QUALITY ASSURANCE FIELD GUIDE

Developing and Manufacturing Medical Devices

A practical guide for QA managers and engineers

From quality-system governance and design assurance to controlled manufacture, objective evidence and lifecycle improvement

General cross-market guidance | Edition 1.0 | August 2026

Table of Contents

How to use this guide

This guide explains how quality-assurance managers and engineers establish, operate and improve the controls needed to develop, manufacture, distribute and maintain medical devices. It covers the quality-management system, design assurance, risk management, supplier quality, production, verification and validation, document control, nonconformities, corrective action, audits, complaints and post-market feedback. It applies to physical devices, connected products, medical software and in vitro diagnostic devices where the relevant obligations apply.

CORE MESSAGE Quality assurance is the disciplined creation and maintenance of confidence that the manufacturer's processes, products, evidence and decisions consistently meet applicable requirements throughout the medical-device lifecycle.

Scope and important limitations

- Begin with the legal manufacturer, intended purpose, device classification, target markets, approved quality-system scope and applicable regulatory obligations.
- Apply ISO 13485, ISO 14971, the FDA Quality Management System Regulation, EU MDR or IVDR and product-specific standards only where they are relevant.
- Distinguish process ownership, independent quality oversight, technical approval and regulatory accountability.
- Use objective evidence, risk-based decisions, controlled records and timely escalation rather than retrospective reconstruction.
- Confirm current controlled editions, jurisdictional requirements, notified-body expectations and company procedures before relying on any reference.

1. The purpose of quality assurance in medical-device development

Quality assurance establishes confidence that the organisation follows suitable processes and that products meet safety, performance and regulatory requirements. It is broader than final inspection and cannot be delegated entirely to a quality department. Every function owns the quality of its work, while QA provides governance, independent challenge and visibility of systemic risk.

Separate assurance, control and ownership

Activity	Primary purpose	Typical example
Quality assurance	Establish and evaluate the processes that should produce compliant outcomes.	Review the design-control procedure, audit its use and assess evidence readiness.
Quality control	Inspect, measure or test an item against defined acceptance criteria.	Inspect incoming components or review final production-test results.
Process ownership	Operate and improve the process that creates the work or product.	Engineering owns design outputs; operations owns approved production processes.
Regulatory accountability	Retain responsibility for the device, market obligations and supporting evidence.	The legal manufacturer approves and maintains the technical documentation.

Define the quality organisation's contribution

- Maintain a coherent quality-management system aligned with device risk, markets and company operations.
- Challenge incomplete, inconsistent or unsupported evidence before it becomes a submission or release problem.
- Ensure appropriate approval, independence, competence, documentation and change control.
- Connect development, risk management, suppliers, production, complaints and corrective action.
- Escalate systemic weakness, patient-safety concern and unsupported release decisions to management.

2. Regulatory foundations and quality-system scope

ISO 13485:2016 defines internationally recognised medical-device quality-management-system requirements. 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. The EU MDR and IVDR impose further obligations covering risk management, technical documentation, post-market surveillance, vigilance and economic-operator responsibilities.

Determine the actual scope of obligations

- Identify the legal manufacturer, sites, outsourced activities, product families and intended markets.
- Determine whether the organisation designs, manufactures, distributes, services, sterilises or operates supporting software.
- Map relevant quality-system requirements to documented processes, owners, records and controls.
- Identify additional national, product-family, clinical, cybersecurity and data-protection obligations.
- Justify any exclusions or non-applicability without omitting required regulatory or safety activities.

Avoid false equivalence between certification and compliance

An ISO 13485 certificate is valuable evidence of quality-system maturity, but it does not automatically demonstrate compliance with every market requirement, product claim or design-control obligation. QA should maintain a clear mapping from applicable requirements to implemented processes and objective evidence.

3. Management responsibility and quality governance

Management is responsible for establishing a quality policy, assigning authorities, providing resources and ensuring that the quality-management system remains effective. QA managers should provide decision-ready information, challenge insufficient resourcing and ensure that quality responsibilities are not obscured by organisational boundaries.

