WHITE PAPER

elevate MEDTECH

HealthTech Activator

# Implementation & Best Practices: Building a QMS Compliant with ISO 13485 and Beyond

## Executive Summary

Bringing ISO 13485 to life inside an organisation is often harder than gaining a basic understanding of the standard itself. No medical device reaches the market without a robust quality management system (QMS), and ISO 13485 has become the key global reference for what "good" looks like. Yet simply adhering to the ISO 13485 standard is not enough. Organisations need a QMS that actually works in day-to-day practice.

This white paper outlines a practical roadmap to implement ISO 13485 sustainably and in line with business goals. It draws on real-world case studies, regulatory guidance, and recognised industry standards to show what effective implementation looks like in practice. The focus lies on concrete steps: how to prioritise processes, how to build a risk-based QMS, and how to translate regulatory text into clear responsibilities, records, and behaviours.

Because ISO 13485 serves as the core QMS framework for medical devices worldwide, the guidance in this paper is relevant for organisations of all sizes, from early-stage developers to established manufacturers. It is particularly valuable for those active in multiple markets. ISO 13485 either underpins, aligns with, or is directly referenced by most major regulatory regimes, including the United States Quality Management System Regulation (QMSR). A QMS built on ISO 13485 supports patient safety, reduces rework and delay, and creates a competitive advantage because the same system can support entry into several jurisdictions without constant redesign.

This matters because weaknesses in the QMS remain one of the most common causes of regulatory findings and warning letters. Industry analyses and inspection data often show that a large proportion of observations are linked to gaps in core processes such as Corrective and Preventive Action (CAPA), supplier control, design and development controls, document and record management, and post-market surveillance. Organisations that treat ISO 13485 as a living framework, embed risk management in their daily work, and integrate quality into product and business decisions tend to face fewer findings in audits and achieve faster, more predictable market access.

## What this paper covers

**A phased, risk-based implementation strategy**
How to sequence ISO 13485 processes, link them to product and business risk, and avoid trying to "do everything at once".

**Key success factors**
Governance, leadership engagement, resourcing, and the role of digital tools in making the QMS usable rather than bureaucratic.

**How to avoid common pitfalls**
Typical failure modes in CAPA, documentation and supplier management – and how to address them early.

**The modern regulatory landscape**
How AI is changing QMS standards, how ISO 13485 interacts with major frameworks and regulations, and what organisations need to consider when planning for multiple markets.

**Real-world case studies**
Examples of organisations that built or upgraded their QMS around ISO 13485, the challenges they faced, and the measurable improvements they achieved.

# Whitepaper

## 1. Introduction: Why ISO 13485 Matters

ISO 13485 is the leading international standard for quality management systems (QMS) in the medical device sector, and it goes far beyond a high-level guideline. Regulators around the world treat it as the reference model for what a compliant QMS should look like, and many legal frameworks build directly on its requirements. In practice, ISO 13485 often defines the baseline for market access.

Major regulators and markets refer to ISO 13485 as follows:

- **United States (FDA)** – From 2 February 2026, FDA's QMSR takes effect and incorporates ISO 13485:2016 by reference, with additional US-specific requirements.[41]
- **European Union** – ISO 13485 supports conformity assessment and CE marking under both the In Vitro Diagnostic Regulation (IVDR 2017/746) and the Medical Device Regulation (MDR 2017/745).[42]
- **Global markets** – China, Japan, Canada, Australia and many emerging markets either require ISO 13485 certification or recognise it as strong evidence of QMS conformity.

### Benefits that go beyond compliance

For manufacturers, alignment with ISO 13485 also makes clear business sense. A well-designed QMS reduces errors in design and manufacturing, stabilises processes and lowers the risk of recalls. Fewer defects mean fewer investigations, less scrap and stronger operational performance. A visible commitment to ISO 13485 also builds trust. A robust QMS signals reliability and care not only to patients and customers, but also to partners, notified bodies and investors. Over time, quality performance becomes part of the organisation's reputation.

### Enabler for speed and scale

Effective QMS processes can also speed up market entry and later scale-up. When teams work with clear procedures, defined interfaces and reliable data, they can move products through design, verification, validation and registration with fewer delays and surprises. As portfolios grow, the same disciplined framework makes it easier to add new product lines, expand into new jurisdictions and manage a more complex supply chain without losing control.

### A framework for emerging risks

ISO 13485 further offers a structured way to deal with new and evolving risks. Topics such as AI and machine learning, standalone software, connectivity and cybersecurity introduce fresh failure modes and regulatory expectations. The standard helps management identify these risks, assess them in a consistent way and integrate suitable controls into the QMS. This supports a more resilient organisation as technology, regulation and clinical practice continue to shift.

For a deeper dive into the foundational ISO 13485 requirements, see our white paper "Building a Quality-Driven Culture in Medical Device Organisations for ISO 13485"

## 2. The Best Approach: A Phased, Risk-Based Implementation Strategy

Implementing ISO 13485 is a substantial change effort. However, for most organisations, a twelve-month timeframe is realistic if the work is broken into manageable steps and aligned with product and business risk. Attempts to roll out all requirements at once usually overload teams and result in a QMS that looks complete on paper but does not shape day-to-day work.

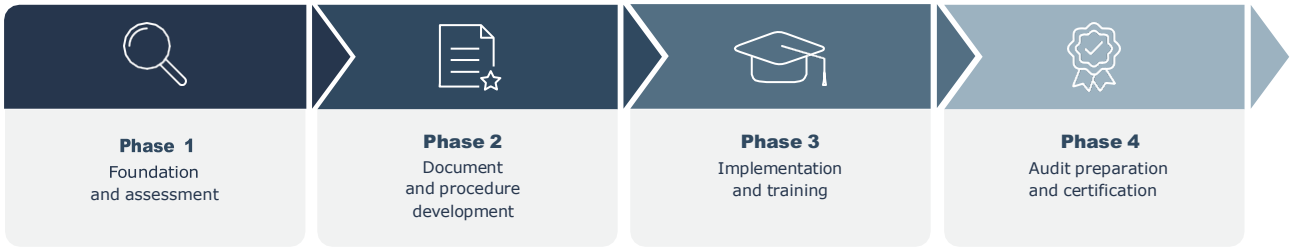
A phased, risk-based approach gives structure. It starts with a clear view of where the organisation stands today, then builds and documents the core processes, brings them into daily practice and, finally, demonstrates that the system is stable enough for certification.

