



treatment operations, which bring the main health, safety and environmental exposures, including effluent and emissions from surface treatment. The distribution and warehousing site holds finished goods and critical-material stock, and so carries stock-security, logistics and supply-continuity risk. Recognising where each type of risk sits helps the company assign ownership and direct monitoring to the right place.

2.3 Manual usage and maintenance

The Risk Manager maintains this manual, keeps it current, issues revisions, and makes sure the controlled master is the version in use. The manual is reviewed at least once a year and whenever a significant change in the company's context, structure or activities calls for revision. Users reach the current version through the controlled document system on the intranet, and printed copies are treated as uncontrolled. Changes are recorded in the revision history, and superseded versions are archived under the records retention schedule.

2.4 How this manual works with the procedures, tools and records

This manual sits at the head of a connected system. When a risk is managed at [Company Name], the process procedures put this manual into action: QP-05 sets the scope and criteria, QP-06 identifies, analyses and scores the risk, QP-07 selects and plans treatment, and QP-08 monitors, reviews and reports. The framework procedures QP-01 to QP-04 keep the system healthy by governing it, understanding context, assigning roles and resources, and running communication and consultation.

To show how the parts fit, the manual threads a single worked example through the system. Risk R-014 concerns the company's dependence on a single overseas supplier for a critical aluminium alloy billet used in about a third of machined production by value. This example appears in the process procedures, in the risk register (T-01) and in the sample completed forms, so that a reader can follow one real risk from identification to treatment and see the manual's principles applied in practice rather than described in the abstract.

Records are the evidence that the system is working. Each procedure names the records it produces, each record has a form in the forms library, and each form has a completed example in the sample filled forms folder. The tools (T-01 to T-03) hold the register, the treatment tracker and the framework maturity assessment. Together the manual, procedures, forms, tools and records make up the documented risk management system of [Company Name].



SECTION 4

Principles

The eight principles of ISO 31000 clause 4 are the foundation of risk management at [Company Name]. Above all, the company treats risk management as a means of creating and safeguarding value.

4 a) Integrated

Conformity. Risk management is built into all of the company's activities rather than run as a stand-alone exercise.

Our approach. The company weaves risk thinking into its governance and its core processes. Business planning, capital approval, contract acceptance, supplier approval, engineering change and project reviews each require risks to be identified and weighed before a decision is confirmed, so that risk is a normal input to decisions rather than an afterthought.

This integration is designed and sustained through QP-01, which embeds risk consideration into the company's defined decision points and names a risk owner for each part of the organisation. Because integration is a standing feature of how the company operates, it does not depend on any single person remembering to consider risk.

In practice at [Company Name], the clearest sign of integration is that a capital-investment paper or a new-customer proposal will not pass its approval gate without a completed risk assessment attached. Risk is therefore part of the evidence a decision-maker weighs, not a separate report produced after the decision has effectively been made.

Supporting documents. POL-01; QP-01; the company's decision and governance procedures.

Records. Risk register (T-01); committee and management review minutes (QF-08-02).

4 b) Structured and comprehensive

Conformity. A structured and thorough approach is used so that results can be relied on and compared.

Our approach. One documented method is applied to scope, assess, treat, monitor and report risk in every part of the business, using common criteria and a single register. A risk in machining and a risk in finance are therefore judged on the same scales and can be ranked side by side.

The structured approach also means that nothing material is left out by accident: the company works through its activities and processes systematically when identifying risk, rather than relying on whatever happens to come to mind in a meeting.



DOCUMENT CONTROL

Field	Detail
Document number	POL-01
Title	Risk Management Policy
Version / Revision	[Revision]
Date of issue	[Date]
Standard clause(s) addressed	ISO 31000:2018, clauses 4 (Principles), 5.2 (Leadership and commitment), 5.4.2 (Articulating risk management commitment)
Prepared by	ISO Consultant Panel
Reviewed by	[Name], [Designation Here]
Approved by	[Name], [Designation Here]
Next review	Annually and on significant change

REVISION HISTORY

Version	Date	Description of change	Author	Approved
1	[Date]	First issue.	ISO Consultant Panel	[Name]

SECTION 1

Purpose and context

[Company Name] is a mid-size precision engineering and manufacturing company that produces CNC-machined metal components, welded sub-assemblies and surface-treated parts for the automotive, industrial-equipment and energy sectors. The company operates from a head office and principal plant, a second manufacturing plant, and a distribution and warehousing site, and employs in the order of 380 people. The ability of the company to win contracts, deliver conforming product on time, protect its people, and sustain profitability depends on how well it anticipates and responds to uncertainty.

Uncertainty is present in every part of the business, from raw-material supply and machine reliability to customer demand, price volatility, workforce competence, information security and regulatory change. This policy establishes risk management as a deliberate, structured and integral part of how the company is governed and operated, so that uncertainty is addressed openly in decision-making rather than left to chance. It reflects the principles of ISO 31000:2018 (clause 4), under which risk management creates and protects value, is integrated into all activities, and is continually improved.