Build clear accountability

- Identify the quality-system owner, process owners, designated management responsibilities and approval authorities.
- Define the relationship between QA, regulatory affairs, engineering, manufacturing, procurement, clinical and post-market functions.
- Provide escalation routes for product risk, audit findings, data-integrity concerns and unsupported release requests.
- Define appropriate independence for reviews, audits, disposition and release decisions.
- Retain evidence that management reviews quality performance, systemic problems, resources and improvement needs.

Use management review for decisions

Review input	Decision it should support
Audit and inspection results	Correct systemic weaknesses, allocate resources and address recurring nonconformities.
Complaints and post-market signals	Assess safety trends, reporting obligations and product or process changes.
Process and product performance	Improve capability, identify adverse trends and protect release quality.
CAPA status	Remove barriers to effective investigation, action completion and effectiveness checks.
Changes and resource needs	Maintain competence, infrastructure, supplier control and lifecycle support.
Regulatory and standards changes	Update procedures, training, evidence and market-specific compliance plans.

4. Quality-system architecture and process ownership

A useful quality-management system is an integrated set of processes, not a directory of procedures. Each process should have a defined purpose, owner, inputs, outputs, controls, interfaces, competence requirements and performance measures.

Identify the core process network

- Management responsibility, quality planning, document control, training and internal audit.
- Design and development, risk management, clinical or performance evaluation and regulatory documentation.
- Supplier management, purchasing, incoming control and outsourced-process oversight.
- Production, service, installation, process validation, equipment, calibration and release.
- Complaint handling, vigilance, post-market surveillance, nonconformity and CAPA.
- Change control, data integrity, cybersecurity, records retention and continuous improvement.

Control interfaces rather than duplicating work

A process map should show how evidence moves between functions. For example, risk controls become requirements, requirements drive verification, production controls preserve verified behaviour and complaints feed risk-file updates. QA should address missing interfaces and inconsistent ownership rather than creating parallel records solely for audit presentation.

5. Document control and record integrity

Controlled documents describe approved intentions; records show what actually happened. QA must ensure that relevant versions are available where needed, obsolete versions are prevented from unintended use and records remain legible, identifiable, retrievable and protected for the required retention period.

Apply effective document controls

- Define document ownership, review, approval, effective date, change history and distribution.
- Ensure current procedures, specifications, drawings and work instructions are accessible to users.
- Identify and control external standards, supplier documents and regulatory references.
- Preserve the relationship between records and the product, process, configuration or decision they support.
- Define retention, backup, access, recovery and protection from unauthorised alteration.

Protect data integrity

Records should be attributable, legible, contemporaneous, original or appropriately preserved, and accurate. Electronic systems should control access, audit trails, approval, version history and recovery according to risk. Backdating, undocumented edits, selective omission of failed results and retrospective recreation undermine both compliance and trust.

6. Competence, training and human performance

Training records are useful only when they support demonstrated competence. QA should help define what personnel must know and be able to do, including when specialist judgement or independent review is required.

Manage competence by role and risk

- Define role descriptions, required knowledge, qualifications and practical skills.
- Assign procedure training before personnel perform controlled activities.
- Assess effectiveness through observed performance, supervised work, testing or other suitable evidence.
- Maintain competence for auditors, risk facilitators, laboratory staff, production personnel and release authorities.
- Reassess needs after process changes, audit findings, complaints or emerging technology.

Distinguish awareness from qualification

Reading a procedure does not qualify someone to perform sterilisation validation, cybersecurity assessment, clinical interpretation or statistical sampling. QA should ensure that technical responsibilities are assigned to people with appropriate expertise and that outsourcing does not hide competence gaps.

7. Design and development planning

Design planning defines responsibilities, lifecycle activities, review points, verification, validation, risk management, transfer and document outputs. QA should enter the programme early enough to influence planning rather than arriving shortly before an audit or market submission.