The implementation journey can be grouped into four phases:

**Phase 1:** Establish the foundations
**Phase 2:** Document and procedure development
**Phase 3:** Implementation and training
**Phase 4:** Audit preparation and certification

The following sections walk through these phases in sequence. Timelines provided in this section are indicative and may overlap depending on organisational size, product complexity, and team maturity. Later chapters also explore the three pillars for successful implementation and highlight the most common pitfalls to avoid along the way.

## The Best Approach: A Phased, Risk-Based Implementation Strategy




### 2.1 Phase 1: Foundation and Assessment (Weeks 1–4)

The first phase sets direction. The aim is to understand the current state, define the scope of the QMS and secure leadership commitment.

Organisations begin with a structured gap analysis against ISO 13485 and all relevant regulations, such as FDA 21 CFR Part 820, IEC 62304 for software and ISO 14971 for risk management. This review shows which requirements are already in place, which are missing and where the greatest risks lie. At the same time, the scope of the QMS is defined: which products, sites, processes and suppliers fall under the system.

A cross-functional steering committee with executive sponsorship is then established. This group owns the implementation path, resolves conflicts and ensures that quality is not treated as a side project. It identifies which clauses of ISO 13485 are applicable and where justified exclusions apply. Process owners and subject matter experts are appointed for each functional area so that responsibilities are clear from the outset.

**Steps:**

1. **Run a gap analysis** against ISO 13485 and other relevant regulations.
2. **Define the QMS scope** (products, sites, processes, suppliers).
3. **Set up a cross-functional steering committee** and assign process owners.

Success metric: leadership alignment on QMS scope, timeline and resource allocation.

### 2.2 Phase 2: Document and Procedure Development (Weeks 5–25)

The second phase builds the core infrastructure for QMS operations. The focus lies on the processes that regulators scrutinise most closely and that carry the highest risk for patients and the business.

Key procedures to prioritise include:

1. **Design and development (Clause 7.3)** – Links stakeholder and user needs to design outputs, verification and validation activities.
2. **Risk management (ISO 14971 integration)** – Provides a consistent approach to hazard identification, risk evaluation, control and residual risk acceptance.
3. **Manufacturing process controls (e.g. Clause 8.5)** – Covers production instructions, process validation, change control and acceptance criteria.
4. **Corrective and preventive action (CAPA) (Clause 8.5.2)** – Ensures structured root-cause analysis and systematic, documented improvement.
5. **Supplier management (Clause 8.4)** – Sets out qualification, monitoring and collaboration with critical suppliers and service providers.
6. **Internal audits (Clause 8.2.4)** – Provides an independent, planned review of QMS effectiveness.
7. **Management review (Clause 5.6)** – Gives executive-level oversight of QMS performance, risks and improvement priorities.
8. **Document and record control (Clause 4.2.3)** – Governs version control, approval, retention and accessibility of documents and records.

with this phase, focus is on the processes with the greatest regulatory and patient risk. A well-written CAPA procedure means little if product development is inconsistent or poorly documented. Procedures should reflect how work actually happens and guide improvement, not describe an ideal process no one follows.

**Practical steps in Phase 2**

1. **Sequence the work by risk**
   Decide the order in which to develop procedures, starting with design and development, risk management and manufacturing controls.

2. **Capture how work is done today**
   For each core process, the process owner maps the real workflow (inputs, decisions, outputs, interfaces) using existing practices as a starting point.

3. **Draft ISO 13485–aligned procedures**
   Convert these workflows into procedures and work instructions that meet the relevant clauses (and linked standards such as ISO 14971 and IEC 62304), without adding unnecessary steps.

4. **Create a minimal set of templates & forms**
   Define standard templates for design documents, risk files, validation reports, CAPA records, supplier assessments and audit reports to enforce consistency and traceability.

5. **Integrate related disciplines into one framework**
   Where software or AI/ML is involved, fold IEC 62304, ISO 14971, usability engineering and Good Machine Learning Practice into the design control process, instead of running separate, siloed processes.

6. **Define traceability rules**
   Agree how stakeholder needs link to design inputs, design outputs, verification, validation and risk controls, and reflect this in both procedures and templates.

7. **Review and approve with the right roles**
   Process owners and relevant regulatory role holders (e.g. PRRC, QA/RA leads) review each procedure, refine it with feedback from users and formally approve it in the document control system.

Success metric: all core processes documented by named process owners and formally reviewed and approved by co-owners or relevant regulatory role holders.

## 2.3 Phase 3: Implementation and Training (Weeks 13–40)

Once procedures exist on paper, they need to come to life in daily work. Phase three focuses on implementation, training and real-world QMS use.

**Practical steps in Phase 3:**

1. **Roll out approved procedures**
   Publish finalised procedures in the QMS, communicate effective dates and retire obsolete documents.

2. **Plan and deliver role-based training**
   Map each role to the relevant procedures, run focused training sessions and record attendance and competence.

3. **Configure and deploy QMS software**
   Implement an electronic QMS (eQMS), set up workflows (document control, CAPA, complaints, audits) and migrate key legacy records where needed.

4. **Establish the central risk management file**
   Create a single, structured risk file and start populating it with existing and new risk analyses for software, hardware and system-level hazards.

5. **Start using core processes “for real”**
   Run live projects under the new design controls, log issues and improvements in CAPA, qualify or re-qualify key suppliers and schedule internal audits.

6. **Monitor adoption and remove obstacles**
   Track usage of procedures and QMS tools, collect feedback from teams and adjust forms, workflows or training where they block effective use.

7. **Run a pilot internal audit**
   Audit a sample of processes, document findings and close them out to test both the system and the organisation’s readiness for certification.

Success metric: staff trained, procedures actively followed in day-to-day work and QMS software in stable operation.

**Note:** Phase 2 and Phase 3 timelines should be understood as indicative only, especially where inhouse manufacturing, assembly, packaging, sterilisation, or other special processes are part of the scope. In such cases, process qualification and validation activities (for example IQ, OQ, PQ and sterilisation validation) can easily add several months, as equipment must be installed, challenged under defined operating ranges, and then shown to perform consistently under routine conditions before being released to full production. For many organisations this means that what is planned as a 3–6 month implementation and training window can expand to 9–12 months or more once process development, engineering runs, and collection of sufficient production data are factored in.