The risk assessment process

Assessment is carried out in five operating steps: identify, analyse (assess controls and score), evaluate, prioritise and record.

6.1 Step 1: Identify risks (clause 6.4.2)

The risk owner, facilitated by the Risk Manager and using WI-06-02, identifies risks that could affect the objectives in scope. Identification uses the company's risk categories (MAN-01, section 3.4) as prompts and looks at where risks come from, the causes and events behind them, both threats and opportunities, weaknesses and strengths, shifts in the context, early signals of new risks, the value of the assets at stake, and the limits of what is currently known. Risks are captured whether or not their source is under the company's control.

Each risk is written as a source, an event and a consequence and given a unique risk ID, so that it can be analysed and owned. Identification deliberately reaches beyond the shop floor to strategic, commercial, supply-chain, cyber and compliance risks, because the risks that damage a manufacturer most are often not the obvious production ones. The criterion is that identification has covered every category in scope and that each risk is described clearly enough to be analysed. The record produced is the risk identification worksheet (QF-06-01).

NOTE

A risk is described as cause and event and consequence, for example: a single overseas supplier (source) suffers an export restriction (event) that halts a machining line (consequence). This makes the later analysis and treatment much clearer.

6.2 Step 2: Analyse risk and assess existing controls (clause 6.4.3)

For each identified risk the risk owner analyses its nature and level. The team considers the uncertainties, sources, consequences, likelihood, events, scenarios and the existing controls and their effectiveness, using qualitative judgement and, where useful, quantitative data. The effectiveness of existing controls is assessed and taken into account when judging the current (residual-of-existing-controls) likelihood and consequence. Assumptions, information quality and any divergence of opinion are recorded and communicated to decision-makers. The criterion is that each risk has a documented basis for its likelihood and consequence judgement. The record produced is the risk analysis and scoring record (QF-06-02).

The effectiveness of existing controls is judged realistically rather than assumed. A control that exists on paper but is not maintained or followed gives little protection, and analysis says so. Where consequences could be severe but are highly uncertain, the team uses more than one technique and records the uncertainty, so that decision-makers understand both the estimate and how much confidence to place in it.



The risk treatment process

Treatment runs through five operating steps and repeats until the residual risk is acceptable.

6.1 Step 1: Formulate and select treatment options (clause 6.5.2)

The risk owner formulates possible treatment options and selects the most appropriate, balancing the benefits to the objectives against the costs, effort and disadvantages. The seven families of option available are set out and explained in Appendix A: stepping away from the activity, deliberately taking on more of the risk to chase an opportunity, taking out the source, reducing how likely the event is, softening its consequences, passing part of it to another party, or keeping it by an informed decision. Selection takes account of the company's obligations, stakeholder views and available resources, and recognises that a treatment can create new risks of its own and that more than one option may be used together.

Options are weighed on more than cost. A cheaper option that a key customer or the workforce would not accept may be set aside in favour of one that is equally effective and more acceptable. Where a risk is an opportunity rather than a threat, the option may be to take more of it, provided that is a conscious choice made against the criteria. The criterion is that the selected options are justified against benefit and cost and recorded. The record produced is the risk treatment option evaluation record (QF-07-01).

NOTE

Justification for treatment is broader than economics. A treatment that is cheaper but unacceptable to a key customer or to workers may be rejected in favour of one that is more acceptable, even if equally effective (clause 6.5.2).

6.2 Step 2: Prepare the treatment plan (clause 6.5.3)

The risk owner prepares a risk treatment plan using WI-07-01. A complete plan records the reasoning behind the chosen options and the benefits expected, names who approves the plan and who carries it out, lists the actions and the order they run in, sets out the people, funds and fallback arrangements each action needs, defines how success will be measured, notes the limits on the work, fixes how and to whom progress is reported and how the treatment is monitored, and gives the dates by which actions start and finish. The plan is folded into the company's management plans and processes rather than kept to one side.

Setting the order of the actions matters. The plan makes clear which treatments come first, so that the actions that reduce the most risk, or that other actions depend on, are not delayed behind less urgent work. The criterion is that the plan contains every element required by clause 6.5.3 and states the order of implementation. The record produced is the risk treatment plan (QF-07-02).

6.3 Step 3: Implement the treatment plan



Likelihood	Descriptor	Guide (per year)
1	Rare	Under 5%
2	Unlikely	5% to 25%
3	Possible	25% to 50%
4	Likely	50% to 80%
5	Almost certain	Over 80%

Consequence	Safety	Financial	Operational
1 Insignificant	First aid	Under [Cur] 25k	Under 4 hours
2 Minor	Medical treatment	25k to 100k	4 hours to 1 day
3 Moderate	Lost-time injury	100k to 500k	1 to 5 days
4 Major	Serious injury	500k to 2.5m	1 to 4 weeks
5 Severe	Fatality	Over 2.5m	Over 4 weeks

4

Method (numbered steps)

4.1 Confirm the risk statement

Check the risk is written as source, event and consequence so that likelihood and consequence can be judged.

