ISO 14971

Medical devices — Application of risk management to medical devices

Condensed Practical Reference & Field Checklists

Prepared for use by quality/regulatory staff, biomedical engineers, and technical teams at medical device manufacturers, refurbishers, and distributors — covering the risk management process and practical, ready-to-use working checklists.

Important note on scope and use: *This document is an original, independently written condensed overview and practical checklist tool. It summarizes, in the author's own words, the general process and key concepts covered by ISO 14971:2019 (and its 2020 European application guidance, EN ISO 14971) for quick field reference. It is* ***not a reproduction of the official standard text****, is not a substitute for it, and must not be used as the sole basis for a formal risk management file, certification audit, or regulatory submission. For any formal compliance, audit, or regulatory work, the current officially licensed ISO 14971:2019 text (and applicable regional regulation, e.g. EU MDR 2017/745, US FDA requirements) must be consulted directly, ideally with input from a qualified quality/regulatory professional.*

Delara Mohammadi
MedTech Consultant

delaramohammadi.com | info@delaramohammadi.com
+98 938 400 3858

1. About This Standard

ISO 14971 is the internationally recognized standard describing how manufacturers (and, in practice, refurbishers and other actors who modify or return medical devices to service) should systematically identify hazards, estimate and evaluate the associated risks, control those risks, and monitor the effectiveness of those controls throughout a device's life cycle. It is not a design or safety standard in itself — it is a *process* standard: it does not tell you what risk is acceptable for a specific device, but it tells you how to systematically arrive at, document, and defend that judgment.

1.1 Why it matters even for refurbishment/export businesses

- ISO 13485 (the QMS standard) explicitly expects risk management to run through design, purchasing, production, and corrective-action decisions — **ISO 14971 is the method referenced to do that consistently**, rather than a separate, optional activity.
- Any modification made during refurbishment (component substitution, software/firmware changes, repurposing for a different clinical use) can introduce new risks not covered by the original manufacturer's risk file, and should be assessed on its own merits.
- Regulators and institutional buyers increasingly expect to see a risk management file (or at least risk-based justification) accompanying technical documentation for refurbished or re-certified equipment, particularly for export into regulated markets.
- Even without full manufacturer-level design authority, a documented risk-based rationale strengthens credibility with hospital procurement teams and regulators alike.

2. The Risk Management Process — Overview

ISO 14971 describes risk management as a continuous cycle across the device life cycle, not a one-time document produced before launch. The core stages are summarized below.

Stage	What it involves
Risk management planning	Define the scope of the device(s) covered, criteria for risk acceptability, roles/responsibilities, and how the process will be reviewed and verified — documented in a risk management plan before analysis begins.
Risk analysis	Identify the device's intended use and reasonably foreseeable misuse; identify hazards and hazardous situations; estimate the probability of occurrence and severity of harm for each.
Risk evaluation	Compare each estimated risk against the pre-defined acceptability criteria to decide whether risk control is required.
Risk control	Identify and implement measures to reduce unacceptable risk, in the standard's preferred order: (1) inherently safe design, (2) protective measures in the device or manufacturing process, (3) information for safety (labeling, warnings, training) — used only after the first two options are exhausted, not as a substitute for them.
Residual risk evaluation	Re-assess risk after controls are applied; verify controls were implemented as intended and are effective; evaluate overall residual risk from all remaining risks together, not just individually.
Risk management review	Confirm the process was carried out as planned before the device is released, with results reviewed by responsible personnel.
Production and post-production information	Continuously collect data after release (complaints, service/repair data, incident reports, literature) and feed it back into the risk file, updating the analysis if new hazards or risks emerge.

3. Key Concepts and Terminology

Term	Meaning
Harm	Physical injury, damage to health, or damage to property/environment.
Hazard	A potential source of harm (e.g. an electrical fault, a dosing error, a sharp edge).
Hazardous situation	A circumstance in which people, property, or the environment are exposed to one or more hazards.
Severity	A measure of the possible consequences of a hazard, typically ranked on a defined scale (e.g. negligible → catastrophic).
Probability of occurrence	The likelihood of a hazardous situation leading to harm, typically ranked on a defined scale (e.g. improbable → frequent).
Risk	The combination of the probability of occurrence of harm and the severity of that harm — usually plotted on a risk matrix (probability × severity) to visualize acceptability.
Risk control measure	An action or device feature intended to reduce a risk — following the hierarchy of inherent safety by design, protective measures, then information for safety.
Residual risk	The risk remaining after risk control measures have been applied.
Overall residual risk	The combined effect of all individual residual risks considered together for the device as a whole — must also be judged acceptable, even if each individual risk is acceptable on its own.
Benefit-risk analysis	Where residual risk is not judged acceptable by the usual criteria, a documented judgment of whether the clinical benefit of using the device outweighs the residual risk.
Reasonably foreseeable misuse	Use of the device in a way not intended by the manufacturer, but which can be reasonably anticipated from human behavior and the device's characteristics — must be considered, not just correct/intended use.

4. Illustrative Risk Matrix (Practical Example)

A risk matrix is a common practical tool for visualizing and evaluating risk once severity and probability have been estimated. The example below uses a simple 5×5 layout; exact scales, category labels, and acceptability zones are decisions each organization must define and justify in its own risk management procedure — the below is illustrative only, not a mandated scale from the standard.