This dependency is exactly why Phase 1 (assessment and planning) is so critical. A robust upfront gap assessment and roadmap clarifies which processes are already mature, where new or changed manufacturing or sterilisation steps will require full validation, and what timelines, resources, and regulatory expectations are realistic for your organisation. Investing time in Phase 1 reduces the risk of late surprises during Phases 2 and 3, helps align stakeholders on priorities and milestones, and ensures that validation activities, QMS implementation, and training are sequenced in a way that supports both compliance and an on time start of routine operations.

## 2.4 Phase 4: Audit Preparation and Certification (Weeks 41–52)

The final phase prepares the organisation to demonstrate sustained compliance and secure ISO 13485 certification.

A full internal audit is performed, covering all applicable clauses and processes within the defined QMS scope. Findings are documented, analysed and closed out with appropriate corrective actions. Management review follows, with documented decisions on resources, priorities and strategic risks related to the QMS.

The organisation compiles objective evidence—procedures, records, risk files, validation reports and training logs—for the certification body. The certification process typically includes a Stage 1 audit focused on documentation and readiness, followed by a Stage 2 on-site audit that tests implementation.

Any non-conformances raised during these audits are addressed with timely root-cause analysis and corrective actions, which are documented in the CAPA system.

### Practical steps in Phase 4

1. **Plan and execute a full internal audit**
   Cover all processes and sites in scope; document findings, classify them and open CAPAs where needed.

2. **Hold a formal management review**
   Review audit results, QMS performance, complaints, CAPA trends and resource needs; document decisions and actions.

3. **Prepare the audit evidence package**
   Compile current versions of procedures, key records, risk files, validation and verification reports, supplier documentation and training evidence.

4. **Engage and schedule the certification body**
   Confirm scope, sites and dates for Stage 1 and Stage 2 audits; brief internal stakeholders on the audit plan.

5. **Run an audit readiness check**
   Walk through the audit agenda, rehearse key process interviews and ensure documents and records are easy to retrieve.

6. **Support the Stage 1 and Stage 2 audits**
   Provide requested evidence, ensure process owners are available and record any observations or non-conformances.

7. **Close out non-conformances**
   Perform root-cause analysis, define and implement corrective actions and provide evidence of closure to the certification body.

Success metric: ISO 13485 certification achieved with zero or minimal non-conformances and a QMS that supports ongoing improvement, not just a one-time audit

## Four-Phase ISO 13485 Implementation Roadmap

| PHASE | DURATION | KEY MILESTONES | RESOURCES REQUIRED |
|---|---|---|---|
| **1. Foundation & Assessment** | 4-8 weeks | Gap analysis, scope definition, steering committee | One QA lead, leadership, external consultant |
| **2. Documentation** | 8 - 30 weeks | Procedures drafted, reviewed, approved | Process owners, process co-owners, Quality Management Responsible, external consultant |
| **3. Implementation & Training** | 8 – 30 weeks | Procedures deployed, staff trained, QMS software operational | Full staff, process owners, QMS tools |
| **4. Audit Preparation** | 6 – 12 weeks | Internal audits, first management review, corrective actions, audit readiness | Internal auditor, QA team, process owners, leadership |
| **5. Ongoing (Post-Certification)** | Continuous | Management Review, internal audits, CAPA, procedure updates, PMS, PMCF | Embedded QA team (typically 2-3 FTE for mid-sized organisation) |

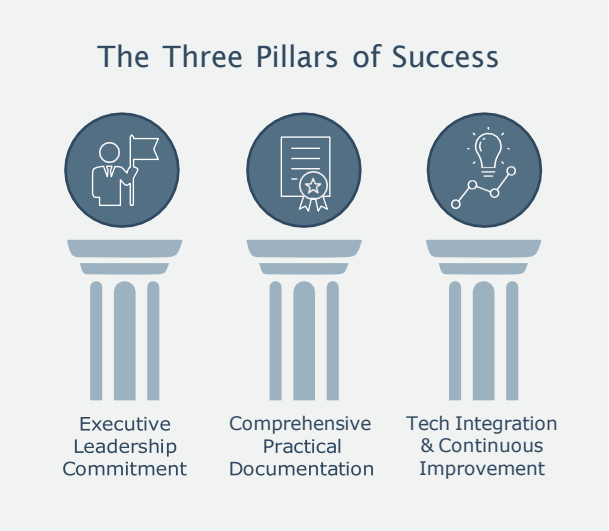
PMS = Post Market Surveillance
PMCF = Post Market Clinical Follow Up

Total timeline to certification: 9-24 months for organisations starting from scratch.

## 3. Success Factors: The Three Pillars

The four phases describe how to sequence ISO 13485 implementation over roughly a year. However, whether the QMS takes root in day-to-day work depends on a few underlying conditions that need to be in place throughout all phases. For ISO 13485 to work in practice, three pillars need to stand firmly:

1. Executive leadership commitment
2. Comprehensive, practical documentation
3. Technology integration and continuous improvement.



### 3.1 Pillar 1: Executive Leadership Commitment

Executive commitment is the base layer of an effective QMS. ISO 13485 implementation demands resources, clear priorities and visible support from the top. If senior leaders treat quality as a side topic, the system will fragment, stall or remain purely cosmetic.

Leadership commitment means that quality is treated as a core business topic, alongside revenue, product strategy and funding. The leadership team is visibly involved in QMS governance, turns up to management reviews, and backs tough decisions when quality conflicts with short-term goals. Quality metrics are reviewed regularly, not only before an audit. When executives follow procedures themselves, respond to quality concerns and recognise people who raise issues early, the rest of the organisation quickly understands that quality is not optional.

Some concrete moves help anchor this pillar:

- **Appoint an executive sponsor** for ISO 13485 with clear accountability for outcomes, not just for "support".
- **Build QMS goals into the business plan** and leadership objectives, for example, audit readiness, CAPA closure times, and complaint trends.
- **Establish a regular QMS governance forum**, chaired or attended by senior leaders, where roadblocks are removed and priorities confirmed.

