A FIELD GUIDE TO MEDICAL-DEVICE SAFETY

ISO 14971

Risk Management for Medical Devices

Building safety into every stage of the device lifecycle — from hazard identification and risk control to post-market surveillance. A concise, decision-ready briefing for MedTech leaders.

ISO 14971:2019 | FDA recognized consensus standard | EU MDR 2017/745 · IVDR | IMDRF aligned

Safety is engineered, not assumed.

Every device carries inherent risk. Across a vast, fast-moving global market, structured risk management is what separates a trusted product from a recall — and a patient kept safe from one who is harmed.

1.5M+

distinct medical devices & 10,000+ device types in use worldwide

Source: World Health Organization

~83,000

deaths & 1.7M injuries linked to devices in adverse-event reports over a decade

Source: ICIJ Implant Files · FDA MAUDE

1 in 10

patients harmed while receiving hospital care in developed countries

Source: World Health Organization

$850B

projected global device market by 2030, up from ~$570B in 2023

Source: Statista market estimates

U.S. device recalls hit a four-year high of 1,059 events in 2024 — with Class I recalls at a 15-year peak. Units affected surged 55%. Design and software defects remain leading root causes.

Sedgwick Recall Index · FDA · UL Solutions

What is ISO 14971?

ISO 14971 is the **international standard for the application of risk management to medical devices.** It defines a systematic process to identify hazards, estimate and evaluate risk, control that risk, and monitor effectiveness across the entire product lifecycle.

Current edition: ISO 14971:2019

Guidance: ISO/TR 24971

Pairs with ISO 13485 QMS

The Risk Management File (RMF)

A single, living record that traces every hazard to its controls and residual risk — the auditable backbone of compliance.

Globally recognized

An FDA recognized consensus standard, harmonized for EU MDR/IVDR and accepted by regulators worldwide.

Whole-lifecycle

Covers concept and design through manufacturing, market and post-market surveillance — not a one-time check.

Structured & auditable

Turns safety into traceable evidence — defensible in audits, submissions and notified-body review.

Benefit–risk clarity

Frames decisions around whether benefits outweigh residual risk — the core question every reviewer asks.

Hazard, harm & the anatomy of risk

ISO 14971 is precise about its vocabulary. A hazard only becomes harm through a chain of events — and risk is what we estimate along the way.

Hazard

A potential source of harm. *e.g. an infusion pump software defect.*

→

Sequence of events

The triggering circumstances. *e.g. dose miscalculated under load.*

→

Hazardous situation

People exposed to the hazard. *e.g. patient connected to the pump.*

→

Harm

Injury or damage to health. *e.g. patient over-infusion.*

RISK = **PROBABILITY** of harm occurring × **SEVERITY** of that harm

Why the chain matters: controls can break the sequence at any link — eliminating the hazard, preventing the situation, or reducing severity — so estimating risk along the chain is what makes mitigation effective.

The ISO 14971 risk-management process

A continuous, closed loop — not a linear gate. Findings from the real world feed back into analysis for as long as the device is on the market.

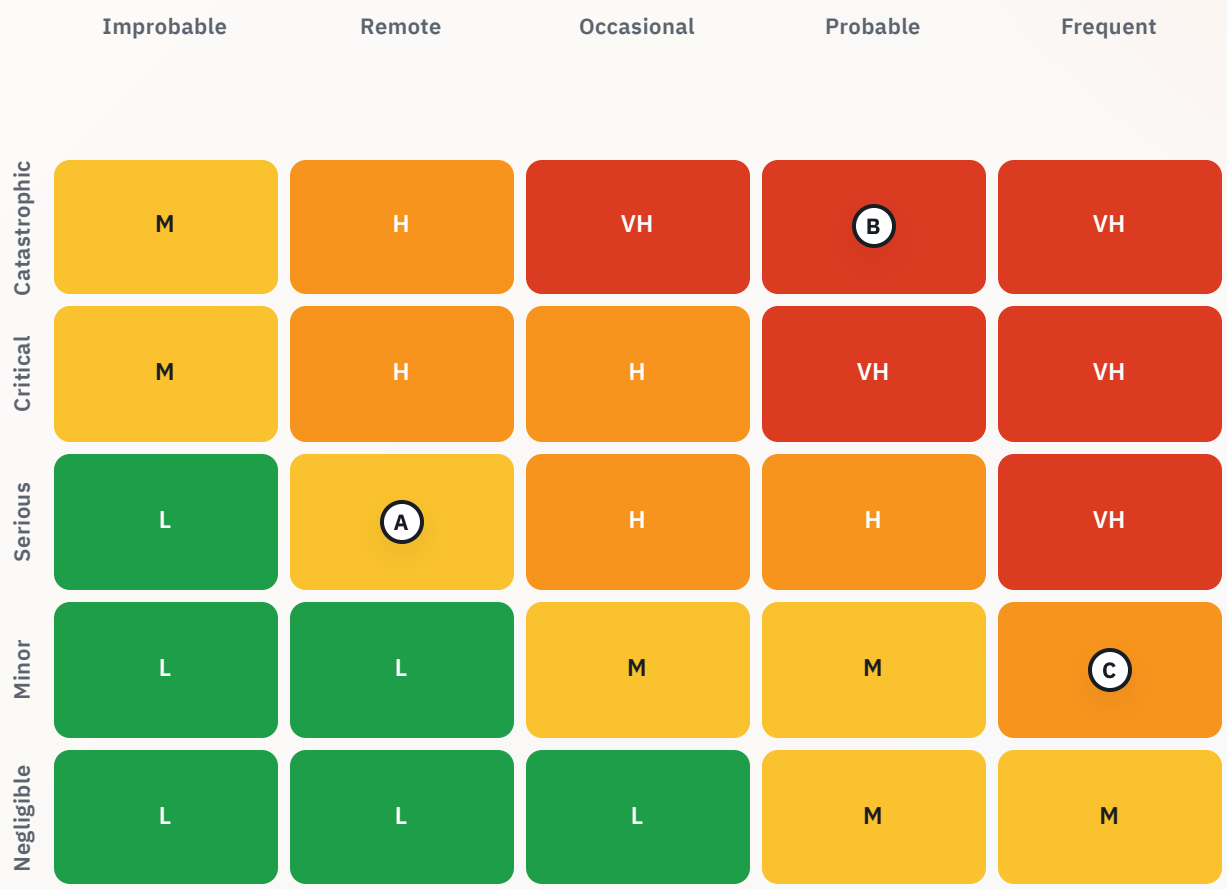
1. **Risk management plan**
   Define scope, responsibilities, acceptability criteria and review cadence.
2. **Risk analysis**
   Intended use & misuse; identify hazards and hazardous situations; estimate risk.
3. **Risk evaluation**
   Compare each estimated risk against your acceptability criteria.
4. **Risk control**
   Select & implement measures; verify effectiveness; check for new risks.
5. **Residual & benefit–risk**
   Evaluate overall residual risk; weigh it against clinical benefit.
6. **Production & post-production**
   Monitor in the field; collect data; act on signals.

