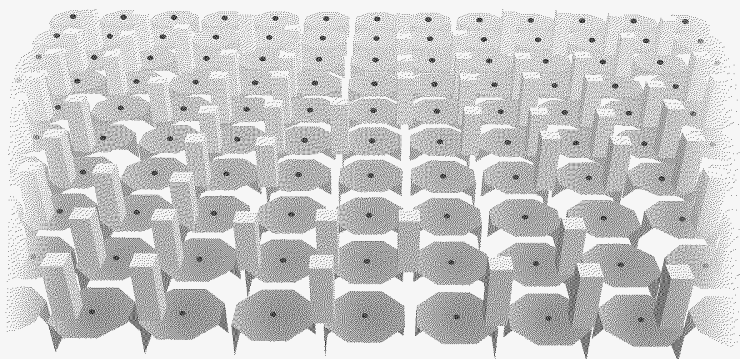




GUIDE 04 RISK MANAGEMENT

Reading an ISO 14971 risk analysis

How a risk file is built, what a good one contains, and the places where a weak one shows.



ABOUT

Every device developed under design controls carries a risk file. It is the manufacturer's own written answer to one question: what can go wrong with this device, and what did we do about it?

This guide explains how a risk file is put together under ISO 14971, how to read its tables, and how to tell whether the failure in front of you was foreseen, controlled, and watched after the device reached the market. It ends with the questions an engineering reviewer asks of every risk file.

FOR

Legal counsel who must decide whether a hazard was known and what the manufacturer did about it.

Manufacturers — engineering and quality teams who maintain a risk file or prepare it for review.

Hospitals — risk managers and clinical engineering who evaluate a supplier's risk documentation.

NOTE

This guide is general technical information. It is not legal advice. ISO 14971:2019 is the current edition; files written under ISO 14971:2007 or EN ISO 14971:2012 use slightly different terms. Read each file against the edition it cites.

In this guide

01	What a risk file is	04
	Figure: the loop, and where it breaks	05
02	Reading the tables	06
03	After the device ships	08
04	Where a weak file shows	09
	Example: one row, read two ways	11
	Checklist	12
	Sources	13
	How Alpha Devices helps	14
	Terms	15

01

What a risk file is

ISO 14971 is the standard for risk management of medical devices. FDA recognizes it, and the Quality Management System Regulation requires risk management throughout design and production, by way of ISO 13485. The standard does not say how safe a device must be. It says how a manufacturer must decide that, write the decision down, and keep it current.

The output is the risk management file. It is not one document but a set: a plan, an analysis, the controls, their verification, an evaluation of what risk remains, and a record of what the field has taught since. A reviewer reads it in that order.

PLAN	What the process will cover, who does it, and the criteria for calling a risk acceptable. The criteria are set here, by the manufacturer, before the analysis.
ANALYSIS	Intended use and foreseeable misuse; the hazards; the sequences of events that lead from hazard to harm; and for each one an estimate of probability and severity.
CONTROLS	For each risk that needs reducing: the measure chosen, in the order the standard requires, and the evidence that the measure works.
RESIDUAL	What risk remains after the controls, judged against the plan's criteria, and the overall benefit-risk conclusion.
FIELD	Production and post-production information, reviewed against the file, with the file revised when the field says something new.

NOTE

A risk file written once and never revised is a file that stopped describing the device the day it shipped.