Review the plan against the real project

- Confirm intended purpose, product boundary, target markets, development model and applicable standards.
- Identify owners, independent reviewers, suppliers, software partners and critical specialist contributors.
- Define deliverables, phase gates, traceability expectations and decision criteria.
- Integrate risk management, usability, cybersecurity, clinical evidence and manufacturing readiness.

- Plan configuration control, change management, sample representativeness and post-market transition.

Adapt without deleting essential controls

Agile, iterative and outsourced development remain compatible with design controls when baselines, approvals, traceability and evidence are built into the workflow. The plan should explain how the chosen operating model meets requirements, not assume that informal velocity compensates for missing records.

8. Design inputs, outputs and requirements quality

Design inputs define what the device must achieve. Design outputs define the implemented product. QA should verify that inputs are complete, unambiguous, approved and verifiable, and that outputs can be reviewed against those inputs.

Assess input readiness

- Confirm user needs, intended use, regulatory obligations, risk controls, interfaces and manufacturing requirements are represented.
- Challenge vague statements, missing units, undefined operating conditions and contradictory limits.
- Ensure every requirement has a source, identifier, owner, approval status and proposed verification method.
- Check that software, connectivity, usability, packaging, labelling, service and cybersecurity are included where applicable.
- Record assumptions, exclusions and open decisions that could affect evidence or release.

Assess output completeness

Outputs may include drawings, bills of materials, software builds, architecture, specifications, test methods, labels, manufacturing instructions and acceptance criteria. QA should ensure that outputs identify characteristics essential to safety and performance and are suitable for verification, transfer and controlled manufacture.

9. Design reviews, phase gates and independent challenge

Formal reviews assess design maturity, unresolved issues, risk and evidence readiness. They should include appropriate functions and at least one reviewer without direct responsibility for the stage being reviewed where required by the applicable process.

Conduct a meaningful design review

1. **Define the decision.** State the lifecycle stage, review scope, intended outcome and required participants.
2. **Prepare the evidence.** Provide the controlled baseline, requirements, risks, outputs, test status and open issues.
3. **Challenge completeness.** Assess technical suitability, regulatory alignment, risk controls and cross-functional dependencies.
4. **Record findings.** Capture decisions, disagreements, actions, owners, deadlines and constraints.
5. **Control conditional approval.** Specify which actions must close before the next activity or release.
6. **Verify closure.** Confirm objective evidence and appropriate authority before the review is considered complete.

Prevent ceremonial approval

A review should not merely confirm that a meeting occurred. If safety-critical requirements remain undefined, risk controls lack evidence or production representativeness is unknown, QA should ensure that the gate outcome reflects those deficiencies and that management understands the consequences.

10. Risk-management integration

ISO 14971 risk management should influence design, verification, usability, production and post-market activity. QA verifies that the approved risk process is actually implemented and that its conclusions are supported by consistent evidence.

Quality-assurance checks for the risk process

- Confirm that management has approved a policy and that the project has an appropriate risk-management plan.
- Check that hazards, sequences, hazardous situations, harms and reasonably foreseeable misuse have been considered.
- Ensure risk-control requirements appear in controlled design or manufacturing documentation.
- Verify evidence of both control implementation and control effectiveness.
- Review overall residual-risk and benefit-risk conclusions against clinical, usability and post-market evidence.

- Confirm that changes, complaints, supplier issues and production trends feed back into the risk file.

Distinguish a process failure from a product hazard

A missing signature is a quality-system nonconformity; whether it creates product risk depends on what was approved, whether the underlying decision was sound and whether safety or evidence may be compromised. QA should assess both dimensions without assuming every procedural defect has the same patient impact.

11. Verification, validation and evidence quality

Verification demonstrates that specified design inputs have been met. Validation demonstrates that the finished device meets user needs and intended use. QA should assess whether methods, samples, conditions, acceptance criteria and records support the actual claim being made.

Review plans, protocols and reports

- Ensure plans define scope, responsibilities, methods, product configurations, sample rationale and approvals.
- Confirm that protocols are approved before execution and contain objective acceptance criteria.
- Check calibration, laboratory competence, environmental conditions and representative samples.
- Review original data, failed results, deviations, investigations, retesting and conclusions.
- Maintain traceability from requirements and risk controls to executed evidence and release configuration.

