ENGINEERING FIELD GUIDE

Developing and Manufacturing Medical Devices

A practical guide for risk managers

From risk-management policy and hazard analysis to effective controls, residual-risk evaluation and lifecycle learning

General cross-market guidance | Edition 1.0 | August 2026

Table of Contents

How to use this guide

This guide explains how medical-device risk managers establish, operate and defend a lifecycle risk-management process. It is aimed at risk-management leads, facilitators and engineers who coordinate product, usability, biological, software, cybersecurity, manufacturing and post-market risk evidence. It follows the logic of ISO 14971 while placing the work in the wider quality-management, regulatory and product-development context.

CORE MESSAGE Risk management is not the production of an FMEA. It is a controlled lifecycle process that connects intended use, reasonably foreseeable misuse, hazards, sequences of events, hazardous situations, harms, risk controls, verification evidence, benefit-risk conclusions and production or post-production information.

Scope and important limitations

- Apply the process to the complete medical device, including hardware, software, accessories, consumables, packaging, services, data flows and external dependencies where relevant.
- Use the manufacturer's approved risk-management policy, procedures, acceptability criteria and market-specific regulatory requirements.
- Confirm the applicable editions and jurisdictional status of standards and guidance before relying on them.
- Treat this guide as practical orientation; it does not replace competent legal, regulatory, clinical, toxicological, cybersecurity or statistical judgement.
- Scale methods and documentation to the device, novelty, uncertainty and potential harm, without omitting required lifecycle activities.

1. The role of risk management in medical-device development

Risk management provides the structured reasoning by which a manufacturer identifies what could cause harm, estimates and evaluates risk, implements controls, judges residual risk and learns from real-world information. It should influence intended use, requirements, architecture, design, verification, labelling, manufacturing controls and post-market activity.

What the risk manager is accountable for

Accountability	Practical outcome
Process integrity	A planned, competent, repeatable and controlled process that conforms to the applicable quality system.
Evidence integration	Technical, clinical, usability, biological, security and production evidence is brought into one coherent risk argument.
Decision transparency	Assumptions, criteria, uncertainties, disagreements and approvals are visible and traceable.
Lifecycle continuity	Development evidence is maintained through transfer, complaints, vigilance, change and obsolescence.
Escalation	Unacceptable risk, inadequate control evidence and emerging safety signals reach the correct decision-makers promptly.

Keep ownership with the manufacturer

Consultants, suppliers and specialist laboratories may contribute analyses, but the legal manufacturer retains responsibility for the process and its conclusions. The risk manager coordinates the evidence and governance; technical owners remain responsible for the accuracy of specialist inputs and management retains responsibility for policy and overall residual-risk decisions.

2. Regulatory and standards foundations

ISO 14971:2019 specifies terminology, principles and a process for medical-device risk management across the lifecycle, including software as a medical device and IVDs. ISO/TR 24971:2020 provides non-mandatory application guidance. ISO 13485:2016 embeds risk-based thinking throughout the quality system. In the United States, the FDA Quality Management System Regulation became effective on 2 February 2026 and incorporates ISO 13485:2016 by reference, together with additional US requirements.

Understand the European regulatory emphasis

- The EU MDR and IVDR require a documented, iterative risk-management system throughout the device lifecycle.
- Risks must be reduced as far as possible without adversely affecting the benefit-risk ratio, following the prescribed hierarchy of control options.

- Residual risks and undesirable side-effects must be acceptable when weighed against evaluated benefits and must be communicated where relevant.
- Risk management must remain consistent with clinical or performance evaluation, usability, post-market surveillance and technical documentation.
- Harmonised standards can support presumption of conformity only within their scope and cited regulatory status.

Avoid standards-only compliance thinking

Conformity to ISO 14971 is important but does not by itself establish compliance with every market requirement. Create an applicability assessment covering legislation, common specifications, product-family standards, recognised consensus standards, guidance and the manufacturer's own policy. Record differences in terminology and risk-control expectations.

3. Risk-management policy, governance and independence

Top management should define and document a policy for establishing criteria for risk acceptability. The policy should reflect applicable regulations, recognised state of the art and stakeholder concerns, and should provide a consistent basis for decisions across projects.