FIGURE

The loop, and where it breaks

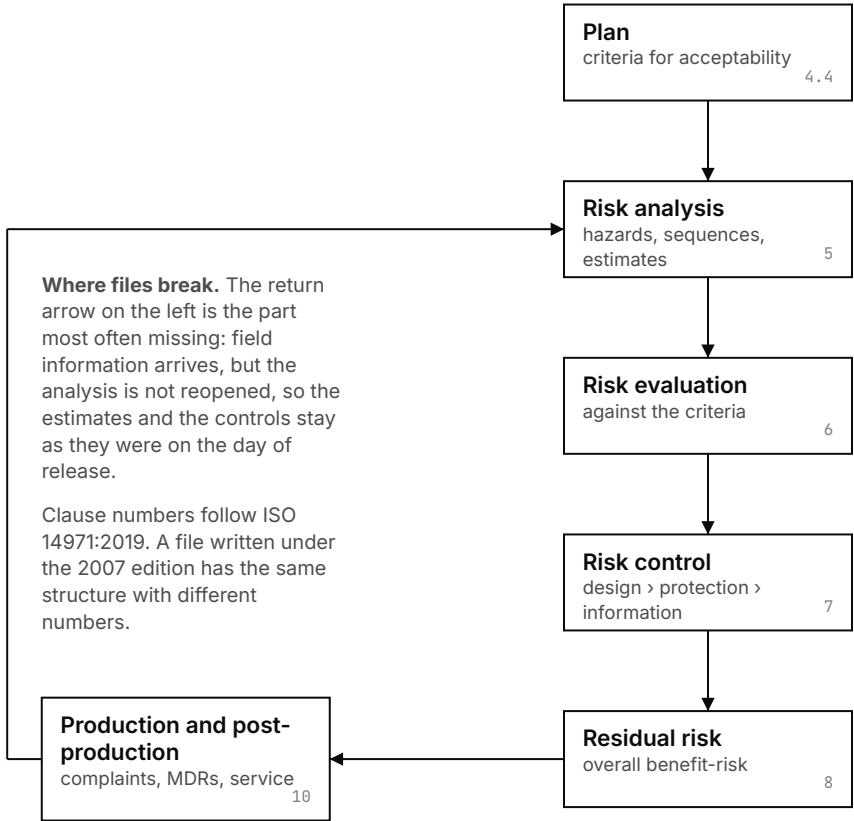


FIG 01

The forward chain runs from the plan to the residual-risk conclusion. Clause 10 closes the loop: what production and the field report must go back into the analysis. A file is current only if that arrow has been followed.

02 Reading the tables

Most of a risk file is tables. Each row is one path from a hazard to a harm, with numbers attached. The steps below are the order in which to read a row, and the questions to ask at each column.

01

Find the hazard, the sequence, and the harm

A row should name three things separately: the *hazard* (a source of harm, such as stored energy, a hot surface, an incorrect output), the *sequence of events* that leads from the hazard to the patient, and the *harm* itself. Rows that name only a component failure ("sensor fails") without the sequence and the harm have not finished the analysis.

Look for the row that matches the event in question. If there is none, the hazard was not foreseen; if there is one, the rest of the row tells you what was done about it.

02

Read the estimates, then ask where they came from

Each row carries a probability and a severity, usually as scores. The scores are the manufacturer's estimates, and the standard requires them to be based on something: field data, test data, published rates, or expert judgment, stated as such.

A probability of "remote" with no data behind it is an assumption. An analysis in which every row lands just inside the acceptable region deserves a second look at how the scores were chosen.

03

Check the order of the controls

ISO 14971 sets the order in which risk-control options must be considered: first a design that removes or reduces the hazard, then a protective measure in the device or its production, and only then information for safety, such as a warning or training. The file should show that the earlier options were considered before a later one was chosen.

A hazard controlled by a warning alone is the lowest form of control the standard allows. The question is whether a design or protective option was available and why it was not used. The answer, if there is one, is in the option analysis.

04

Look for the verification of each control

A control is a claim until it is verified. The file should point, for each control, to the test or the design evidence that shows it works, and should consider whether the control itself introduced a new hazard. "Control: alarm" is not verified by the existence of the alarm; it is verified by a test that the alarm sounds in the conditions the row describes.

CAUTION

A failure mode and effects analysis (FMEA) is one input to a risk analysis, not the whole of it. An FMEA starts from component failures and works outward; it misses hazards that arise with no failure at all, such as a foreseeable misuse or a correct output used in the wrong situation. A file that consists only of FMEA tables has covered half the question.

03

After the device ships

Clause 10 is the part of the standard that connects the risk file to the rest of the manufacturer's record. The manufacturer must collect information from production and from the field, complaints, service, adverse-event reports, and the literature, and review it against the file. When the information shows a hazard not foreseen, a risk estimate that was wrong, or a control that does not work in the field, the analysis must be reopened and the file revised.

This is the arrow on the left of the figure, and it is the one most often missing. The risk file was written to get the device released. The complaint system was built to handle complaints. Often nobody owns the link between them, and the file keeps the estimates of the day of release while the complaint database fills.

READ WITH

Guide 13 (complaints, MDRs and CAPA) and guide 15 (the timeline). A risk file dated before the first complaints, placed on the timeline next to those complaints, is the clearest picture of this gap.

KEY POINT

The risk file shows what the manufacturer decided. The complaint file shows what the device did. A reviewer reads them together, and the dates decide which one was written in the knowledge of the other.

04

Where a weak file shows

These are the patterns an engineering reviewer looks for. Each is a question for the file, and a well-kept file answers it.

01

Estimates without data

Probability scores with no source, or the same score on every row. Ask for the data or the rationale the plan requires.

02

Severity rated down

A harm scored as “minor” that the complaint file describes as an injury. Compare the harm in the row with the harm in the field.

03

Warnings as the control

Rows where information for safety is the only control, with no option analysis of design or protective measures.

04

Acceptable by assertion

Rows marked acceptable with no criteria in the plan, or criteria changed after the analysis so the rows fit.

05

Controls not verified

Controls listed without a reference to the test or evidence that shows they work, or verified only in the lab.

06

No revision after the field

A file whose last revision predates the complaints, the MDRs, or the recall. The clause 10 arrow was not followed.

07

The event is not in the file

No row matches what happened. Either the hazard was not foreseen, or it was removed between revisions. Ask for every revision.

EXAMPLE

One row, read two ways

An invented row for a generic infusion device, shown as a file might present it, and then as a reviewer reads it.

