C-SUITE EXECUTIVE FIELD GUIDE

Developing and Manufacturing Medical Devices

A practical guide for C-suite executives

From strategy, governance and investment to evidence-based decisions, market responsibility and patient safety

General cross-market guidance | Edition 1.0 | August 2026

Table of Contents

How to use this guide

This guide explains what the C-suite must understand and govern in an organisation that develops, manufactures, distributes or maintains medical devices. It is intended for chief executives and leaders responsible for operations, finance, technology, quality, regulatory affairs, commercial performance, people and information security. It translates regulated-product obligations into executive decisions about strategy, resources, evidence, accountability and risk.

> **CORE MESSAGE** Executive leadership is part of the medical-device control system. The C-suite establishes priorities, resources, authority and culture—and remains accountable for decisions that influence patient safety, product quality and regulatory compliance.

Scope and important limitations

- Use this guide to frame executive questions, governance and investment decisions rather than to replace specialist technical or legal assessment.
- Apply current legislation, market requirements, standards and company procedures to the actual device and jurisdictions.
- Require clear evidence from quality, regulatory, clinical, engineering, manufacturing, cybersecurity and commercial leaders.
- Distinguish informed risk acceptance from unsupported optimism, schedule pressure or retrospective justification.
- Escalate potential patient harm, serious noncompliance, data-integrity concerns and mandatory reporting without delay.

1. Why executive leadership matters

Medical-device organisations convert investment and technical capability into products that can affect diagnosis, treatment and patient wellbeing. Executive choices about schedule, staffing, suppliers, markets, evidence and culture determine whether the organisation can meet its obligations reliably.

Connect executive decisions to regulated outcomes

Executive decision	Possible product or compliance impact
Portfolio commitment	A launch date or feature commitment can exceed the time needed to generate adequate safety and performance evidence.
Resource allocation	Insufficient specialist, verification, manufacturing or post-market capacity can create systemic quality gaps.
Operating model	Unclear ownership or excessive outsourcing can weaken accountability, knowledge and evidence access.
Market entry	Entering a new jurisdiction can create additional classification, registration, privacy and support obligations.
Cost reduction	Supplier, staffing or control reductions can remove safeguards and increase lifecycle exposure.
Leadership behaviour	Pressure to hide failures or soften evidence can damage patient safety, culture and regulatory credibility.

Define the executive contribution realistically

Executives do not personally perform every design review, test or regulatory submission. They ensure that competent people own the work, sufficient resources and independence exist, evidence reaches decision-makers and unresolved risks are not concealed by commercial enthusiasm.

2. Understand the medical-device business model

The regulated business model includes more than selling product. It encompasses development, market authorisation, controlled manufacture, distribution, customer support, complaints, cybersecurity maintenance, regulatory updates and eventual product retirement.

Recognise lifecycle commitments

Lifecycle stage	Executive commitment
Concept and feasibility	A credible clinical need, strategic fit, regulatory route, technical feasibility and funding envelope.
Design and development	Competent multidisciplinary teams, controlled requirements, risk management and objective evidence.

Lifecycle stage	Executive commitment
Verification and validation	Independent challenge, representative testing, clinical or usability evidence and resolution of failures.
Manufacturing transfer	Qualified suppliers, capable processes, trained people, traceability and production readiness.
Launch and market access	Approved claims, registrations, distribution controls, customer support and launch readiness.
Post-market lifecycle	Complaints, vigilance, security updates, CAPA, service, continuity and responsible product retirement.

Avoid a launch-only financial model

Revenue projections should include the cost of maintaining evidence, monitoring safety, supporting installed products, addressing vulnerabilities, managing suppliers and complying with changes in regulation throughout the product lifetime.

3. Regulatory and quality-system foundations

The quality-management system is the organisation's operating model for consistently meeting product and regulatory requirements. It should connect responsibilities, processes, decisions and records rather than operate as a parallel documentation function owned only by quality assurance.