Establish governance that can withstand programme pressure

- Assign a risk-management process owner, project risk manager, technical contributors, reviewers and approval authorities.
- Define competence requirements and ensure appropriate clinical, usability, biological, software, security, manufacturing and regulatory expertise.
- Specify when unresolved disagreements, novel hazards or unacceptable residual risks require escalation.
- Separate facilitation from unilateral technical decision-making: the risk manager should challenge evidence without inventing specialist conclusions.
- Retain records of decisions, dissent, assumptions and management approvals.

Translate policy into usable criteria

A colour matrix is not a policy. Define how probability and severity categories are interpreted, how detectability is treated, which risks require controls, whether any region of risk is unacceptable, and how the criteria apply before and after controls. Avoid allowing arithmetic scores to conceal catastrophic severity, uncertainty or weak evidence.

4. Intended use, reasonably foreseeable misuse and product boundary

Risk analysis begins with a clear understanding of the device and its context. The intended use should identify the medical purpose, indications, patient or specimen population, intended users, use environment, operating principle and significant limitations. Foreseeable misuse must be considered without redefining deliberate abuse as normal use.

Define the complete risk-management scope

- Identify all device configurations, accessories, consumables, medicinal products, reagents and compatible third-party equipment.
- Include installation, transport, storage, commissioning, use, cleaning, reprocessing, calibration, service, update and disposal as applicable.
- Include embedded software, mobile applications, cloud services, networks, data stores and remote support dependencies.
- Consider patients, users, service staff, carers, bystanders, laboratory personnel and the environment where harm is credible.
- Document exclusions and justify why they cannot affect safety, performance or benefit-risk conclusions.

5. Risk-management planning

The risk-management plan defines how the process will be applied to a specific device or family. It should be approved early, maintained as the project changes and sufficiently concrete to guide actual work rather than repeat the procedure.

Essential contents of the plan

- Scope, product description, lifecycle phases, intended markets and applicable standards or regulations.
- Responsibilities, authorities, required competence, review arrangements and escalation routes.
- Risk acceptability criteria derived from the approved policy, including overall residual-risk evaluation.
- Methods for risk analysis, verification of control implementation and effectiveness, and collection of production or post-production information.
- Interfaces with requirements, usability, clinical or performance evaluation, biological evaluation, cybersecurity, suppliers and manufacturing.

- Planned reviews, deliverables, configuration control, change management and risk-management report approval.

Set review gates

Gate	Risk-management readiness question
Concept	Are intended use, principal hazards, novelty and major uncertainties understood well enough to proceed?
Design inputs	Are safety-related needs and risk-control requirements explicit, approved and verifiable?
Architecture	Have safety mechanisms, independence assumptions, interfaces and common-cause vulnerabilities been analysed?
Verification	Are controls implemented and are effectiveness protocols approved against traceable requirements?
Release	Are residual risks, overall benefit-risk, production controls and post-market plans acceptable and approved?
Change	Has the impact on hazards, controls, evidence and real-world risk been assessed before implementation?

6. Hazard identification and hazardous characteristics

Hazard identification should be systematic and multidisciplinary. Begin with energy, biological, chemical, informational, functional, environmental and use-related sources of harm rather than starting only from component failures. Product-family standards, analogous devices, complaints, literature and expert experience provide important prompts but do not replace product-specific reasoning.

Use multiple complementary perspectives

Perspective	Examples of questions
Energy and substances	What electrical, mechanical, thermal, radiation, biological or chemical energy can reach people or the environment?
Function and performance	What happens if a medical function is absent, delayed, excessive, inaccurate, intermittent or misleading?
Information and data	Could loss, corruption, delay, misassociation, disclosure or incorrect interpretation lead to harm?

Perspective	Examples of questions
Use and workflow	How can perception, cognition, workload, training, environment or foreseeable misuse create a hazardous situation?
Lifecycle and production	How can ageing, transport, maintenance, contamination, variation or obsolescence alter risk?
Security	How could a threat exploit a vulnerability and ultimately create a safety, privacy or operational harm?