When staff see that leadership protects quality time, funds training and tools, and accepts short delays if they are needed to stay compliant, the QMS gains real authority.

### 3.2 Pillar 2: Comprehensive, Practical Documentation

Documentation is how a QMS becomes visible. It shows what should happen and what actually happened. Weak documentation is either too vague to guide anyone or so theoretical that no one follows it. Both fail in daily work and under audit.

The aim is lean, practical documentation that fits the organisation and reflects real processes. Procedures should be clear enough that a new team member can follow them, but not so detailed that every minor step requires a revision. They should describe how work is done today and then guide improvement over time.

In practice, this pillar rests on a few disciplined habits. Each core process has a named owner who is responsible for the related procedure and records. Templates for design files, risk analyses, validation reports, CAPA, audits and supplier assessments are standardised so that information looks and feels familiar regardless of who created it. Document control is managed centrally, with clear versioning, approvals and access rights, so teams do not work from outdated files.

To keep documentation alive rather than static, organisations schedule regular reviews of key procedures and fold feedback from audits, projects and users back into the documents. Short, focused "walk-throughs" with the people who actually use a procedure work well: they quickly show which steps are unclear, duplicated or ignored.

A simple set of actions helps make documentation a strength rather than a burden:

- **Assign one owner for each key procedure** and give them time to maintain it.
- **Standardise a small set of templates** and keep them only in the controlled document repository, not on personal drives.
- **Introduce a review cycle** (for example, yearly) for high-impact procedures and track completion.

When documentation is practical and accessible, teams are far more likely to follow it, and auditors will find a coherent story from policy through to records.

### 3.3 Pillar 3: Technology Integration and Continuous Improvement

Manual, paper-heavy QMS processes can work for a single product and a small team. They rarely work for long. As volumes grow, spreadsheets get out of sync, emails go missing and no one is quite sure which version of a document is current. Data integrity risks increase, and the QMS becomes hard to trust.

A modern electronic QMS (eQMS) helps avoid this. It automates approvals, tracks changes, enforces workflows and generates audit trails without extra effort. When document control, training, CAPA, complaints, audits and supplier management sit in one system, it becomes much easier to see how issues connect. Dashboards make quality performance visible: open CAPAs, overdue training, audit findings, supplier trends. Remote and cross-functional teams can collaborate in real time rather than chasing files.

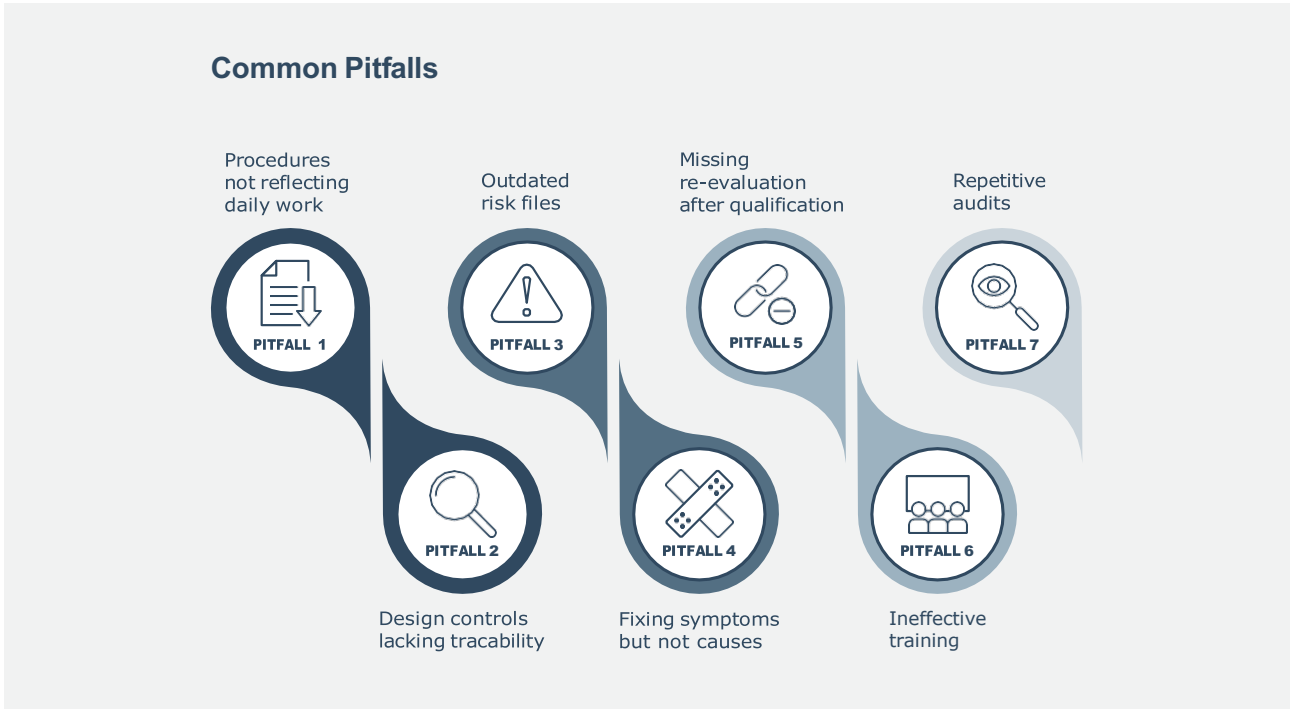
Technology alone, however, does not guarantee improvement. The real power comes when eQMS data feeds a deliberate continuous improvement cycle. Findings from audits, CAPA, complaints and production are reviewed, prioritised and turned into changes in design, process or training. Methods such as Failure Mode and Effects Analysis (FMEA) and structured risk reviews are used not just once during development, but repeatedly as new information appears.

Practical steps to anchor this pillar include:

- **Select and implement an eQMS** that fits the organisation's size, products and regulatory scope, and configure workflows for document control, change control, CAPA and audits.
- **Set up a small number of quality dashboards** and review them in management and quality meetings to guide decisions.
- **Plan regular risk and performance reviews,** where recent issues, FMEAs and risk files are updated based on actual experience.