What effective executive oversight looks like

- Management understands which entities are legal manufacturers and which markets and product classes are involved.
- Quality-system processes have accountable owners, appropriate authority and sufficient resources.
- Management review uses evidence about quality objectives, audits, complaints, CAPA, suppliers and product risk.
- Important regulatory obligations and deadlines are visible in portfolio and financial planning.
- Independent quality and regulatory escalation can reach senior leadership without commercial filtering.
- Executive commitments to regulators, customers and notified bodies are realistic and tracked to completion.

Keep accountability with the manufacturer

Outsourcing design, software, manufacturing, sterilisation, testing or distribution does not remove the manufacturer's responsibility to define requirements, oversee performance and retain access to necessary evidence.

4. Governance, roles and decision rights

Good governance identifies who recommends, challenges, decides and executes. Product decisions become fragile when project authority, technical authority, quality oversight and commercial ownership are confused.

Establish clear decision architecture

- Name accountable executives for product, quality, regulatory, technology, operations, security and post-market performance.
- Define approval authorities for development milestones, risk acceptance, market release, major changes and field actions.
- Protect independence for quality, clinical, safety, verification and regulatory judgement.
- Assign deputies and escalation routes for critical responsibilities and time-sensitive decisions.
- Clarify responsibilities across subsidiaries, shared services, suppliers, partners and international markets.
- Record the evidence, dissent, conditions and rationale behind significant decisions.

Separate decision authority from seniority

A senior commercial or project title does not automatically confer competence to approve a safety conclusion, clinical claim, software classification or regulatory submission.

5. Product strategy and portfolio governance

Portfolio governance should connect clinical value, customer need, evidence, regulatory feasibility, technical risk, supply capability and lifecycle cost. A strategically attractive product can still be an unsound investment if essential evidence or operating capability is missing.

Use evidence-based portfolio questions

- What unmet need and intended purpose are being addressed, and how will benefit be demonstrated?
- Which markets, classifications and regulatory pathways shape development time and evidence?
- What are the principal safety, usability, cybersecurity, clinical and manufacturing uncertainties?
- Which scarce capabilities, suppliers, technologies or datasets create strategic dependencies?
- What post-launch support, surveillance, service, security and product-retirement commitments follow?
- Which assumptions would make the business case invalid if they prove false?

Fund uncertainty reduction before scale

Early investment should resolve the assumptions most likely to invalidate safety, feasibility, market access or economics. Scaling a programme before these questions are answered compounds cost and commitment.

6. Intended purpose, claims and market choice

Intended purpose shapes whether a product is a medical device, how it is classified, what evidence is needed and which claims may be made. Market, user, patient population and use environment decisions therefore belong in executive strategy as well as regulatory documentation.

Align promise, evidence and operating capability

- Define the clinical or diagnostic purpose, intended users, patient population and use environment.
- Ensure approved claims are consistent across submissions, labels, contracts, websites and sales materials.
- Understand how new features, artificial intelligence, connectivity or accessories may change regulatory scope.
- Assess whether service, training, distribution and customer support can sustain the promised use.
- Review the cost and timing of market-specific evidence, registration, language and post-market obligations.

- Prevent sales commitments that extend intended use beyond available evidence or approvals.

Treat claim expansion as a product decision

A broader claim can change classification, risk, evidence needs and liability exposure. It should not enter the market through marketing language before the organisation has approved the underlying product strategy.

7. Resource planning and organisational capability

Quality-system effectiveness depends on competent people, appropriate infrastructure and enough capacity to perform, review and support the work. Resource shortages are executive risks when they affect safety evidence, independence or lifecycle obligations.

Build a capability model, not only a headcount plan

- Identify critical disciplines across systems, engineering, software, verification, clinical, usability, quality, regulatory and manufacturing.
- Quantify review, approval, investigation, supplier oversight and post-market effort as well as direct project work.
- Recognise scarce expertise, single points of failure, succession needs and excessive contractor dependency.
- Fund laboratories, tools, cybersecurity monitoring, quality systems and controlled infrastructure.
- Assess capability impact before reorganisations, acquisitions, outsourcing or headcount reduction.
- Track vacancies, competence gaps, workload and delayed quality activities as business risks.