Record uncertainty explicitly

Absence of known harm is not evidence that no hazard exists. Record knowledge gaps, assumptions, immature technology, limited field history and populations for which evidence is weak. Use these uncertainties to drive design exploration, verification, clinical work, supplier controls and post-market monitoring.

7. Sequences of events, hazardous situations and harms

A robust analysis distinguishes the hazard from the sequence of events, hazardous situation and resulting harm. A failure mode is neither automatically a hazard nor a harm. This distinction prevents vague rows and supports meaningful probability estimation and control selection.

Build a causal chain

1. **Identify the hazard.** State the potential source of harm, such as energy, substance, biological agent or incorrect information.
2. **Describe initiating events.** Include faults, normal-use conditions, foreseeable misuse, environmental exposure and external-system behaviour.
3. **Develop the sequence.** Explain how events and failed barriers could place a person or the environment in a hazardous situation.
4. **State the hazardous situation.** Describe the circumstance in which exposure to the hazard exists.
5. **Identify credible harms.** State clinically or otherwise meaningful injuries or damage, using an appropriate level of specificity.
6. **Link controls and evidence.** Show which part of the sequence each control addresses and how effectiveness will be demonstrated.

Avoid over-compressed risk rows

Rows such as “software error causes injury” are not analysable. They conceal the affected function, initiating cause, exposure pathway, clinical context, barriers and harm. Split materially different sequences when their controls, probability assumptions or harms differ.

8. Risk estimation and evaluation

Risk estimation considers the probability of occurrence of harm and the severity of that harm. Where quantitative data are unavailable, qualitative estimates may be appropriate, but they must remain transparent, consistent and supported by the best available evidence.

Separate the probability elements where useful

- Consider the probability that the relevant sequence of events occurs and the probability that exposure leads to a particular harm.
- Use field data, reliability evidence, clinical literature, usability results, production data and justified engineering estimates.
- Do not treat lack of complaints, short exposure time or no observed failures in a small sample as proof of remote probability.
- Use ranges or qualitative uncertainty when a single precise number would create false confidence.
- Estimate each relevant harm severity and probability rather than averaging dissimilar outcomes.

Evaluate against approved criteria

Risk evaluation determines whether risk reduction is required according to the plan and policy. Apply the criteria consistently and do not lower severity because a control is expected to work. Initial risk describes the uncontrolled or existing design state defined by the procedure; residual risk is reassessed after implemented controls and supporting evidence.

9. Selecting risk-control measures

Risk controls should follow the required hierarchy: inherent safety by design, protective measures in the device or manufacturing process, and information for safety. Information

and training are generally less reliable than eliminating the hazard or preventing exposure.

Choose controls that address the causal chain

Control option	Examples	Risk-manager challenge
Inherent safety by design	Eliminate hazardous energy, constrain output, simplify workflow, remove unsafe states.	Has the hazard or exposure been eliminated or materially reduced at its source?
Protective measures	Guards, interlocks, monitoring, alarms, redundancy, safe states, process controls.	Is the measure sufficiently independent, timely and robust under fault conditions?
Information for safety	Warnings, contraindications, instructions, training, residual-risk disclosure.	Can the intended user perceive, understand and act correctly in the real use environment?

Assess risks introduced by controls

- Analyse new hazards, use errors, failure modes and cybersecurity exposures introduced by the control.
- Assess shared dependencies and common-cause failures between primary functions and protective mechanisms.
- Check that a control does not transfer unacceptable risk to another person, lifecycle phase or product configuration.
- Update requirements, architecture, labelling, manufacturing controls and verification plans.
- Repeat risk estimation after implementation using evidence rather than intention alone.

10. Risk-control requirements and design traceability

Every selected control should be translated into one or more controlled, verifiable requirements allocated to the appropriate system, subsystem, manufacturing process, labelling or post-market activity. A risk-control statement in a spreadsheet is not a substitute for a design input.

Create bidirectional traceability

- Link hazards, sequences, hazardous situations and harms to the selected control and its rationale.
- Link each control to approved requirements and design outputs that implement it.
- Link requirements to verification protocols, execution records, results and anomalies.
- Link residual-risk conclusions to verified control effectiveness and current product configuration.
- Ensure changes can be traced back from affected components and requirements to the relevant risk analysis.