## 4. Common Pitfalls

Even with a solid plan, ISO 13485 implementation can stall on a handful of recurring problems. Most issues cluster around six areas: procedures and documentation, risk management, CAPA, supplier management, training and internal audits. The patterns are remarkably similar across organisations, which makes them easier to anticipate and avoid.



## Pitfall 1: Procedures that do not match day-to-day work

One of the most common failures is a QMS that looks convincing in documents but bears little resemblance to how people actually work. Procedures are drafted by a small core team, sometimes lifted from generic templates, and then rolled out without checking whether they fit real workflows. On the shop floor and in development teams, staff quietly keep using their own methods because the official process feels unrealistic, slow or unclear.

This creates a split system: a "paper QMS" for auditors and a "real QMS" built on habit and local fixes. Training sessions cover the documented procedures, but staff revert to familiar shortcuts once the session ends. New colleagues learn more from colleagues' explanations than from controlled instructions. When auditors ask people to describe a process, the story they hear often does not match what is written in the procedure.

The impact is serious. The organisation cannot rely on its own documentation to predict outcomes, quality becomes person-dependent and audit confidence drops as soon as inconsistencies surface.

To keep procedures aligned with reality, development needs to start where the work happens:

- map the actual workflow with the people who do the job, then write the procedure around that flow
- run a short "trial period" where the draft procedure is used in real tasks and adjusted based on feedback

write in plain, concrete language so that someone new to the role can follow the steps without extra explanation

## Pitfall 2: Design controls without clear traceability

Another common weakness lies in design documentation that looks complete at first glance but lacks clear links from user needs to verification and validation. Stakeholder requirements, design inputs, design outputs and test evidence exist in separate documents, with no obvious way to follow the chain.

This makes it hard to show that all intended uses and hazards have been addressed. Important requirements can slip through untested. In the worst case, this leads to recalls or serious field issues because a "known" risk was never properly verified or validated.

Effective design control creates an explicit thread from initial concept through to testing. Design inputs spell out user needs, intended use and performance requirements. Design outputs translate these into technical specifications. Verification and validation plans are defined early and reference the inputs they cover. For software and AI/ML, IEC 62304 and appropriate machine learning practices sit inside this same framework rather than alongside it.

In practice, this means:

- creating clear design input and design output documents with explicit links between the two
- planning verification and validation early in the project, not at the end
- using traceability matrices to connect stakeholder requirements, design elements and tests
- embedding software and AI/ML controls into the same design control process, rather than running separate streams

## Pitfall 3: "One-off" risk files that are never updated

Risk management often starts well during initial development, then quietly fades. The risk file is completed for the first submission, approved, and then left untouched while designs evolve, suppliers change, or new clinical data emerges. Over time, risk documentation no longer reflects the product in the market.

When inspectors open these files, they quickly see that new risks, new features and new field data have not been considered. This raises questions about the organisation's control of device safety across the lifecycle, not just at launch.

To avoid this, risk management needs to sit at the centre of the lifecycle. A single, central risk management file is maintained for each product or product family and updated whenever design, manufacturing, software or clinical use change. Change control, CAPA and post-market surveillance all link back into this file so that any event that could affect safety triggers a review.

Practical habits that support this include:

- keeping one controlled risk management file per product and updating it with every relevant design or process change
- integrating risk review into change control, CAPA and complaint handling workflows
- clearly documenting risk decisions and the evidence behind them
- scheduling periodic risk reviews (at least annually) to reassess residual risks and emerging issues
- providing targeted training on new risk areas such as AI/ML or cybersecurity so teams can recognise and assess them properly

## Pitfall 4: Fixing symptoms but not causes

Many organisations respond quickly when something goes wrong: a batch is reworked, a customer receives a replacement, a checklist is updated. These actions correct the immediate problem but often leave the root cause untouched. The same non-conformance then reappears months later under slightly different circumstances.

Regulators look for evidence that CAPA drives systemic change, not just quick fixes. If similar findings appear year after year in audits, or the same complaint themes repeat, it suggests that root causes are not being understood or addressed.

A strong CAPA process requires formal root cause analysis as a standard step, not an optional extra. Teams are encouraged to ask why an issue occurred, what in the system allowed it to happen, and how to change that system. Corrective actions then focus on design updates, process changes, training or supplier improvements, rather than only on the immediate incident.

Useful actions here are to:

- make structured root cause analysis mandatory for significant non-conformances and repeat issues
- link CAPA outcomes to specific changes in procedures, training, design or supplier controls
- define how and when CAPA effectiveness will be checked, and close actions only when recurrence has genuinely reduced
- review CAPA trends regularly at management review to spot patterns that point to wider system weaknesses.

## Pitfall 5: Strong qualification, weak follow-up

Supplier management commonly starts with a thorough qualification audit, questionnaires and contract review. Once the supplier is approved, attention shifts elsewhere. Years can pass without any structured review of performance or capability.

This gap shows up when a critical supplier changes its processes, staff or sub-suppliers without notice. Quality issues appear in incoming goods, production schedules slip and complaint volumes rise. Investigations then reveal that no one has looked closely at the supplier for a long time.

ISO 13485 expects ongoing supplier control. That applies to both physical suppliers and service providers such as cloud platforms, testing labs or consultants. Regular performance monitoring, periodic audits and clear expectations in contracts are key.

Practical steps include:

- defining supplier performance metrics such as defect rates, response times and on-time delivery, and reviewing them at least annually
- scheduling periodic supplier audits or reviews based on risk and criticality
- making quality expectations and responsibilities explicit in supplier agreements
- treating critical service providers with the same discipline as component suppliers, including risk assessment and performance review.

## Pitfall 6: Training that is recorded but not effective

Training records often look impressive: high completion percentages, many sessions, long attendance lists. Yet audits still reveal staff who cannot explain procedures relevant to their job, or who work from outdated instructions. The problem is not the lack of training events, but the weak link between training content, current procedures and actual tasks.

When training is not taken seriously, people may sit through sessions without understanding how the material changes their work. Over time, they rely on habit instead of updated procedures. Effective training connects specific procedures to specific roles and checks that people can apply what they have learned. It uses refresher sessions when procedures change, not only on a fixed yearly cycle, and it draws on audits and incidents to target where more support is needed.