Challenge apparent efficiency that removes control

Reducing independent review, verification capacity or product-support teams may improve a short-term cost metric while increasing failure, delay, audit and field-action exposure.

8. Quality culture and psychological safety

Culture determines whether people report failed tests, question unsupported assumptions and stop unsafe work. The behaviour of senior leaders is often more influential than the wording of the quality policy.

Demonstrate the culture expected

- Ask for evidence, uncertainty and risk rather than only schedule and favourable conclusions.
- Thank people who raise concerns and protect them from retaliation or reputational penalty.
- Do not demand that technical teams change conclusions to fit commercial preferences.
- Treat deviations, complaints and near misses as learning inputs rather than individual embarrassment.
- Support independent quality, regulatory and safety escalation when programmes are under pressure.
- Act consistently when leaders backdate records, bypass controls or conceal adverse information.

Listen for organisational silence

A project reporting no failures, disagreements or uncertainty may be exceptionally capable—or may have learned that bad news is unwelcome. Executives should test which explanation is true.

9. Product risk and executive risk acceptance

Product-risk management identifies hazards, implements controls and evaluates residual risk. Executive involvement is required where risk policy, business decisions, unresolved severe hazards or benefit-risk conclusions require management authority.

Make risk acceptance evidence-based

- Approve a risk-management policy with clear, consistent risk-acceptability criteria.
- Require the team to identify foreseeable harms, vulnerable users, misuse and lifecycle dependencies.
- Confirm that risk controls are implemented, verified and connected to requirements and production controls.

- Understand the severity and uncertainty behind aggregated risk summaries.
- Ensure new complaints, supplier issues and cybersecurity information update product-risk conclusions.
- Document residual-risk and benefit-risk decisions without rewriting technical evidence to make it comfortable.

Do not convert schedule pressure into risk tolerance

A delayed launch may be commercially painful, but it does not alter the severity of harm or prove that an unverified control works. Risk criteria should remain stable when programme pressure rises.

10. Development planning and design controls

Design controls create a disciplined chain from user needs and intended purpose through requirements, architecture, implementation, verification, validation and controlled change. Executive governance should make completion of this evidence a condition of progression.

Ask whether the development system is coherent

- Are user needs and product requirements clear, testable and consistent with intended purpose?
- Does the architecture allocate functions, safety controls, interfaces and cybersecurity responsibilities?
- Are risks connected to design requirements and objective verification evidence?
- Are reviews independent enough to challenge assumptions and unresolved failures?
- Can the organisation identify the approved product configuration and reproduce its evidence?
- Are open issues visible, owned and assessed before each milestone?

Avoid documentation after the decision

Creating plans, requirements or approvals retrospectively weakens both product control and credibility. Evidence should guide the decision rather than be reconstructed to justify it.

11. Evidence-based milestone decisions

A milestone is a management decision about readiness, not a presentation event. The decision should reflect defined entrance and exit criteria, objective evidence, open risks and the organisation's ability to execute the next stage.

Structure a defensible milestone review

1. **Define the decision.** State what authority is being requested and which lifecycle transition it enables.
2. **Review required evidence.** Compare actual deliverables with approved criteria, plans and product-risk needs.
3. **Expose uncertainty.** Identify failures, missing evidence, assumptions, dependencies and conflicting conclusions.
4. **Assess consequences.** Consider patient, regulatory, technical, supply, financial and schedule implications.
5. **Decide with conditions.** Approve, reject or conditionally approve with named actions, owners and limits.
6. **Record and follow through.** Preserve the rationale and prevent incomplete actions from disappearing after the meeting.

Reject traffic-light governance without evidence

A green status should mean that defined criteria are satisfied, not that the project manager believes recovery is possible. Executives should ask what evidence and assumptions produce the colour.