4.2 Judge likelihood (1 to 5)

Select the likelihood level from the scale, using data where available and informed judgement where not. Record the basis for the judgement.

4.3 Judge consequence (1 to 5)

Assess the consequence in each relevant category (safety, financial, operational, environmental, compliance/reputation) and take the highest applicable level.

4.4 Calculate the score

Multiply likelihood by consequence to get a score from 1 to 25.

4.5 Read the band

Low 1 to 4; Medium 5 to 9; High 10 to 15; Extreme 16 to 25. Record the band.

4.6 Record inherent and current



Where useful, score both the inherent risk and the current risk after existing controls, to show the value of controls.

WORKED EXAMPLE

R-014: likelihood 4 (Likely) x consequence 4 (Major) = 16, which is Extreme. After treatment: likelihood 2 x consequence 3 = 6, which is Medium.

5

The 5x5 rating grid

L \ C	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

Read likelihood down the left and consequence across the top; the cell is the score. Scores 16 and above are Extreme, 10 to 15 High, 5 to 9 Medium, and 1 to 4 Low.

6

Good practice and common mistakes

Score consistently. The point of a shared scale is that a score of 12 means the same thing in machining as in finance. When judging likelihood, use the probability guide and any data available, and only fall back on judgement where there is none; record the basis either way so the score can be challenged. When judging consequence, assess every relevant category and take the highest that applies, so a rare event with a possible fatality is not understated because its financial cost would be small.

Avoid these common mistakes. Do not average the consequence categories; take the worst credible one. Do not anchor on a number because it feels comfortable; a genuine Extreme should be scored Extreme even if that is uncomfortable, because hiding it does not make it smaller. Do not confuse inherent and residual scoring: be clear whether you are scoring the risk before controls or after them, and where controls are weak in practice, do not give them full credit. Where a severe consequence is very uncertain, combine techniques rather than forcing a single precise number.

Use the score to drive action, not to end it. A score is only the input to evaluation (QP-06, Step 4): High and Extreme risks must be treated, and an Extreme risk is escalated immediately. The score is a means of prioritising attention, not a substitute for the decision that follows.



Item	Detail
Participants	People who know the work: operators, engineers, planners, buyers, quality, plus the risk owner. Six to ten works well.
Inputs	The scope and context (QF-05-01), the risk categories (MAN-01 section 3.4), past incidents and near-misses, and the current register.
Materials	Risk identification worksheet (QF-06-01); the category prompts; a means to capture risks visibly.

4

Method (numbered steps)

4.1 Open and set the scope

State the objectives and boundaries from QF-05-01 and the ground rule that all risks, including opportunities and unwelcome ones, are wanted and no blame attaches to raising them.

4.2 Work category by category

Take each risk category in turn and ask what could help or prevent the objectives. Use the prompts: sources, causes and events, threats and opportunities, vulnerabilities, changes in context, emerging-risk indicators.

4.3 Describe each risk

For each risk agreed, capture it as source, event and consequence, and give it a draft risk ID. Avoid vague statements.

4.4 Challenge for gaps

Ask what has been missed: risks whose source is outside the company's control, rare but severe events, and risks arising from existing controls or from other risks.

4.5 Group and de-duplicate

Combine duplicates and group related risks, keeping distinct risks separate so they can be owned and treated.

4.6 Assign owners and next step

Propose a risk owner for each risk and confirm the risks will be analysed and scored under QP-06.

FACILITATION TIP

Keep scoring out of the identification workshop. Judging likelihood and consequence too early narrows

	FORM Risk Identification Worksheet Associated procedure: QP-06 [Company Name]	QF-06-01 Rev [Revision] Issued [Date]
---	--	---

Section 1 Identification

ASSESSMENT REF	DATE	FACILITATOR

Risk ID	Category	Source	Event	Consequence

This documentation toolkit was developed by the consultant panel of isofolder.



FORM

Risk Treatment Plan

Associated procedure: QP-07- |
[Company Name]

QF-07-02

Rev [Revision]
Issued [Date]

Section 1 Plan header

RISK ID

OWNER

TARGET RESIDUAL

RATIONALE AND EXPECTED BENEFITS

Section 2 Actions

Action	Owner	Resource	Measure	Start / finish	Status

Section 3 Reporting, constraints, approval

REPORTING, MONITORING AND CONSTRAINTS

PREPARED BY	REVIEWED BY	APPROVED BY
ISO Consultant Panel Designation: ISO Consultant Panel Signature / Date:	[Name] Designation: [Designation Here] Signature / Date:	[Name] Designation: [Designation Here] Signature / Date:

This documentation toolkit was developed by the consultant panel of isofolder.