Distinguish process controls from product controls

A safe development process reduces the likelihood of defects but does not automatically control every product-specific risk. When process activities are claimed as controls, define the controlled failure mechanism, required outputs, objective evidence and any complementary product measures.

11. Verification of implementation and effectiveness

ISO 14971 requires verification that risk-control measures have been implemented and that they are effective. These are distinct questions. Inspection of a design output may confirm presence; effectiveness usually requires objective evidence under the relevant operating, fault or use conditions.

Demand evidence proportionate to the claim

Evidence question	Example
Was the control implemented?	Approved schematic, software build, drawing, label or manufacturing instruction contains the specified measure.
Does it function as specified?	Verification demonstrates detection threshold, response time, safe-state behaviour or physical strength.
Does it reduce the identified risk?	Testing challenges the relevant sequence of events and shows exposure or probability is reduced as intended.
Does the user-mediated control work?	Usability evidence demonstrates that intended users perceive, understand and act correctly.

Evidence question	Example
Does it remain effective over life?	Environmental, ageing, maintenance, cybersecurity and production evidence supports continued effectiveness.

Manage failed or incomplete evidence

A failed verification result cannot be converted into an acceptable control by narrative. Preserve the result, investigate cause and scope, reassess affected risks, correct the design or requirement where justified, and execute approved retesting. Record any limitations, deviations and remaining uncertainty in the risk file and release decision.

12. Overall residual-risk evaluation and benefit-risk analysis

After individual risks have been controlled and evaluated, the manufacturer must evaluate the overall residual risk posed by the device, taking account of the contributions and interactions of all residual risks. It is not sufficient to count green rows or sum arbitrary risk-priority numbers.

Perform an evidence-based overall evaluation

- Consider the nature, severity and distribution of residual harms, including rare catastrophic outcomes and cumulative exposure.
- Consider interactions, common causes, user burden, uncertainty, vulnerable populations and risks that cannot be meaningfully aggregated.
- Use current clinical or performance evidence to define the expected benefits for the intended population and indication.
- Compare benefits and residual risks in the actual context of use, including available alternatives and recognised state of the art.
- Document the rationale, expert contributions, unresolved uncertainty and approval authority.

Use benefit-risk analysis correctly

Benefit-risk analysis is not a mechanism for avoiding feasible risk reduction. First apply the hierarchy of control and reduce risk as required. Where a residual risk remains unacceptable according to the criteria, continuation requires a documented determination that medical benefits outweigh that residual risk, supported by appropriate evidence and market requirements.

13. Information for safety and disclosure of residual risk

Information for safety may be a legitimate risk-control measure, but it must be specific, actionable and designed for the intended user. It should not be used to compensate for avoidable design weaknesses. Relevant residual risks, contraindications, warnings, precautions and limitations must remain consistent across the risk file, labelling, training and clinical documentation.

Evaluate information as a real control

- Identify the intended recipient, point in the workflow, required decision and consequence of misunderstanding.
- Use terminology, prominence, symbols and placement appropriate to user capability and environment.
- Verify comprehension and correct action through usability engineering where use error could lead to harm.
- Ensure translations preserve risk meaning and are controlled across regional variants.
- Monitor complaints and use data for evidence that the information remains effective.

14. Usability-related risk management

Use-related risk is integrated into product risk management and supported by the usability engineering process. The risk manager should ensure that user-interface characteristics, critical tasks, foreseeable use errors and risk controls remain traceable to formative and summative evidence.

Connect use scenarios to the risk file

- Identify user groups, environments, workflows, physical or cognitive capabilities and reasonably foreseeable misuse.
- Describe use-related sequences without assigning blame to the user.
- Identify critical tasks and user-interface elements whose failure or misuse could lead to serious harm.
- Use formative evaluation to improve controls before design freeze and validation.
- Reconcile residual use-related risks, training, labelling and summative findings with the overall residual-risk evaluation.