12. Verification, validation and release readiness

Verification asks whether the product was built correctly against requirements; validation asks whether the resulting device meets user and intended-use needs. Release readiness also requires manufacturing, regulatory, supplier and support evidence.

Require a complete readiness picture

- Approved requirements, risk controls and traceability to objective test evidence.
- Representative product configurations, justified samples and resolved test anomalies.
- Appropriate usability, clinical, performance and cybersecurity evidence.

- Qualified suppliers, validated processes, trained personnel and controlled manufacturing records.
- Approved labelling, registrations, distribution controls and customer-support arrangements.
- A clear account of residual risks, unresolved actions and post-launch monitoring commitments.

Treat failed tests as information

Failures reveal product or process knowledge. Repeating a test without understanding the failure can create a favourable result without demonstrating that the underlying problem has been controlled.

13. Manufacturing and supply-chain resilience

A conforming design must be manufactured repeatedly using approved materials, capable processes and controlled suppliers. Supply continuity is an executive concern where shortages, obsolescence or supplier failure threaten patient availability or force risky substitutions.

Govern production and supply risk

- Identify critical suppliers, sole sources, custom components, special processes and long-lead materials.
- Require qualification, quality agreements, change notification, monitoring and traceability proportionate to risk.
- Fund equipment qualification, process validation, calibration, maintenance and contamination control.
- Monitor yield, scrap, rework, supplier defects and unauthorised process adjustments.
- Plan approved alternatives, strategic stock, obsolescence response and business continuity.
- Prevent emergency sourcing or component substitution without technical and regulatory assessment.

Measure total cost of quality

A cheaper component or supplier may increase inspection, scrap, investigation, revalidation and field-failure costs. Executive sourcing decisions should consider lifecycle exposure, not only purchase price.

14. Software, cybersecurity and digital dependency

Connected devices, cloud services, mobile applications, software components and production systems create continuing obligations after launch. Cybersecurity can affect both information and patient safety, while third-party digital services can become critical operational dependencies.

Establish executive digital accountability

- Identify safety-relevant software, connected interfaces, cloud services and sensitive data flows.
- Fund secure development, independent verification, vulnerability monitoring and controlled updating.
- Define ownership for security incidents, regulatory reporting, customer communication and remediation.
- Require supplier transparency, software inventories, supported lifetimes and exit arrangements.
- Monitor legacy systems, unsupported components, patch performance and unresolved vulnerabilities.
- Include service outages, data loss and cyberattack scenarios in business-continuity and crisis exercises.

Do not treat cybersecurity as an IT-only risk

A security failure can alter therapy, delay diagnosis, disable a service or prevent safe product use. Product, quality, regulatory and clinical leaders must share ownership with information-security specialists.

15. Artificial intelligence and data strategy

Artificial intelligence may create value through diagnosis, decision support, automation or operational insight, but it also introduces dependencies on data quality, model performance, human oversight, supplier behaviour and evolving regulation.

Govern AI as a product capability

- Define the intended purpose, decision role, user oversight and consequences of incorrect output.
- Understand training-data rights, provenance, representativeness, bias and performance limitations.

- Require validation, change control, monitoring and clear responsibility for model updates.
- Assess the interaction between medical-device, privacy, cybersecurity, AI and product-liability requirements.
- Control claims about autonomy, accuracy and continuous learning against approved evidence.
- Plan for supplier failure, model drift, service withdrawal and the ability to support affected users.

Avoid AI strategy by demonstration

An impressive prototype does not demonstrate clinical validity, generalisable performance, safe human interaction or regulatory feasibility. Investment gates should be tied to those questions.

16. Clinical evidence, usability and patient focus

Medical-device value depends on evidence that the product is safe, performs as intended and can be used effectively by the intended population. Clinical and usability evidence should be planned as core product work rather than as late submission packaging.