Protect the distinction between evidence types

Evidence type	Question answered
Design verification	Does the approved design fulfil specified requirements?
Design validation	Does the finished product meet intended use and user needs?
Risk-control verification	Was the measure implemented, and does it effectively reduce the identified risk?

Evidence type	Question answered
Process validation	Can the process consistently produce an acceptable result when output verification is insufficient?
Clinical or performance evidence	Are the intended medical or diagnostic benefits and performance claims supported?

12. Traceability and design-history evidence

Traceability connects user needs, risks, requirements, outputs, verification, validation, changes and conclusions. The relevant design records may be distributed across systems, but QA should be able to reconstruct the approved evidence chain without inventing or retrospectively rewriting events.

Audit the evidence chain

- Identify the approved intended use, user needs and product requirements.
- Trace safety-related requirements back to hazards and selected controls.
- Trace requirements forward to design outputs, verification methods and results.
- Connect validation and clinical evidence to the intended users, environment and claims.
- Confirm product versions, approvals, change history and treatment of open anomalies.

Prefer live traceability to release reconstruction

Traceability should be maintained as work progresses. Creating it only for a submission often exposes missing decisions, inconsistent configurations and uncontrolled changes that cannot be repaired by adding links after the event.

13. Supplier qualification and purchasing controls

Supplier controls should reflect the effect of purchased products and services on device safety, performance, manufacturing and regulatory evidence. The manufacturer remains responsible for the suitability of outsourced design, testing, software, materials, sterilisation and production.

Establish a risk-based supplier lifecycle

- Classify suppliers by product impact, complexity, availability and ability to affect risk controls.
- Evaluate quality-system capability, competence, facilities, historical performance and relevant certifications.
- Define approved specifications, purchasing data, quality agreements and acceptance criteria.
- Require notification and assessment of material, process, location, software or subcontractor changes.
- Monitor performance, complaints, nonconformities, delivery, obsolescence and corrective action.

Challenge supplier evidence before accepting it

A certificate without an identified configuration, scope, method, result or limitation may not support the intended claim. QA should ensure that external reports remain traceable to the actual purchased item, approved process and device application.

14. Incoming inspection, acceptance and material control

Incoming controls confirm that purchased items and materials meet defined acceptance requirements before use. The inspection strategy should match supplier risk, history, critical characteristics and the ability of downstream processes to detect defects.

Define suitable acceptance controls

- Identify the item, supplier, revision, lot, expiry, storage conditions and acceptance criteria.
- Use justified inspection or sampling plans, calibrated equipment and competent inspectors.
- Define quarantine, release, rejection and segregation of suspect or nonconforming material.
- Control traceability of safety-critical parts, biological materials, reagents and software components as applicable.
- Reassess sampling and supplier status when complaints, process changes or adverse trends emerge.

Avoid inspection as a substitute for supplier capability

Final or incoming inspection cannot compensate indefinitely for an unstable supplier process. Persistent defects should trigger supplier investigation, improved controls, process changes or requalification rather than an ever-increasing inspection burden.

15. Production controls and manufacturing readiness

Production must operate from approved specifications, work instructions, trained personnel, suitable equipment and defined acceptance criteria. QA should confirm that the transferred design can be manufactured consistently and that product risk controls remain effective in routine production.

Review production readiness

- Confirm released drawings, bills of materials, software versions, specifications and work instructions.
- Identify critical characteristics, process parameters, environmental controls and in-process acceptance criteria.
- Verify equipment qualification, maintenance, calibration and operator competence.
- Assess production builds against the verified product configuration and approved design outputs.
- Define traceability, batch or serial records, nonconformity handling and release authority.

Connect process performance to product risk

A process can meet a nominal production target while drifting towards conditions that compromise a safety-critical characteristic. Monitor capability, yield, rework, defects and complaints in relation to product risk rather than treating production indicators only as cost metrics.