15. Software, data and cybersecurity risk

Software risk analysis should address hazardous behaviour of the medical device, not only software defects. Cybersecurity risk management uses additional threat, vulnerability and exploitability concepts, but cybersecurity findings must connect to patient safety, privacy, availability and operational harms where relevant.

Integrate without collapsing distinct processes

Discipline	Primary focus	Required connection
Product safety risk	Hazards, hazardous situations and harms throughout the device lifecycle.	Software and security causes feed product risk and control requirements.
Software problem analysis	Faults, architecture, failure propagation, SOUP and lifecycle controls.	Safety classification and verification depth reflect possible contribution to hazardous situations.
Cybersecurity risk	Assets, threats, vulnerabilities, attack paths, exploitability and security controls.	Security compromise is translated into safety, privacy or operational consequences and post-market action.

Account for connected-system dependencies

- Identify cloud, mobile, network, identity, update, time, certificate and external-data dependencies.
- Analyse degraded connectivity, stale or misassociated data, service outage, partial update and rollback conditions.
- Define secure updateability, vulnerability monitoring, coordinated disclosure and timely remediation.
- Verify security controls and safety-relevant behaviour under credible attack or failure conditions.
- Maintain traceability between threat models, security requirements, product risks and residual-risk communication.

16. Biological, chemical and infection risks

Biological evaluation is a risk-management activity based on the finished device, nature and duration of contact, materials, manufacturing residues, degradation, sterilisation and

available evidence. A list of material certificates or a small set of tests is not automatically a complete biological evaluation.

Coordinate specialist evidence

- Define patient-contacting materials, indirect contact, contact duration, populations and cumulative exposure.
- Assess chemical characterisation, toxicological risk, biocompatibility endpoints and gaps in supplier information.
- Consider manufacturing residues, cleaning agents, packaging, ageing, degradation and repeated processing.
- Address sterility, microbial contamination, infection pathways and reprocessing where applicable.
- Ensure specialist conclusions and residual uncertainties feed the product risk file and change process.

17. Manufacturing, supplier and process risks

Risk controls frequently depend on material specifications, suppliers, validated processes, inspection, calibration, cleanliness and production tests. The risk manager should ensure that design risk conclusions remain valid after transfer to routine manufacture.

Connect the risk file to production controls

- Identify critical characteristics and process parameters derived from risk-control requirements.
- Determine where process validation is required because subsequent verification cannot fully confirm the result.
- Assess supplier capability, change notification, counterfeit or obsolescence risk and incoming-control strategy.
- Link production nonconformities, concessions and deviations to product-risk impact assessments.
- Use process capability, yield, complaint and service data to challenge probability assumptions and control effectiveness.

Control outsourced evidence and activities

Supplier certificates and external reports must identify the relevant item, configuration, method, acceptance criteria and limitations. Define responsibilities contractually, qualify

the provider and retain enough evidence to support the manufacturer's conclusion. Outsourcing does not outsource accountability.

18. Clinical, performance and state-of-the-art evidence

Clinical or performance evaluation defines the benefits, clinical performance, undesirable side-effects, alternatives and state of the art that support benefit-risk conclusions. Risk management should neither duplicate these processes nor use unsupported clinical assertions.

Maintain consistency across evidence sets

- Align intended purpose, indications, contraindications, target populations and claimed benefits.
- Use literature, clinical investigations, performance studies and post-market data to inform severity and probability.
- Compare residual risks with available alternatives and accepted clinical practice.
- Resolve contradictions between the risk file, clinical evaluation, labelling, usability conclusions and post-market plans.
- Update benefit-risk conclusions when evidence, practice or competitor technology changes materially.

19. The risk-management file and configuration control

The risk-management file is the organised set of records and references that demonstrates conformity with the planned process. It may be distributed across controlled systems, but the relationships and current approved state must be readily retrievable.

Maintain a coherent evidence structure

File element	Expected content
Policy and procedure	Management-approved acceptability approach, lifecycle process and governance.
Risk-management plan	Device-specific scope, criteria, methods, responsibilities, reviews and production-information plan.
Risk analyses	Hazards, sequences, hazardous situations, harms, estimates, controls and residual-risk evaluations.