Ask whether the patient proposition is demonstrated

- Is the clinical or diagnostic benefit clear, relevant and supported by an appropriate evidence strategy?
- Does evaluation cover intended users, vulnerable populations, foreseeable misuse and realistic environments?
- Are human-factors findings translated into design changes and verified risk controls?
- Are residual limitations communicated accurately in labels, training and commercial materials?
- Can the organisation sustain required clinical or performance evaluation after launch?
- Are study ethics, participant safety, data integrity and publication responsibilities appropriately governed?

Keep patient value visible in commercial decisions

Features, claims and launch priorities should be tested against the actual clinical need and risks rather than only competitor comparison or sales appeal.

17. Market access and regulatory strategy

Regulatory strategy converts intended purpose, classification, evidence and business sequencing into a credible route to each market. It affects design, clinical evidence, labelling, manufacturing, local representation and post-market support.

Integrate regulatory strategy with the business plan

- Identify target jurisdictions, device classification, conformity route and external-review dependencies.
- Understand submission evidence, testing, fees, translation, registration and lead-time assumptions.
- Sequence market entry based on product readiness and operational ability to maintain compliance.
- Plan economic-operator, importer, distributor and local-support arrangements.
- Monitor regulatory change and its effect on current products, pipeline and technical documentation.
- Avoid making customer commitments before the regulatory pathway and evidence are credible.

Treat market expansion as operational expansion

A new registration can create obligations for vigilance, language, distribution, privacy, cybersecurity and local authority cooperation. Approval cost is only part of the lifecycle commitment.

18. Commercial conduct and evidence-based claims

Commercial teams translate product capability into customer expectations. Executive leadership must ensure that growth incentives do not encourage off-label promotion, unsupported comparison, inappropriate healthcare-professional influence or commitments the product cannot meet.

Align incentives with responsible growth

- Require coordinated regulatory, clinical, technical and legal review of significant claims.
- Ensure sales materials, demonstrations, tenders and contracts match approved intended purpose.

- Control statements about accuracy, safety, autonomy, interoperability, security and service availability.
- Manage interactions with healthcare professionals, distributors and public purchasers ethically.
- Monitor complaints and customer feedback for signs that promotion creates foreseeable misuse.
- Avoid rewarding revenue that depends on unapproved markets, claims or product configurations.

Do not let disclaimer text carry the strategy

Small-print limitations cannot reliably correct a prominent unsupported promise. The overall customer proposition should be accurate and consistent with the evidence.

19. Post-market surveillance and lifecycle management

After launch, the organisation must learn from complaints, incidents, service records, literature, cybersecurity intelligence and real-world performance. Executives should ensure that this information changes priorities and decisions when necessary.

Maintain active post-market oversight

- Track serious incidents, complaint trends, recurring defects and emerging patient-safety signals.
- Monitor CAPA progress, field actions, supplier investigations and effectiveness of corrective measures.
- Review cybersecurity vulnerabilities, patch status, unsupported components and customer uptake of updates.
- Ensure clinical or performance evidence remains current for the marketed product and claims.
- Fund product maintenance, service, spare parts and responsible end-of-life communication.
- Escalate information that changes the benefit-risk conclusion or market suitability.

Avoid starving mature products of support

Older products may generate less growth but can have the largest installed base and greatest accumulated exposure. Lifecycle support should reflect patient and regulatory obligations, not only new-project excitement.

20. Complaints, incidents and field actions

A serious complaint or safety signal tests both operational capability and leadership judgement. The organisation must protect patients, preserve evidence, assess reporting obligations and communicate accurately under time pressure.

Lead a disciplined safety response

- Establish the facts, affected product, potential harm, distribution scope and immediate containment.
- Mobilise quality, regulatory, clinical, engineering, legal, cybersecurity and communications expertise.
- Preserve devices, logs, records and supplier evidence without obstructing urgent corrective action.
- Meet applicable reporting and authority-cooperation requirements in each market.
- Decide field action using patient risk and effectiveness rather than reputational preference.
- Track customer communication, completion, effectiveness and lessons for the wider system.

Avoid negotiating the vocabulary before acting

Whether an action is ultimately called a correction, recall or field safety corrective action depends on facts and jurisdiction. Terminology debate must not delay effective risk reduction.