16. Process validation and revalidation

Process validation is required where the resulting output cannot be fully verified by subsequent inspection or testing, or where verification alone is insufficient to establish consistent conformity. Typical examples may include sterilisation, aseptic processing, sealing, welding, moulding, software-controlled production and cleaning, depending on the product.

Structure validation around evidence

Validation activity	Practical objective
Process definition	Identify intended output, critical parameters, equipment, materials, risks and acceptance criteria.
Installation qualification	Confirm equipment and supporting utilities are installed and configured as intended.
Operational qualification	Demonstrate operation across justified ranges and relevant challenge conditions.
Performance qualification	Show that the process performs consistently under representative routine conditions.
Continued monitoring	Maintain control using process data, maintenance, environmental information and trend review.
Revalidation	Reassess after relevant changes, adverse trends, equipment movement or loss of control.

Do not confuse a protocol with validated status

Validation requires approved planning, suitable studies, actual data, reviewed deviations and an approved conclusion. A drafted protocol or a supplier statement does not demonstrate that a process is validated for the manufacturer's actual product, equipment and operating window.

17. Equipment, calibration and measurement systems

Acceptance decisions are reliable only when the supporting measurements are suitable. QA should ensure that monitoring and measuring equipment is identified, maintained, calibrated and appropriate to the required accuracy, resolution and decision limits.

Control measurement capability

- Identify equipment, calibration status, intervals, measurement range and authorised use.
- Use traceable calibration where appropriate and assess measurement uncertainty near acceptance boundaries.
- Define controls for software tools, fixtures, reference materials, environmental conditions and operator influence.

- Investigate out-of-calibration findings and assess previously accepted product or evidence.
- Maintain suitable records for equipment qualification, maintenance and calibration review.

18. Nonconforming product, deviations and concessions

Nonconformity management prevents unintended use or release of product, material, evidence or processes that do not meet specified requirements. QA should ensure segregation, evaluation, disposition, investigation and any regulatory or safety escalation.

Manage disposition transparently

- Identify the nonconformity, affected product, configuration, quantity, location and potential distribution.
- Assess safety, performance, regulatory, traceability and customer impact.
- Define approved options such as rework, rejection, return, controlled concession or further investigation.
- Validate or verify rework where needed and retain the original nonconformity record.
- Escalate recurring issues, serious risk, supplier failure or systemic process weakness into CAPA.

Use concessions cautiously

A concession is not a mechanism to accept an unknown or unsafe condition. The technical, regulatory and risk rationale should be explicit, appropriately approved and limited to identified product. Repeated concessions for the same issue indicate that the underlying specification or process requires correction.

19. Corrective and preventive action

Corrective and preventive action addresses the causes of existing or potential nonconformities and prevents recurrence or occurrence. QA managers should ensure that action is proportionate to risk, that root-cause analysis is evidence-based and that effectiveness is checked after implementation.

Operate an effective CAPA lifecycle

1. **Define the problem.** State the observed issue, affected scope, evidence, risk and required containment.

2. **Investigate the cause.** Use suitable analysis to distinguish symptoms, immediate causes and systemic contributors.
3. **Plan the action.** Assign owners, deadlines, approvals and actions that address the verified cause.
4. **Implement under control.** Update designs, processes, suppliers, training or documents through the relevant change process.
5. **Verify implementation.** Confirm that the planned action was completed and documented.
6. **Evaluate effectiveness.** Check over an appropriate period that the issue does not recur and no unacceptable new risk was introduced.

Avoid procedural closure without improvement

Training everyone again is rarely a complete root-cause response. QA should challenge conclusions based solely on operator error, lack of awareness or isolated oversight where design, workload, process clarity, tooling or management decisions also contributed.

20. Complaint handling, vigilance and post-market surveillance

Complaints and post-market information provide real-world evidence of product performance and safety. QA should ensure that complaints are captured, evaluated, investigated and connected to reporting, CAPA and risk management as appropriate.