File element	Expected content
Supporting analyses	Usability, software, cybersecurity, biological, manufacturing, clinical and specialist evidence.
Traceability and verification	Approved requirements, implementation evidence, effectiveness evidence and anomalies.
Risk-management report	Completion review, overall residual-risk conclusion and confirmation of production-information arrangements.
Lifecycle updates	Complaints, vigilance, CAPA, change assessments, trend reviews and revised conclusions.

Control baselines and assumptions

Identify the product version, requirements, software, accessories, manufacturing state and labelling to which each analysis applies. Record assumptions and pending evidence. When the design changes, assess whether hazards, sequences, estimates, controls, verification or benefit-risk conclusions are affected.

20. Risk-management review and report

Before commercial release, the risk-management process should be reviewed to confirm that the plan has been appropriately implemented, the overall residual risk is acceptable, suitable methods exist to collect and review production and post-production information, and required approvals are complete.

Run a formal closure review

1. **Confirm planned activities.** Check that required analyses, reviews, specialist evaluations and lifecycle interfaces are complete.
2. **Confirm risk controls.** Verify implementation and effectiveness evidence for each selected control.
3. **Review residual risk.** Assess individual risks, interactions, uncertainty and the overall residual-risk conclusion.
4. **Reconcile evidence.** Confirm consistency with clinical, usability, biological, software, security, labelling and manufacturing records.
5. **Review open issues.** Evaluate deviations, anomalies, concessions and deferred actions for risk and release impact.

6. **Approve lifecycle arrangements.** Confirm production and post-production monitoring responsibilities, triggers and escalation.

Write a decision document, not a summary of activity

The report should identify the approved plan and product configuration, state whether the plan was implemented, explain the overall residual-risk judgement, record unresolved limitations and confirm arrangements for lifecycle information. Approval should include the competence and authority appropriate to the device and conclusion.

21. Production and post-production information

Risk management continues after release. The manufacturer should establish a system to collect and review information about the device and similar devices during production and post-production, determine whether new hazards or changed risks exist, and feed conclusions into appropriate action.

Define meaningful information sources and triggers

- Complaints, service records, returns, nonconformities, CAPA, production trends and supplier notifications.
- Vigilance reports, recalls, field safety corrective actions and regulatory communications.
- Post-market surveillance, post-market clinical or performance follow-up, registries and literature.
- Cybersecurity vulnerabilities, threat intelligence, penetration findings and third-party component notices.
- Comparable-device incidents, changes in clinical practice, new standards and changes in recognised state of the art.

Close the feedback loop

Predetermine review frequency, signal thresholds, responsibilities and escalation. Assess whether probability or severity estimates have changed, controls remain effective, overall residual risk remains acceptable and corrective or preventive action is required. Update the risk file, technical documentation, labelling and post-market plans as necessary.

22. Change control, regression and evidence reuse

Every change should be assessed for its possible effect on hazards, sequences, users, interfaces, risk controls, production processes, verification evidence and post-market

commitments. The absence of a changed risk-table row does not prove that risk is unaffected.

Perform a structured impact assessment

- Identify the changed product, software, material, supplier, process, labelling, intended use or external dependency.
- Trace affected requirements and interfaces to relevant hazardous situations and controls.
- Assess new hazards, control degradation, common-cause effects and changed probability or severity.
- Determine required analysis, regression verification, validation, clinical or biological evidence.
- Approve updated residual-risk and benefit-risk conclusions before implementation.

Reuse evidence only with a documented bridge

Previous evidence can remain valid when the configuration, method, conditions, assumptions and acceptance criteria remain applicable. Document the equivalence assessment and any bridging work. Platform similarity, supplier assurances or unchanged part numbers are not sufficient by themselves.

23. Facilitating effective multidisciplinary risk reviews

A strong workshop converts specialist knowledge into explicit causal reasoning and decisions. It should not become a meeting where participants silently score a pre-written spreadsheet. The facilitator should prepare the scope, evidence and prompts, then preserve ownership of conclusions with the appropriate experts.