Probability ↓ / Severity →	Negligible	Minor	Moderate	Major	Catastrophic
Frequent	Med	Med	High	High	High
Probable	Low	Med	Med	High	High
Occasional	Low	Low	Med	Med	High
Remote	Low	Low	Low	Med	Med
Improbable	Low	Low	Low	Low	Med

Example application: *a refurbished infusion pump with a worn occlusion sensor might have a hazardous situation of "under-infusion not detected," estimated as Occasional probability and Major severity (potential for inappropriate therapy) → falls in the "Medium" zone → requires a documented risk control decision (e.g. sensor replacement and functional verification as part of the refurbishment procedure) before the residual risk is re-evaluated and accepted.*

5. Applying This to a Refurbishment/Export Context

- **Treat each refurbishment/service scope as a mini risk-analysis trigger:** ask what could newly go wrong because of the specific work performed (part substitution, cleaning process, software update), not just whether the device passes its standard functional test.
- **Document reasonably foreseeable misuse for the destination context** — e.g. differing power quality, language barriers with labeling, or different clinical staffing levels in the export market may change which hazardous situations are realistic.
- **Prefer design/inherent fixes over warning labels** — if a recurring fault is discovered across a device population (e.g. a specific model's connector wears out early), the preferred response is a physical/process fix (e.g. revised inspection criteria, part upgrade), not simply a new warning sticker.
- **Feed field data back into the file** — complaints, repeat repairs, and incident reports from customers should be reviewed periodically and connected back to the relevant hazard/risk entries, consistent with the standard's post-production information stage.
- **Keep records defensible** — a risk management file should let a third party (auditor, regulator, customer) trace the logic from hazard → estimated risk → control measure → residual risk → acceptance decision.

6. Practical Field Checklists

Use these as a starting self-assessment and working-document set for risk management activities. They condense the general process above into actionable items; they do not replace a formal risk management file developed and reviewed by qualified quality/regulatory personnel per the full standard.

A. Risk Management Planning Checklist

Check Item / Action	Status
■ Scope of the risk management activity defined (which device/model/modification is covered).	Y / N / NA
■ Risk acceptability criteria defined and documented before analysis begins (not decided case-by-case after the fact).	Y / N / NA
■ Roles and responsibilities for risk management activities assigned.	Y / N / NA
■ Method for risk analysis (e.g. matrix approach, scales for severity/probability) documented.	Y / N / NA
■ Plan for verification of risk control measures and overall residual risk evaluation defined.	Y / N / NA
■ Plan for collecting and reviewing post-production information (complaints, service data, incident reports) defined.	Y / N / NA

B. Risk Analysis Checklist

Check Item / Action	Status
■ Intended use and intended patient/user population documented.	Y / N / NA
■ Reasonably foreseeable misuse scenarios identified and documented (not just correct/intended use).	Y / N / NA
■ Hazards identified systematically (electrical, mechanical, biological, use-related, software, etc.).	Y / N / NA
■ Hazardous situations linked to each hazard, describing how exposure could occur.	Y / N / NA
■ Severity of potential harm estimated for each hazardous situation using a defined scale.	Y / N / NA
■ Probability of occurrence estimated for each hazardous situation using a defined scale.	Y / N / NA
■ Each risk plotted/evaluated against the pre-defined acceptability criteria.	Y / N / NA

C. Risk Control Checklist

Check Item / Action	Status
■ For each unacceptable risk, control options considered in the standard's preferred order: inherent safety by design first, then protective measures, then information for safety.	Y / N / NA
■ Selected control measure(s) documented with rationale.	Y / N / NA
■ Control measures implemented and verified as actually in place (not just planned).	Y / N / NA
■ New risks potentially introduced by the control measure itself identified and assessed.	Y / N / NA
■ Residual risk after controls re-estimated and compared against acceptability criteria.	Y / N / NA
■ Where residual risk remains above the acceptance threshold, a documented benefit-risk analysis performed.	Y / N / NA
■ Overall residual risk (combined effect of all remaining individual risks) evaluated, not just each risk in isolation.	Y / N / NA

D. Risk Management Review & File Checklist

Check Item / Action	Status
■ Risk management plan was followed as documented, or deviations are explained and justified.	Y / N / NA
■ All identified risks have a documented evaluation outcome (accepted, controlled, or benefit-risk justified).	Y / N / NA
■ Overall residual risk formally reviewed and accepted by a responsible, named individual before release.	Y / N / NA
■ Risk management file is complete and traceable: hazard → risk estimate → control → residual risk → acceptance decision, for every entry.	Y / N / NA
■ File is readily available for audit/regulatory review and is version-controlled.	Y / N / NA

E. Post-Production / Post-Market Feedback Checklist

Check Item / Action	Status
■ Defined channel exists to collect field information: complaints, repair/service data, user feedback, relevant literature or incident reports from similar devices.	Y / N / NA
■ Field data reviewed on a defined schedule (not only reactively after a serious event).	Y / N / NA
■ New or previously unidentified hazards found in the field are added to the risk analysis.	Y / N / NA
■ Where field data suggests a risk estimate was too optimistic, the relevant risk entries are re-evaluated and, if needed, the device/process/labeling is updated.	Y / N / NA
■ Trends (not just isolated incidents) are analyzed to detect systemic issues across a device population.	Y / N / NA
■ Serious findings are cross-checked against regulatory vigilance/incident-reporting obligations (see the companion ISO 13485 checklist set, Section F).	Y / N / NA

Reminder: *these checklists are a practical starting template for internal self-assessment and team discussion. A complete, defensible risk management file — especially one intended to support regulatory submission or certification — should be developed and reviewed with a qualified quality/regulatory professional against the full ISO 14971:2019 text.*