Create an integrated feedback process

- Capture product identity, event description, reporter, affected population, seriousness and available evidence.
- Assess whether the issue indicates a device deficiency, serious incident, reportable event or field action.
- Investigate product, software, use, supplier, manufacturing and distribution factors.
- Evaluate implications for residual risk, intended use, labelling, verification evidence and comparable devices.
- Use trends, literature, service records, cybersecurity intelligence and production data to detect emerging signals.

Respect market-specific reporting requirements

Reportability, timelines and recipient authorities vary between jurisdictions. QA should ensure the organisation has current procedures, competent decision-makers and

documented reasoning, and that commercial or reputational concerns do not delay required safety communication.

21. Internal audits and inspection readiness

Internal audits assess whether the quality-management system conforms to planned arrangements and is effectively implemented. Audit programmes should consider process importance, product risk, previous findings, changes and emerging regulatory expectations.

Plan audits that test reality

- Define scope, criteria, audit frequency, methods, auditor competence and appropriate independence.
- Use risk-based sampling across records, products, sites, suppliers and process interfaces.
- Follow a real product or decision through requirements, risks, design, evidence, production and complaints.
- Classify findings consistently and require actions proportionate to significance.
- Verify correction, root cause, CAPA and effectiveness rather than accepting document updates alone.

Prepare continuously for inspections

Inspection readiness is the ability to locate controlled evidence, explain the process and discuss known issues honestly. QA should maintain current process maps, ownership, key records and issue status rather than launching a temporary evidence-collection exercise immediately before an audit.

22. Change control and configuration management

Changes to design, software, suppliers, materials, processes, labelling, intended use, claims or quality-system procedures can affect product safety and evidence. QA should ensure that proposed changes receive proportionate impact assessment before implementation.

Assess the complete impact

- Identify the changed item, affected configurations, product versions, sites and markets.

- Assess requirements, risks, usability, cybersecurity, clinical evidence and regulatory approvals.
- Determine required verification, validation, process revalidation, supplier qualification and production controls.
- Update controlled documents, training, traceability and customer or authority communication where required.
- Approve implementation and confirm effectiveness before the change is considered complete.

Control evidence reuse

Previous evidence can remain valid when the tested configuration, conditions, assumptions and acceptance criteria still support the current claim. QA should require a documented comparison and bridging rationale rather than relying on unchanged part numbers or general platform similarity.

23. Software tools, electronic systems and computer software assurance

Electronic quality systems, manufacturing software, laboratory applications, spreadsheets and automated test tools can influence product acceptance and quality records. Their assurance should be proportionate to intended use and the risk that failure could affect safety, quality or data integrity.

Apply a risk-based tool assurance approach

- Identify intended use, users, workflows, interfaces and the decisions supported by the software.
- Assess the potential effect of incorrect calculation, unavailable data, unauthorised change or lost records.
- Define suitable configuration, access control, backup, audit-trail and supplier-management requirements.
- Use testing and assurance activities proportionate to the actual risk, including targeted unscripted testing where justified.
- Control changes, patches, periodic review, issue management and retirement.

Avoid excessive documentation without assurance

The purpose of software assurance is confidence in the intended use, not a large collection of pre-written scripts. Conversely, claiming a tool is low risk does not eliminate

the need to understand what it does, protect records and document a defensible assurance rationale.

24. Quality metrics, trend analysis and continuous improvement

Metrics help identify process weakness, product risk and resource constraints when they support meaningful decisions. QA managers should avoid measures that reward rapid closure, high audit scores or large document counts without demonstrating improved outcomes.

Select indicators that reveal real quality

Indicator	Useful management interpretation
Complaint rate and severity	Detect changes in field performance, usability and patient risk.
CAPA ageing and effectiveness	Identify blocked investigations and actions that do not prevent recurrence.
Audit finding recurrence	Reveal systemic weakness or ineffective management response.
Supplier performance	Show whether critical suppliers sustain capability, quality and change communication.
Production nonconformity and rework	Identify process drift, design weakness and release pressure.
Verification and risk-control coverage	Expose missing evidence, unresolved failures and critical release gaps.
Training effectiveness	Show whether competence gaps contribute to deviations or recurring issues.