21. Financial planning, reserves and insurance

Regulated-product finance should account for development evidence, market access, quality infrastructure and long-tail lifecycle exposure. Short-term budget optimisation can create larger costs through delay, remediation, recall or loss of market access.

Make hidden quality costs visible

- Fund verification, validation, clinical evidence, supplier qualification and regulatory submissions realistically.
- Recognise costs of scrap, rework, investigation, delayed launch, audit remediation and field action.
- Plan reserves and contingency for technical uncertainty, supply disruption and regulatory change.

- Review product-liability, clinical-study, cyber, recall and business-interruption insurance.
- Understand exclusions, territorial scope, notification requirements and limits of supplier indemnities.
- Avoid financial targets that reward shipment before evidence or release requirements are satisfied.

Treat quality investment as business infrastructure

Quality systems, laboratories, security monitoring and competent reviewers are not optional overhead when they enable market access and protect the organisation's licence to operate.

22. Partnerships, acquisitions and due diligence

Strategic transactions can import product liability, quality-system weaknesses, unsupported claims, software dependencies and post-market commitments. Executive diligence should test the evidence behind certificates and management assurances.

Examine regulated-product fundamentals

- Confirm legal manufacturer roles, product classifications, registrations and target-market status.
- Review quality-system maturity, audit findings, CAPA, complaints, field actions and regulator correspondence.
- Assess intended purpose, clinical evidence, risk management and product-development traceability.
- Identify critical suppliers, source-code access, intellectual-property rights and technical knowledge dependencies.
- Review privacy, cybersecurity, AI, software licensing, product liability and insurance exposure.
- Assess the resources and time required to integrate, remediate or separate the regulated operation.

Avoid valuation based on unverified pipeline claims

A promising product has less value if its evidence cannot support registration, its manufacturer lacks technical access or substantial remediation is required before safe launch.

23. Organisational change and business continuity

Reorganisation, outsourcing, leadership departure, site closure and cost reduction can change process ownership, independence, competence and product support. These changes should be assessed like other significant business risks before implementation.

Protect regulated capability through change

- Identify affected process owners, technical authorities, authorised approvers and regulatory responsibilities.
- Assess competence, workload, independence, succession and loss of product-specific knowledge.
- Maintain access to records, source code, facilities, suppliers and external service arrangements.
- Plan continuity for complaints, vigilance, cybersecurity, servicing and field actions.
- Update procedures, organisational records, training and authority assignments promptly.
- Test business-continuity and crisis arrangements using realistic product and supply scenarios.

Do not assume duties disappear with the team

Closing a project or department does not end obligations associated with marketed devices. Ownership and resources must transfer explicitly.

24. Management review and executive metrics

Executive metrics should reveal capability, risk and system health. Completion percentages and aggregated traffic lights can hide severe individual issues, weak evidence and overdue patient-safety actions.

Use a balanced executive dashboard

Decision area	Illustrative leading and outcome indicators
Product risk	Unresolved severe hazards, overdue controls, new safety signals and benefit-risk changes.
Development evidence	Milestone criteria met, critical test failures, traceability gaps and aged open actions.

Decision area	Illustrative leading and outcome indicators
Quality system	Audit themes, CAPA effectiveness, overdue investigations and recurring deviations.
Supply and production	Critical supplier exposure, process capability, yield, rework, obsolescence and continuity risk.
Post-market	Serious complaints, reporting timeliness, field actions, patch adoption and investigation ageing.
People and culture	Critical vacancies, workload, competence gaps, turnover and evidence of suppressed escalation.
Regulatory and market	Submission status, commitments, expiring approvals and emerging legislative impact.
Financial exposure	Cost of poor quality, remediation forecast, recall reserve and uninsured or concentrated risk.

Ask what the aggregate conceals

A high training-completion percentage, good overall yield or low complaint rate can coexist with one missing critical competence, a severe recurring defect or an unreported safety event.