A practical approach is to:

- map each role to the procedures and records that person needs to know
- update training materials whenever key procedures change, and trigger refresher training accordingly
- use on-the-job observation, competency checks or targeted questions during internal audits to confirm that training has “landed”
- promote cross-training where appropriate, so the organisation is less vulnerable to single points of knowledge

## Pitfall 7: Internal audits that never change the picture

An internal audit is an independent check, carried out by the organisation itself, to verify that processes follow ISO 13485 and internal procedures and to identify opportunities for improvement. They are meant to act as an early warning system and a driver of improvement. In many organisations, though, they become routine inspections that generate the same categories of findings year after year. Checklists are reused without much thought, and audit results are filed away with limited follow-up.

This pattern signals that audits are not probing root causes or feeding into broader QMS improvements. Regulators may then question how the organisation learns from its own findings, especially if external audits reveal issues that internal audits missed.

Raising the value of internal audits does not always require more audits, but better ones. Auditors need training, independence where possible, and support to look beyond surface symptoms. Audit results should flow into CAPA and management review, with clear actions and timelines.

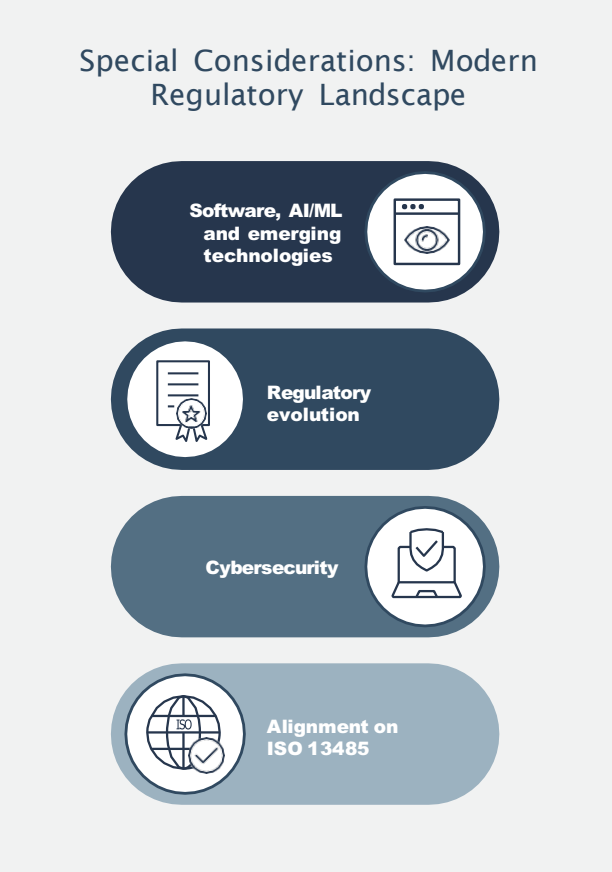
Concrete ways to strengthen this area:

- plan audits based on risk, focusing more attention on high-impact processes and recent change areas
- use auditors who are trained and, where practical, not auditing their own work
- ensure audit findings are reviewed in management meetings and translated into specific corrective actions
- track whether the volume and severity of findings decrease over time in areas where actions have been taken.

## 5. Special Considerations: Modern Regulatory Landscape

ISO 13485 provides a stable backbone, but the environment around it moves quickly. Software-driven devices, AI and machine learning, and rising cybersecurity expectations have reshaped what "good practice" looks like.

At the same time, regulators are aligning more closely on ISO 13485 while still keeping regional specifics. A QMS that ignores these shifts risks being technically compliant on paper but unconvincing in front of authorities and customers.



## 5.1 Software, AI/ML and Emerging Technologies

Software now sits at the centre of many medical devices, whether as embedded code, connected components or standalone Software as a Medical Device (SaMD). For these products, ISO 13485 alone is not enough. It needs to be read together with standards such as **IEC 62304 for software lifecycle processes and IEC 82304-1 for health software safety and security**. Design and development procedures must reflect this combined view so that software requirements, architecture, implementation, verification and maintenance are controlled in a structured way.

### SaMD and complex system architectures

For SaMD and complex system architectures, software validation becomes a core quality and regulatory topic. Regulators expect clear test strategies, robust evidence and traceability from requirements through to test results. This applies not only at initial release but also across updates and maintenance, especially where cloud deployment or frequent releases are involved. Change control must be able to cope with iterative development without losing oversight.

### AI and machine learning

AI and machine learning applications bring further challenges. Algorithms can evolve based on new data, which blurs the line between "development" and "post-market". Good Machine Learning Practice (GMLP) principles therefore need to sit inside the software development lifecycle, rather than next to it. They prompt teams to think about data representativeness, bias, robustness and monitoring from the outset.

Key AI-specific concerns include:

- how and when algorithms are retrained
- how training and validation datasets are sourced, cleaned and governed
- how performance is measured across different sub-populations and use conditions
- how drifts in performance are detected and acted on once the product is in the field.

### Cybersecurity

Cybersecurity cuts across both software and connected hardware. Vulnerabilities in communication protocols, third-party components or cloud environments can have direct implications for patient safety and for regulatory compliance. Modern expectations treat cybersecurity as part of risk management, not as a separate IT topic.

Risk controls may include secure development practices, hardening measures, access controls, encryption, update mechanisms and incident response plans. Post-market security patches and updates must be planned and documented with the same care as any other design change. In this landscape, ISO 13485 remains the anchor, but the QMS must be capable of absorbing and connecting these additional standards and practices. Software lifecycle controls, AI/ML governance and cybersecurity risk management become part of one coherent system rather than a collection of add-ons.

## 5.2 Regulatory Evolution: FDA Updates and International Alignment

Regulators have moved steadily towards greater alignment around ISO 13485, while still keeping national and regional priorities. The practical implication is clear: a rigid, single-jurisdiction QMS will struggle as soon as the organisation looks beyond its first market.

A flexible, modular ISO 13485 framework, by contrast, can support several regulatory regimes at once. Regional requirements can then be addressed through targeted additions—such as extra records, reports or evaluations—without rewriting the underlying quality system each time.

### FDA

As of February 2026, the US FDA's recognition of ISO 13485 is formal and permanent.[41] This gives manufacturers a clearer pathway: a QMS built on ISO 13485 can serve as the core reference for FDA expectations under the Quality Management System Regulation (QMSR). However, specific FDA requirements still apply, so alignment does not mean full identity.