Post-market findings feed back into risk analysis & the Risk Management File

Risk Management Report — Signed off **before release** — confirming the plan was implemented and residual risk is acceptable.

Estimating risk: severity × probability

A risk matrix turns judgement into a shared, defensible map. Each hazardous situation is placed by how badly it could harm and how likely it is.



- **Low** — broadly acceptable; document and monitor
- **Medium** — reduce as far as possible (ALARP)
- **High** — control required before release
- **Very high** — unacceptable; redesign needed

Example placements

A · Sensor drift causing a misread — serious, but remote.

B · Software fault delivering a lethal dose — rare but catastrophic.

C · Frequent minor skin irritation from an adhesive.

ISO 14971 · Illustrative 5×5 matrix — criteria are device-specific

The risk-control hierarchy

ISO 14971 requires controls in a strict priority order. Designing the risk out beats warning about it — labeling is the last resort, not the first.

MOST EFFECTIVE

LEAST EFFECTIVE

1 **Inherently safe design & manufacture**
Eliminate the hazard or reduce its severity at the source — safer materials, fail-safe architecture, removing a failure mode entirely.

2 **Protective measures**
Guards, alarms, interlocks, redundancy and automatic safety functions built into the device or its manufacturing process.

3 **Information for safety**
Warnings, labeling, instructions for use and training — relied on only when design and protection cannot reduce risk further.

Reduction in practice

Design · Connector keyed so a tube cannot be misconnected.

Protect · Software dose-limit alarm with hardware cutoff.

Inform · Clear IFU and on-screen confirmation step.

Each control must be verified for effectiveness — and checked that it introduces no **new** risks.

Risk management across the lifecycle

Risk management starts at the first concept sketch and never stops — the file is updated as the device moves from idea to retirement.

Concept
Intended use, early hazard identification

Design & Development
Risk analysis drives design controls

Verification & Validation
Confirm controls are effective

Transfer & Manufacturing
Process risks, change control

Launch
Risk Management Report sign-off

Post-Market
Surveillance, vigilance, improvement

Pre-market activities

- Establish the risk management plan & acceptability criteria
- Identify hazards; estimate and evaluate every risk
- Implement & verify risk controls in the design
- Assess overall residual risk and benefit–risk

Post-market activities

- Active surveillance, complaint handling & vigilance reporting
- Trend production & field data against expectations
- Feed new information back into risk analysis (CAPA)
- Update the Risk Management File — and the device if needed

Common mistakes & best practices

Most findings aren't exotic — they're the same avoidable patterns. The fixes are well understood.

Common pitfalls

- Treating risk management as a one-time document for the submission
- Starting risk analysis after the design is already frozen
- Ignoring use error & human factors as a hazard source
- Over-relying on warnings & labeling instead of design controls
- A weak or non-existent post-market feedback loop

Best practices

- Start at concept & keep the Risk Management File living
- Integrate risk with design controls & the ISO 13485 QMS
- Apply IEC 62366 usability engineering to use-related risk
- Prioritize design-level controls; document benefit–risk explicitly
- Close the loop: surveillance data drives design improvement

Industry insight: device design and software design account for roughly **50% of AI/ML-enabled device recalls** — and software design is the single largest software-related recall cause across the FDA's 56,000-record database.

JMIR · IEEE Spectrum (FDA data)

Build safety in — and keep it living.

01 **Start at concept**
The cheapest, most effective controls are the ones designed in early.

02 **Keep the file living**
The RMF is a continuous record, not a submission artifact.

03 **Design out, don't warn around**
Honor the control hierarchy — labeling is the last resort.

04 **Close the post-market loop**
Field evidence is the truest test of your risk estimates.

WHERE IT'S HEADING

- AI/ML device governance
- Cybersecurity as safety
- Real-world post-market data
- Global harmonization (IMDRF)

Designing a connected medical device?

CitrusBits builds safety-first apps, devices and regulated software — with ISO 14971 risk management built into the process from day one.

sales@citrusbits.com

925-452-6012 · Pleasanton, CA