Use trends to trigger action

Define thresholds, review frequency, ownership and escalation in advance. Compare data by product, supplier, site, process and severity. A rising trend may require action before an individual event crosses a reporting or rejection threshold.

25. Product release and quality decision-making

Release confirms that a defined product or batch meets approved requirements and that any unresolved issue has been properly evaluated. QA should understand the difference between production release, software release, design release, regulatory authorisation and commercial launch.

Apply a defensible release review

- Identify the approved product, software, manufacturing and labelling configuration.
- Confirm required acceptance records, verification evidence, process status and traceability.
- Review nonconformities, concessions, complaints, open CAPAs and deviations relevant to the release.
- Assess product risk, regulatory status, supplier changes and any limitations or conditions.
- Ensure authorised personnel approve the decision and that distribution or deployment records are controlled.

Escalate conflicts between schedule and evidence

A shipment target, customer commitment or revenue forecast does not resolve missing evidence or unacceptable risk. QA must make the deficiency and decision authority explicit, preserve the record and escalate when commercial pressure threatens patient safety or compliance.

26. Common quality-system failures and practical responses

Recurring quality problems usually result from unclear ownership, weak interfaces, incomplete evidence or incentives that prioritise appearance over effectiveness. QA should distinguish isolated errors from systemic failures and direct improvement to the cause.

Recognise common failure patterns

Failure pattern	More effective response
Procedures exist but actual work differs.	Observe the process, identify constraints and align controlled requirements with compliant practice.
Design controls are reconstructed at release.	Integrate requirements, review, traceability and approval into the development workflow.

Failure pattern	More effective response
The risk file is disconnected from engineering.	Trace risk controls to approved requirements, outputs and verification evidence.
Suppliers are approved only by certificates.	Evaluate critical capability, change control, performance and evidence access.
CAPAs close without effectiveness.	Require verified root cause, implemented action and risk-based follow-up.
Complaints remain separate from risk management.	Connect post-market signals to risk, CAPA, design change and reporting decisions.
Quality metrics reward administrative closure.	Measure recurrence, critical evidence gaps, process capability and patient impact.

Questions QA should ask at every milestone

- Do we understand the approved product, intended purpose, market and configuration?
- Are relevant processes owned, current, implemented and supported by competent people?
- Are requirements, risks, design outputs and verification or validation evidence consistent?
- Do suppliers, production processes and measurement systems preserve the approved design?
- Are failures, deviations, complaints and changes investigated and visible to the right decision-makers?
- Would an independent reviewer be able to follow the actual evidence without retrospective explanation?

PRACTICAL RULE A quality system is effective when the organisation can explain what it intended to do, show what it actually did, demonstrate that the product meets requirements and correct problems without hiding or rewriting the evidence.

Appendix A. Quality-assurance deliverables by development phase

Development phase	Representative QA deliverables
Concept and feasibility	Applicable-process assessment, regulatory scope, quality planning, resource and competence needs.
Design inputs	Design-plan review, input completeness assessment, risk-plan review and traceability expectations.
Architecture and development	Design reviews, document control, supplier qualification, change oversight and risk-control traceability.
Verification and validation	Plan and protocol review, sample and calibration checks, deviation oversight and evidence assessment.
Design transfer	Production readiness, process validation, supplier controls, critical characteristics and release procedures.
Release	Configuration review, acceptance evidence, residual issues, authorised approval and distribution readiness.
Post-market and change	Complaint and vigilance oversight, CAPA, trend review, audits, change impact and lifecycle records.

Appendix B. Essential quality-assurance review checklist

Review area	Minimum question
Scope and governance	Are the legal manufacturer, sites, products, markets and responsibilities clearly defined?
Documents and records	Are approved versions controlled and original evidence accurate, retrievable and protected?
Competence	Do personnel have the knowledge, experience and authority required for their role?
Design controls	Are needs, requirements, outputs, reviews, verification and validation complete and traceable?
Risk management	Are risk controls implemented, effective and connected to lifecycle evidence?
Suppliers	Are critical suppliers qualified, monitored and bound by suitable change and quality controls?

