been observed more than once — verification is required each time the operation occurs.
	Red — Level 4 An identified hazard deemed uncontrolled without monitoring each time the activities associated with the risk occur.

A Living Document

The outcome section holds the up-to-date summary as of the effective date. Review the assessment at least annually — and whenever processes change — to verify it is accurate for current operations.

© Melissa Brewer Consulting & Compliance. This guide is general education, not legal or certification advice.
Certification decisions belong to independent, accredited certification bodies.