25. Crisis leadership and external communication

A product crisis requires rapid patient protection, accurate facts, clear authority and disciplined communication. Executive leadership should prepare before an incident rather than inventing roles under public and regulatory pressure.

Prepare the executive response system

- Define crisis leadership, technical decision authority, regulatory contacts and board escalation.
- Maintain access to product, distribution, customer, supplier and technical evidence.
- Exercise scenarios involving patient harm, cybersecurity, contamination, supplier failure and service outage.
- Separate verified facts, working assumptions and unknowns in internal and external communication.

- Coordinate regulators, customers, healthcare professionals, insurers, partners and the media.
- Capture decisions and complete a lessons-learned review after immediate risk is controlled.

Communicate uncertainty honestly

Early facts may be incomplete. Credibility is protected by stating what is known, what is being investigated and what protective action is under way—not by offering premature reassurance.

26. Executive evidence and audit readiness

Auditors and regulators may test whether management understands the quality system, provides adequate resources and acts on significant information. Executive evidence should arise from routine governance rather than last-minute preparation.

Maintain an audit-ready governance set

Evidence	Question it answers
Strategy and responsibility map	Which products, markets, legal entities and executives own regulated obligations?
Management-review records	Did leaders receive meaningful quality, risk, resource and post-market information?
Portfolio and milestone decisions	Were development transitions approved against evidence and defined criteria?
Resource and capability plans	Were competent people, infrastructure, independence and lifecycle support provided?
Risk and escalation records	How were severe hazards, dissent, uncertainty and emerging safety signals managed?
Regulatory commitments	Are authority, notified-body and customer commitments visible, owned and completed?
Crisis and continuity evidence	Can the organisation respond to field action, cyberattack, supplier failure or product interruption?

Answer from the operating system

Executive confidence is credible when routine records show consistent attention, action and follow-through. A polished presentation cannot replace missing ownership or unresolved evidence.

27. Executive review at every major decision

The C-suite should ask a consistent set of questions whenever it authorises significant investment, market entry, release, acquisition, outsourcing, cost reduction or lifecycle change.

Recognise common executive failure patterns

Failure pattern	More effective response
A date is committed before the evidence plan is credible.	Use ranges and explicit assumptions until regulatory, clinical and technical uncertainty is reduced.
Quality is delegated entirely to the quality department.	Make process owners and executives accountable for the effectiveness of regulated work.
Red status is treated as poor project behaviour.	Reward early escalation and ask what support or decision is required.
Launch is approved with unresolved critical evidence.	Apply defined gate criteria and record any tightly controlled conditions or refusal.
Mature products lose maintenance funding.	Plan support according to installed-base, safety, security and regulatory obligations.
Cost reduction removes specialist independence.	Assess quality, patient and lifecycle consequences before implementing organisational change.

Questions every executive should ask

- What patient or user outcome does this product decision affect?
- What objective evidence supports the recommendation, and what remains unknown?
- Which severe risks, dissenting views or failed assumptions are hidden by the summary?
- Do accountable teams have the competence, capacity, independence and authority to succeed?

- What obligations continue after launch, sale, outsourcing, reorganisation or product retirement?
- Would we be comfortable explaining this decision to patients, employees, regulators and the board?

PRACTICAL RULE Set direction, fund capability, demand evidence, protect escalation and act when patient safety or regulatory integrity is at risk.

Appendix A. Executive deliverables by lifecycle stage

Lifecycle stage	Representative executive outputs
Concept and feasibility	Strategic fit, intended-purpose alignment, funding envelope and evidence-based continuation criteria.
Design and development	Accountable leadership, capability plan, approved risk policy and milestone governance.
Verification and validation	Independent challenge, evidence-readiness review and resolution of critical failures.
Manufacturing transfer	Production-readiness decision, supply assurance and validated-process oversight.
Market launch	Market-authorisation, claims, distribution, support and launch-readiness decision.
Post-market lifecycle	Management review, safety-signal response, CAPA oversight and funded lifecycle support.
Change or retirement	Impact assessment, continuity plan, customer communication and transfer of remaining obligations.