Review area	Minimum question
Manufacture	Are processes, equipment, calibration, acceptance and release under effective control?
Nonconformity and CAPA	Are issues contained, investigated, corrected and checked for effectiveness?
Post-market	Are complaints, vigilance, trends and field information reviewed and acted upon?
Management oversight	Do reviews and metrics lead to decisions, resources and sustained improvement?

Appendix C. Commonly relevant standards and frameworks

Confirm current controlled editions, applicability, amendments, jurisdictional status and product-specific requirements before claiming conformity.

Topic	Common reference	Quality-assurance relevance
Quality management	ISO 13485:2016; US 21 CFR Part 820 QMSR	Quality-system governance, design, production, suppliers, records and improvement.
Risk management	ISO 14971:2019; ISO/TR 24971:2020	Lifecycle risk process, control effectiveness and production or post-production feedback.
EU device legislation	Regulation (EU) 2017/745; Regulation (EU) 2017/746	Manufacturer obligations, technical evidence, GSPRs and post-market duties.
Software lifecycle	IEC 62304, applicable edition	Software planning, safety classification, development, verification and maintenance.
Usability engineering	IEC 62366-1, applicable edition	Use-related risk, user-interface design and usability validation.
Cybersecurity	IEC 81001-5-1; FDA cybersecurity guidance	Secure product lifecycle, vulnerability management and security-control evidence.
Medical electrical equipment	IEC 60601 series, where applicable	Basic safety, essential performance and applicable product-family evidence.

Topic	Common reference	Quality-assurance relevance
Biological evaluation	ISO 10993-1:2025 and relevant parts	Biological safety evaluation, material control and risk-based evidence.
Laboratory competence	ISO/IEC 17025:2017	Testing and calibration competence relevant to product and process acceptance.
Manufacturer information	ISO 20417:2026; ISO 15223-1, as applicable	Controlled product information, labelling, instructions and symbols.

Appendix D. Glossary

Term	Meaning in this guide
Acceptance criterion	A predefined condition used to decide whether a product, process or result conforms.
Audit	A systematic, independent evaluation of whether requirements are implemented and effective.
CAPA	Corrective and preventive action used to address causes and prevent recurrence or occurrence.
Change control	Documented assessment, approval and implementation of a proposed change.
Complaint	Information indicating a possible deficiency in device identity, quality, durability, reliability, safety or performance.
Concession	Approved permission to use or release an identified nonconforming product under justified conditions.
Design input	An approved requirement defining what the product must achieve.
Design output	A controlled specification, record or implementation describing the resulting design.
Nonconformity	Failure to fulfil a specified requirement.
Objective evidence	Data or information supporting the existence or fulfilment of a requirement.
Process validation	Confirmation that a process can consistently produce results meeting predefined requirements.

Term	Meaning in this guide
Quality assurance	Planned and systematic activities establishing confidence that quality requirements will be fulfilled.
Quality control	Operational techniques used to determine whether a product or process meets requirements.
Quality-management system	The organisation's controlled processes, responsibilities and resources for achieving quality objectives.
Risk control	A measure intended to reduce or maintain medical-device risk within acceptable limits.
Traceability	The maintained relationship between needs, risks, requirements, outputs, evidence and decisions.
Validation	Confirmation that requirements for a specified intended use have been fulfilled.
Verification	Confirmation that specified requirements have been fulfilled.

Appendix E. Authoritative starting sources

- ISO — ISO 13485:2016, Medical devices quality management systems
- 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/IEC 17025:2017, Testing and calibration laboratory competence
- 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 — Quality Management System Regulation: Frequently Asked Questions
- FDA — Applying Human Factors and Usability Engineering to Medical Devices
- FDA — Cybersecurity in Medical Devices: Quality Management System Considerations
- 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

CONTROLLED USE Consult current controlled editions of applicable legislation, standards and regulatory guidance. Quality-system scope, evidence expectations and release decisions depend on the actual product, intended use, markets and approved company processes.