Run productive reviews

- Circulate the intended use, architecture, workflow, previous analyses, incidents and open evidence before the meeting.
- Use diagrams, use scenarios and causal chains to explore exposure rather than reading columns aloud.
- Separate hazard identification from scoring so low estimates do not prematurely suppress discussion.
- Record the rationale, owner and due date for assumptions, actions and unresolved disagreements.

- Time-box broad workshops and arrange focused follow-ups with the specialists needed for difficult topics.

Ask questions that expose weak reasoning

- What person is exposed to what hazard, in which circumstance, and what harm can result?
- Which barriers must fail, and are they independent or dependent on the same component, data or user action?
- What evidence supports the probability estimate and how uncertain is it?
- Where is the control implemented, and what evidence demonstrates both presence and effectiveness?
- What new risk does the control introduce, and does it remain effective over the intended lifetime?
- Would the conclusion still be credible to an independent clinical, technical or regulatory reviewer?

24. Metrics, audits and recurring failure modes

Metrics should reveal risk-management quality and decision readiness, not reward the number of completed spreadsheet rows. Useful indicators focus on control evidence, ageing uncertainty, cross-functional consistency, emerging signals and closure of safety-critical actions.

Monitor indicators that support decisions

- Percentage of risk controls with approved requirements and both implementation and effectiveness evidence.
- Age and criticality of open assumptions, missing specialist inputs, failed tests and unresolved anomalies.
- Consistency of intended use, harms, residual risks and controls across technical documentation.
- Timeliness of complaint, vigilance, cybersecurity and production-signal review.
- Change assessments completed before implementation and overdue risk-file updates.

Recognise common failures and corrective direction

Failure pattern	Corrective direction
The FMEA is treated as the complete risk process.	Add intended-use, hazard-based, use-related, system, benefit-risk and lifecycle analyses as appropriate.
Risk scores are precise but unsupported.	Document evidence, uncertainty, probability logic and expert rationale.
Controls exist only in the risk spreadsheet.	Create approved requirements and trace them to design outputs and verification evidence.
Warnings replace feasible design controls.	Reapply the hierarchy of control and justify residual information-for-safety measures.
Verification confirms presence only.	Demonstrate effectiveness against the relevant sequence, fault and use condition.
Overall residual risk equals a count of green rows.	Perform a documented holistic evaluation using benefits, interactions and uncertainty.
The file is frozen at release.	Operate production and post-production feedback, signal review and change control.

PRACTICAL RULE A defensible risk conclusion states what can cause harm, how exposure occurs, which evidence supports the estimate, where the control is implemented, whether it is effective and why the residual risk is acceptable for the released device.

Appendix A. Risk-management deliverables by development phase

Development phase	Representative deliverables
Concept	Intended-use draft, product boundary, preliminary hazards, regulatory assumptions and major uncertainties.
Design inputs	Approved plan, acceptability criteria, initial analyses and risk-control requirements.
Architecture and design	Updated system, usability, software, security, biological and manufacturing analyses.

Development phase	Representative deliverables
Verification and validation	Control implementation and effectiveness evidence, anomalies and updated residual-risk evaluations.
Transfer and release	Production controls, overall residual-risk evaluation, report and post-market information plan.
Post-market	Signal reviews, complaints, vigilance, CAPA, trend analysis and risk-file updates.
Change	Impact assessment, revised analyses, regression evidence and updated benefit-risk conclusion.

Appendix B. Essential risk-management review checklist

Review area	Minimum question
Scope	Does the file cover the complete device, intended use, lifecycle and relevant people?
Policy and plan	Are criteria, responsibilities, methods and reviews approved and project-specific?
Hazards	Were hazards identified systematically using product, use, lifecycle and field evidence?
Causal reasoning	Are sequences, hazardous situations and harms clear enough to support controls?
Estimation	Are probability, severity and uncertainty supported and consistently evaluated?
Controls	Was the hierarchy applied and were control-introduced risks assessed?
Requirements	Are controls translated into approved, verifiable design or process requirements?
Evidence	Do records establish both implementation and effectiveness for the released configuration?
Residual risk	Are individual and overall residual risks acceptable in relation to demonstrated benefits?

Review area	Minimum question
Lifecycle	Are production, post-market and change feedback arrangements active and effective?