Appendix B. Essential C-suite review checklist

Review area	Minimum executive question
Purpose and market	Is intended purpose clear and is the regulatory and commercial pathway credible?
Accountability	Are decision rights, process ownership, independence and escalation routes explicit?

Review area	Minimum executive question
Evidence	Do requirements, risks, verification, validation and clinical evidence support the decision?
Resources	Are competent people, tools, suppliers and lifecycle funding realistically available?
Manufacture and supply	Can the approved design be built consistently with resilient, controlled supply?
Digital and security	Are software, data, cloud, AI and cybersecurity dependencies governed throughout life?
Launch	Are regulatory, production, labelling, distribution and customer-support controls ready?
Post-market	Can complaints, incidents, updates, field actions and ongoing evidence be managed?
Culture	Can people challenge, stop and escalate without pressure to conceal unwelcome evidence?
Decision integrity	Are uncertainty, conditions, dissent and follow-up actions recorded and controlled?

Appendix C. Commonly relevant standards and frameworks

This is an orientation list. Applicability, current editions, transition provisions and jurisdiction-specific requirements should be confirmed by competent specialists.

Topic	Common reference	Executive relevance
Quality management	ISO 13485:2016; US 21 CFR Part 820 QMSR	Management responsibility, resources, quality-system effectiveness and evidence of controlled operations.
Risk management	ISO 14971:2019; ISO/TR 24971:2020	Risk policy, accountability, product-risk decisions and lifecycle feedback.
EU medical devices	Regulation (EU) 2017/745; Regulation (EU) 2017/746	Manufacturer obligations, market access, economic operators, vigilance and lifecycle duties.
Software lifecycle	IEC 62304, where applicable	Software governance, lifecycle capability, evidence and maintenance commitments.

Topic	Common reference	Executive relevance
Cybersecurity	IEC 81001-5-1; applicable FDA guidance	Secure development, vulnerability response, updateability and executive incident oversight.
Usability engineering	IEC 62366-1, where applicable	Safe user interaction, intended users, foreseeable misuse and human-factors evidence.
Electrical safety	IEC 60601 series, where applicable	Essential performance, safety evidence, production controls and continued conformity.
Artificial intelligence	Regulation (EU) 2024/1689, where applicable	AI accountability, evidence, oversight, data strategy and regulatory interaction.
Product liability	Applicable national law; Directive (EU) 2024/2853 transition	Defective products, software, economic exposure and evidence supporting defensible decisions.

Appendix D. Glossary

Term	Meaning in this guide
Benefit-risk	A reasoned comparison of expected clinical or user benefit with residual product risk.
CAPA	Corrective and preventive action addressing causes of actual or potential systemic problems.
Design control	The managed lifecycle connecting needs, requirements, design, risk, verification, validation and change.
Economic operator	A manufacturer, authorised representative, importer, distributor or other party with defined market duties.
Intended purpose	The use intended by the manufacturer as expressed through approved product information and claims.
Management review	Structured senior-management evaluation of quality-system suitability, adequacy and effectiveness.
Residual risk	Risk remaining after applicable risk-control measures have been implemented.

Term	Meaning in this guide
Validation	Objective evidence that the resulting product or process meets its intended use or application.
Verification	Objective evidence that specified requirements have been fulfilled.
Vigilance	Assessment and reporting of defined safety events and field actions under applicable device law.

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
- FDA — Quality Management System Regulation
- FDA — Quality Management System Regulation: Frequently Asked Questions
- European Union — Regulation (EU) 2017/745 on medical devices
- European Union — Regulation (EU) 2017/746 on in vitro diagnostic devices
- European Union — Regulation (EU) 2024/1689, Artificial Intelligence Act
- European Union — Directive (EU) 2024/2853, Product Liability Directive
- European Commission — MDCG endorsed documents and other guidance

CONTROLLED USE Consult current legislation, company procedures and qualified quality, regulatory, legal and technical specialists before applying this guide to a specific executive decision.