### Medical Device Single Audit Program (MDSAP)

Other frameworks reinforce this trend. The Medical Device Single Audit Program (MDSAP) allows one audit to cover multiple jurisdictions, including the US, Canada, Japan, Brazil and Australia. Participating regulators rely on MDSAP outcomes as part of their oversight, which raises the bar for the consistency and maturity of the QMS. ISO 13485 sits at the heart of this programme, but each country's particular rules still shape the details of the audit.

### Europe

In Europe, the Medical Device Regulation (MDR 2017/745) and the In Vitro Diagnostic Regulation (IVDR 2017/746) have tightened expectations around risk management, clinical evidence and post-market surveillance. ISO 13485 supports these requirements, especially around design control, documentation and lifecycle processes, but manufacturers must still address MDR/IVDR-specific obligations such as clinical evaluation, post-market clinical follow-up and the roles of economic operators.

### China and Emerging Markets

China's NMPA has also moved closer to ISO 13485 while maintaining local extensions and specific documentation and registration practices. Many emerging markets follow a similar pattern: they adopt ISO 13485 as a base, then add country-specific amendments or implementation rules. This combination rewards organisations that design their QMS as a common core with configurable elements, rather than as a patchwork of separate systems.

## 6. Case Studies: From Pitfalls to Proven Success

Now that the key principles, phases and pitfalls of ISO 13485 implementation are clear, the next step is to see how they play out in real organisations. The following case studies trace real organisations as they build or upgrade their QMS, run into familiar obstacles and adjust their approach. Each case highlights concrete decisions, missteps and course corrections, along with measurable outcomes such as audit results, time-to-market and defect trends.

### Case Study 1: SaMD manufacturer's first MDR Audit – Design Validation Clinical Evaluation

**Background:**

A long-established SaMD manufacturer specialising in cardiology decision-support software prepared for its first EU MDR Notified Body (NB) audit with high confidence, relying on its decade-long market presence and legacy CE marks under the former MDD. During MDR transition, the company focused on upgrading technical documentation and cybersecurity, assuming that existing clinical publications and key opinion leader support would be sufficient to demonstrate clinical evidence for the European market.

**Problem:**

During the Stage 2 NB audit, the auditor requested the Clinical Evaluation Procedure and related Clinical Evaluation Plan and Report, only to find that the QMS contained no dedicated procedure describing how clinical evaluation would be planned, performed, appraised, and updated in line with MDR Article 61 and Annex XIV and SaMD-specific guidance. The NB raised a major non-conformity because, despite having various clinical data, the manufacturer could not show a systematic, repeatable clinical evaluation process or demonstrate that evidence had been assessed against state of the art, benefit–risk, and post-market data as required for MDR. An internal investigation revealed the root cause: there was no formal regulatory strategy for the EU, responsibilities for regulatory intelligence were fragmented, and MDR-specific requirements for SaMD (including clinical evaluation expectations) had never been fully identified or translated into the QMS.

**Solution:**

The manufacturer implemented a formal EU regulatory strategy covering device classification, conformity assessment route, clinical evaluation, PMCF, and timelines for each SaMD product family, and established a cross-functional regulatory steering group responsible for monitoring MDR/MDCG guidance and feeding it into QMS and product plans.

A comprehensive Clinical Evaluation Procedure was introduced, defining roles, inputs (state of the art, clinical data, PMS data), literature methodology, evidence appraisal, benefit–risk assessment, and criteria for maintaining up-to-date Clinical Evaluation Reports throughout the lifecycle, aligned with MEDDEV 2.7/1 rev. 4 and MDCG 2020-1 for software. Within a year, robust Clinical Evaluation Plans and Reports were in place for the core SaMD portfolio, the NB accepted the revised system during a follow-up assessment, and the major non-conformity was closed, demonstrating how a structured regulatory strategy and documented clinical evaluation process can turn a serious audit finding into a foundation for long-term MDR compliance.

**Key Success Factors:** structured regulatory strategy

## Case Study 2: Medical Device Company Class 1 – document control and customer focus

**Background:**

A long-established medical device manufacturer had placed a non-sterile Class I device on the European market for many years under ISO 13485 certification, without Notified Body involvement as allowed for such devices. The company relied on long customer relationships and assumed that its existing technical documentation and quality system would remain sufficient for EU market access.

**Problem:**
During a routine check by a European national competent authority at an importer's premises, the authority reviewed the available documentation and found that the technical documentation, labelling, and EU declaration of conformity were outdated and no longer compliant with current MDR requirements. At the same time, the documents available to the distributor/importer were not controlled versions; obsolete documents had remained in circulation, contrary to ISO 13485 requirements to prevent the unintended use of outdated documents and to ensure that only current, approved versions are available at the point of use. The company's QRA responsible person was unaware of the documents handed over to the authority because there were no defined regulatory contact points with the importer; distributor and importer qualification focused on commercial criteria only, and sales had not recognised the need for structured regulatory communication or controlled document provision.

**Solution:**
The manufacturer introduced a formal process for qualification and ongoing management of new importers and distributors that explicitly integrates regulatory requirements. QRA was defined as a mandatory stakeholder in selecting and onboarding external partners, verifying that current declarations, technical documentation, and labelling sets are in place before any products are shipped to the EU. A central, controlled repository was established for all market-specific regulatory documents, with clearly defined access rights for external partners so that importers and distributors can always retrieve up todate, approved documentation for inspections and authority requests, thereby reducing compliance risk and strengthening oversight across the supply chain in line with ISO 13485 and EU MDR expectations for document control.

**Key Success Factors:** document control, regulatory communication, distributor management

## Case Study 3: Medical Device Startup – Software Change Control

**Background:**

A mid-size manufacturer SaMD operated under ISO 13485 and IEC 62304, but its procedures for software development, change control, and configuration management were high level and not clearly linked. The change request workflow in the QMS existed on paper, but roles and interfaces between Software Development, Software QA/ Testing, and Regulatory/Quality were vague, and day-to-day work followed agile boards and chats rather than the documented process.