Appendix C. Commonly relevant standards and frameworks

This table is a starting point. Confirm applicability, current editions, amendments, recognised or harmonised status and product-specific requirements.

Topic	Common reference	Risk-management relevance
Core risk management	ISO 14971:2019; ISO/TR 24971:2020	Lifecycle process, terminology, controls, evaluation and production information.
Quality management	ISO 13485:2016; US 21 CFR Part 820 QMSR	Governance, design and development, suppliers, production, CAPA and records.
EU legislation	Regulation (EU) 2017/745; Regulation (EU) 2017/746	Iterative risk management, GSPRs, control hierarchy and benefit-risk.
Usability	IEC 62366-1, applicable edition	Use-related hazards, critical tasks, user-interface controls and validation.
Software lifecycle	IEC 62304, applicable edition	Software safety classification, lifecycle controls and verification.
Health-software security	IEC 81001-5-1; FDA cybersecurity guidance	Security risk, vulnerability management and safe updateability.
Medical electrical equipment	IEC 60601 series, where applicable	Basic safety, essential performance and product-specific hazards.
Biological evaluation	ISO 10993-1:2025 and applicable parts	Biological evaluation within a risk-management process.
Manufacturer information	ISO 20417:2026; ISO 15223-1, as applicable	Residual-risk communication, safety information and symbols.
Post-market surveillance	MDR/IVDR; MDCG 2025-10	Lifecycle information, signals, trends and feedback to risk management.

Appendix D. Glossary

Term	Meaning in this guide
Benefit	Positive impact or desirable outcome of use of the medical device on health or patient management.
Harm	Injury or damage to the health of people, or damage to property or the environment.
Hazard	Potential source of harm.
Hazardous situation	Circumstance in which people, property or the environment are exposed to one or more hazards.
Intended use	Use for which a product, process or service is intended according to the manufacturer's specifications and information.
Overall residual risk	Combined residual risk associated with the device after all controls have been implemented.
Reasonably foreseeable misuse	Use not intended by the manufacturer but resulting from readily predictable human behaviour.
Residual risk	Risk remaining after risk-control measures have been implemented.
Risk	Combination of the probability of occurrence of harm and the severity of that harm.
Risk analysis	Systematic use of available information to identify hazards and estimate risk.
Risk control	Process in which decisions are made and measures implemented to reduce risks to, or maintain risks within, specified levels.
Risk estimation	Process used to assign values to probability and severity.
Risk evaluation	Comparison of estimated risk against given acceptability criteria.
Risk-management file	Set of records and documents produced by risk management and the references connecting them.
Risk-management plan	Device-specific description of scope, responsibilities, criteria, activities, reviews and lifecycle information.
Risk-management report	Review record confirming implementation of the plan, overall residual-risk acceptability and lifecycle arrangements.
Safety	Freedom from unacceptable risk.

Term	Meaning in this guide
Severity	Measure of the possible consequences of a hazard.
State of the art	Developed stage of technical capability at a given time regarding products, processes and services, based on relevant consolidated findings.

Appendix E. Authoritative starting sources

- ISO — ISO 14971:2019, Application of risk management to medical devices
- ISO — ISO/TR 24971:2020, Guidance on the application of ISO 14971
- ISO — ISO 13485:2016, Medical devices quality management systems
- ISO — ISO 10993-1:2025, Biological evaluation of medical devices
- ISO — ISO 20417:2026, Information supplied by the manufacturer
- FDA — Quality Management System Regulation
- FDA — Cybersecurity in Medical Devices: Quality Management System Considerations
- FDA — Applying Human Factors and Usability Engineering to Medical Devices
- European Union — Regulation (EU) 2017/745 on medical devices
- European Union — Regulation (EU) 2017/746 on in vitro diagnostic devices
- European Commission — MDCG endorsed documents and other guidance
- European Commission — MDCG 2025-10, Post-market surveillance guidance
- European Commission — Harmonised standards for medical devices

CONTROLLED USE Consult current controlled editions of applicable legislation, standards and regulatory guidance. Risk-management conclusions depend on the actual device, intended use, evidence, market, recognised state of the art and approved quality-management-system processes.