HAZARD	SEQUENCE / HARM	P	S	CONTROL
Under-delivery of therapy	Line kinks; pressure rises; occlusion alarm delayed; dose not delivered; delayed therapy	2	3	Alarm; IFU warning

AS FILED Probability 2 of 5, severity 3 of 5, product inside the acceptable region. Control: the occlusion alarm, plus a warning in the instructions. Verified: "alarm function tested". Status: acceptable.

AS READ Where does probability 2 come from, and does the complaint file agree? Why is the harm "delayed therapy" when the drug in the intended use is one where a delay is an injury? The alarm is a protective measure; was a design option, such as a pressure limit that stops the pump, considered and rejected, and why? "Alarm function tested": under which occlusion pressure, which line, which flow rate, and how long did the alarm take? Was the row revised after the complaints about late alarms?

WHAT FOLLOWS Each question points to a document: the plan's criteria, the complaint trend, the option analysis, the verification protocol, the revision history. None of them decides the case alone. Together they show whether the row was an analysis or a form.

CHECKLIST

Reading a risk file

- ☐ Plan obtained; acceptability criteria read before the tables
- ☐ Edition of ISO 14971 cited; terms read against that edition
- ☐ Every revision of the file obtained, with dates
- ☐ Row found that matches the event, or its absence noted
- ☐ Hazard, sequence, and harm named separately in that row
- ☐ Source of each probability and severity estimate identified
- ☐ Order of controls checked: design, protection, information
- ☐ Verification evidence found for each control in the row
- ☐ New hazards from the controls considered
- ☐ Clause 10 review found: field data compared with the file
- ☐ File revision dates placed on the timeline next to complaints and MDRs
- ☐ Questions written as questions, with the document each one points to

SOURCES

Sources and further reading

ISO 14971:2019 — Application of risk management to medical devices

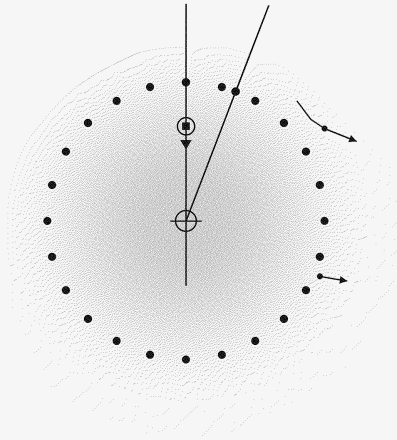
[iso.org](https://www.iso.org)

ISO/TR 24971:2020 — Guidance on the application of ISO 14971

[iso.org](https://www.iso.org)

FDA — Recognized Consensus Standards database (ISO 14971 recognition)

accessdata.fda.gov



SERVICES

We test the row against the device

A risk file makes claims about how the device behaves. We check those claims on the bench, against the complaint record, and against the standard the file cites.

01

Risk file review

We read the file as engineers: estimates, option analyses, verification, and revisions, and we list the questions each row leaves open.

02

Verification on the bench

We test the controls the file relies on, in the conditions the rows describe, and report what the control does and does not do.

03

Connecting the record

We place the file's revisions on the timeline with the complaints, MDRs, and changes, and explain what the sequence shows.

TERMS

Terms used in this guide

Hazard

A potential source of harm: an energy, a substance, a sharp edge, a software fault.

Hazardous situation

A circumstance in which people, property, or the environment are exposed to one or more hazards.

Harm

Injury or damage to the health of people, or damage to property or the environment.

Risk

The combination of the probability of occurrence of harm and the severity of that harm.

Risk control

The measures taken to reduce a risk: inherently safe design first, protective measures second, information for safety last.

Residual risk

The risk that remains after risk control measures have been taken, judged against the criteria in the plan.

Risk management file

The set of records produced by the risk management process, from the plan to the post-production review.

Post-production information

Complaints, service data, field actions, and literature that must be reviewed against the risk file after the device is on the market.

Tell us about the device.

Send a short description of the device, the event, and any deadlines. We will tell you what to preserve now and recommend the next steps.

EMAIL info@alphadevices.io

WEB alphadevices.io

GUIDES

- | | | | |
|----|---|----|--------------------------------------|
| 01 | A device failed. What happens next? | 09 | How a device reaches the market |
| 02 | Searching MAUDE with purpose | 10 | Why the alarm did not help |
| 03 | Understanding waterfall design | 11 | When the software is the suspect |
| 04 | Reading an ISO 14971 risk analysis | 12 | Use error is a design question |
| 05 | The manufacturer's record | 13 | Complaints, MDRs and CAPA |
| 06 | Using LLMs to review case documents | 14 | Recalls, corrections and quiet fixes |
| 07 | What the device recorded | 15 | What did they know, and when? |
| 08 | The joint inspection | | |

Alpha Devices

2101 Brandywine Street, Suite 200
Philadelphia, PA 19130

Independent medical device engineering. © 2026 Alpha Devices.