**Problem:**
During a scheduled ISO 13485 internal audit, the auditor sampled several recent bug fixes and feature updates in the SaMD. By reviewing tickets, test reports, and Git logs, the auditor discovered that Software QA testers routinely communicated defects and desired changes directly to individual developers via chat or informal tickets, who then implemented code changes and pushed them for test without raising formal change requests, impact assessments, or approvals as required by the QMS. Several production builds contained changes that were traceable only to chat threads, with no documented risk assessment, no linkage to design requirements, no documented verification of the specific change, and no update of the software configuration list or risk file, contrary to IEC 62304 expectations that all configuration items be changed only via approved change requests with full traceability.

The internal audit raised multiple nonconformities, including:

- Inadequate implementation of documented change control procedure (changes implemented without approved change requests or impact assessments).
- Lack of traceability from problem reports and test findings to formal change records, risk management, and design documentation.
- Configuration management records not complete; version history did not consistently reference approved change requests.

**Root cause – culture and process misalignment**
Root cause analysis showed that teams saw the documented QMS change process as "too slow for agile development," so QA testers and developers had built an informal, faster path via direct communication. Management had not clarified how agile tools and sprints map to the formal change control process, and training on IEC 62304 and ISO 13485 change control expectations had been minimal.

**Solution:**
Corrective and preventive actions The company implemented several CAPAs:

- Revised and detailed the software change management SOP to explicitly link agile tools (backlog items, stories, bugs) to formal change requests, including when each ticket automatically generates a change record and required risk and impact assessment steps.
- Updated the RACI for software changes so that QA testers log findings into the issue-tracking system, which automatically creates or links to a controlled change record; developers may not implement code changes unless a change request is approved by the designated authority.
- Introduced configuration control rules so every code commits and build references a change request ID and problem report ID, creating a complete audit trail.
- Conducted targeted training for developers and QA on IEC 62304 and ISO 13485 requirements for change control, emphasising that no ad-hoc changes are allowed and that every modification must be documented, reviewed, and verified against defined acceptance criteria

A follow-up internal audit confirmed that all sampled software changes had corresponding approved change requests, documented impact and risk assessments, traceable test evidence, and updated configuration records. The company reduced the risk of unassessed software modifications reaching the field, strengthened its inspection readiness for regulators and Notified Bodies, and aligned day-to-day agile practices with the formal QMS.

**Key Success Factors:** training, QMS – agile process alignment, clearly defined process interaction.

## 7. Recommendations: How to Be Successful

This chapter turns our key findings into a concrete sequence of actions. The recommendations are grouped into three timeframes: steps for the first few weeks, activities to carry through the first year, and habits that keep ISO 13485 effective long after certification. Together, they provide a clear path from an initial concept to a QMS that is active, reliable and resilient.

### 7.1 Immediate Actions (Weeks 1–4)

1. Secure Executive Sponsorship: Ensure the leadership team understands ISO 13485 requirements and commits resources
2. Conduct Gap Analysis: Against ISO 13485, applicable regulations (FDA, EU, local), and industry-specific standards (IEC 62304, ISO 14971)
3. Define Scope: Which products, processes, and suppliers are included in the QMS?
4. Assign Roles: Identify QMS Manager, process owners, and SMEs
5. Select QMS Software: Implement a modern, scalable eQMS platform early to support implementation

### 7.2 Medium-Term Actions (Weeks 5-52)

6. Prioritise Core Processes: Focus on design, manufacturing, risk management, and CAPA first—these drive regulatory scrutiny
7. Develop Procedures: Involve frontline staff to ensure procedures reflect practice; use clear, concise language
8. Conduct Training: Comprehensive training with clear linkage to job responsibilities
9. Execute QMS Processes: Begin real CAPA investigations, internal audits, and management reviews with documented records
10. Conduct Pilot Audit: Identify gaps before the certification body arrives ++

### 7.3 Long-Term Success (Post-Certification)

11. Embed Quality Culture: Leadership models quality; quality metrics are discussed monthly
12. Continuous Improvement: Use internal audits, management review, and CAPA to systematically enhance QMS
13. Monitor Regulatory Changes: Stay informed of updates to ISO 13485, FDA guidance, and regional regulations
14. Invest in Training: Annual refresher training, specialized training for new hires, and advanced training for process owners
15. Leverage Data: Use QMS dashboards to make performance data visible and actionable

## 8. Conclusion

For ISO 13485 to work day to day, several elements need to interlock: leadership, processes, documentation and, above all, the people who use the system. The case studies in this paper point to three clear patterns.

1. Regulatory strategy defines QMS needs: It makes required procedures and records explicit so missing processes become visible early.
2. Document control extends to all partners: Current, controlled documents must reach every economic operator who represents or supplies customers.
3. Process owners shape compliant practice: They design processes within the regulatory framework so daily work, including agile methods, remains traceable and auditable.

Across all successful projects, one feature stands out: quality is not delegated to the quality

department and left there. Senior leaders own it, processes embed it and meaningful metrics track it over time.

Most organisations need around one to two years to build and stabilise an ISO 13485-compliant QMS. The effort is considerable, but the benefits run far beyond a certificate on the wall.

A robust QMS helps bring safer devices to patients, supports entry into new markets and absorbs new regulatory expectations without constant reinvention. In that sense, the QMS becomes a real competitive advantage: it saves time, resources and money over the long term and strengthens the organisation's position and reputation. An investment that is very likely to pay off.

**References**

[41] FDA. (2025, November 20). Quality Management System Regulation: Final Rule Amending the Quality System Regulation – Frequently Asked Questions. Retrieved from https://www.fda.gov/medical-devices/quality-system-qs-regulationmedical-device-current-good-manufacturing-practices-cgmp/quality-management-system-regulation-final-rule-amending-quality-system-regulation-frequently-asked

[42] Oxford University Press. (2025, January 10). How can ISO 13485 standards transform quality, safety, and organizational excellence? International Journal for Quality in Health Care. Retrieved from https://academic.oup.com/intqhc/advance-article/doi/10.1093/intqhc/mzaf032/8102172

**Author | Anne Arndt CEO**
Elevate Med Tech New Zealand Limited

+64 (0) 20 4183 1943
anne.arndt@elevate-med.tech

Qb Studios | 235 High Street.
Christchurch CBD 8011
New Zealand

www.elevate-med.tech