QUALITY EXCELLENCE SERVICES

Quality Excellence Services
18 Maple Avenue, Ste. 148
Barrington, RI 02806
United States of America
+1 (401) 246-3204 · +1 (401) 252-9653
mweeden@qesisbest.com · https://QESisBest.com

STANDARDS & GUIDANCE REPORT · INTERNATIONAL · INTERNATIONAL STANDARD

ISO 14971:2019

Medical devices — Application of risk management to medical devices

DOCUMENT	QES-WP-103, Rev B	DATE	November 7, 2026
ISSUED BY	ISO/TC 210 with IEC/SC 62A	PREPARED BY	Conner Davidson
EDITION	Third edition, 2019 (EN ISO 14971:2019 + A11:2021 in the EU), with guidance in ISO/TR 24971:2020	STATUS CHECKED	October 24, 2026
INDUSTRIES	Medical Devices	ONLINE	qesisbest.com/standard-iso-14971.html

CURRENT EDITION ISO/TR 24971:2020 gives the guidance, and ISO/TS 24971-2:2026 now adds guidance for devices that use machine learning. **Next:** No new edition announced.

What It Covers

The process a manufacturer uses to identify hazards, estimate and evaluate risks, control them, judge the overall residual risk against the benefits, and keep watching once the device is on the market.

Who It Applies To

Every medical device manufacturer, for every device, across the whole life cycle. ISO 13485, the EU MDR and the US QMSR all expect it, directly or through the state of the art.

Key Requirements

- A risk management plan and a risk management file for each device (4.4, 4.5).
- Criteria for risk acceptability set by a policy from top management (4.2).
- Risk analysis, evaluation and control, in the order: inherent safety by design, protective measures, information for safety (5–7).
- Evaluation of overall residual risk against the benefits, and a review before release (8, 9).
- Production and post-production information collected and fed back into the risk file (10).

Structure at a Glance

PART	TOPIC	WHAT IT ASKS FOR
4	General requirements	Process, management responsibilities and policy, competence, the plan, and the file.
5	Risk analysis	Intended use, safety characteristics, hazards and hazardous situations, risk estimation.
6	Risk evaluation	Comparing each estimated risk against the acceptability criteria.
7	Risk control	Option analysis, implementation, residual risk, benefit-risk, new risks, completeness.
8	Overall residual risk	Judging the residual risk of the device as a whole against its benefits.
9	Risk management review	Confirming before release that the plan was carried out.

PART	TOPIC	WHAT IT ASKS FOR
10	Production and post-production	Collecting and reviewing information and acting on it.

What an Auditor Asks to See

- The risk management plan and the acceptability criteria behind it.
- Traceability from each hazard through its controls to verification of their effectiveness.
- The overall residual risk evaluation and the benefit-risk conclusion.
- Evidence that complaints and post-market data have reopened the risk file when they should.

Requirements Checklist

Work down the list with the evidence in hand; write where each item is evidenced in the right-hand column.

#	REQUIREMENT	EVIDENCE ON FILE
1	Risk policy and acceptability criteria approved by top management.	
2	Plan states scope, responsibilities, review requirements, acceptability criteria, and verification activities.	
3	Intended use and reasonably foreseeable misuse documented.	
4	Hazards identified for normal and fault conditions, including use error and software.	
5	Each risk estimated and evaluated against the criteria.	
6	Controls chosen in the priority order the standard sets.	
7	Each control verified as implemented and as effective.	
8	Residual risks disclosed, including in the information for safety.	
9	Overall residual risk and benefit-risk conclusion documented.	
10	Risk management review completed before commercial release.	
11	Post-market information sources defined and reviewed on a schedule.	
12	Risk file updated when new hazards or changed estimates appear.	

Implementation Roadmap

1. Policy	Set the risk policy and acceptability criteria at management level.
2. Plan	Write a plan per device or family, naming the people and the reviews.
3. Analyze and control	Work through hazards, estimates, controls and verification, traceably.
4. Decide	Evaluate overall residual risk and benefit, and review before release.
5. Watch	Connect complaints, service, and literature back into the file.

How It Fits With Other Requirements

ISO 13485 requires risk-based decisions throughout the system; ISO 14971 supplies the device-level method. IEC 60601-1, IEC 62304, and IEC 62366-1 each call on its process. Under the EU MDR, Annex I's general requirements 1 to 9 are, in practice, met through it.

Findings We See Most Often

- Hazard lists that stop at design and ignore use error and post-market data.
- Severity and probability scales with no defined meaning.
- Benefit-risk asserted in one sentence rather than reasoned.
- Post-market reviews that never change a single estimate.

Where Systems Fall Short

- A risk file written for submission and not updated since launch.
- Risk controls listed but never verified as implemented and effective.
- Labeling used as the first control rather than the last.

How QES helps. Risk management files rebuilt so each control traces to its verification, and post-market feedback wired back into them. See the PMS plan build: qesisbest.com/services.html#pms-build · +1 (401) 246-3204 · mweeden@qesisbest.com

Sources, checked October 24, 2026. ISO — ISO 14971:2019 — www.iso.org/standard/72704.html; Johner Institute — ISO/TS 24971-2:2026 — blog.johner-institute.com/regulatory-affairs/iso-ts-24971-22026-risk-management-for-ml-based-medical-devices; iTeh — EN ISO 14971:2019/A11:2021 — standards.iteh.ai/catalog/standards/cen/b435080b-ca83-4c7a-804b-055ea4ca3c82/en-iso-14971-2019-a11-2021.

A summary for orientation, prepared by Quality Excellence Services. It does not reproduce or replace the standard or regulation: read the official text, which governs. Not legal advice.