Congenius

mdeg
we do medtech!

Whitepaper

How to integrate an ISMS into your existing QMS

May 2025

By Jörg Dogwiler & Daniel Ziegelmayer

The importance of an effective ISMS in MedTech

Information security is not just an IT issue – it's fundamental to patient safety. MedTech companies handle sensitive product data, patient information, intellectual property, and regulatory documentation. A single data breach can jeopardise trust, compliance, and business continuity.

An Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2022 provides a risk-based framework for the systematic identification, evaluation, and control of information security risks. Importantly, ISO 27001 follows the same structure as ISO 13485, enabling easy integration into your existing QMS. If you already operate a QMS under ISO 13485, you've done much of the groundwork. This whitepaper demonstrates how to leverage what you already have - and how to build what's missing, with minimal friction.

Read on to discover how to implement an ISMS according to ISO/IEC 27001 and seamlessly integrate it into your existing ISO 13485 QMS.

Step 1 | Educate on the value of an ISMS

An ISMS is about more than cybersecurity – it provides structured, proactive business protection.

Communicating the necessity of an ISMS to your organisation and winning employee buy-in is a crucial first step in the process. To help facilitate the conversation:

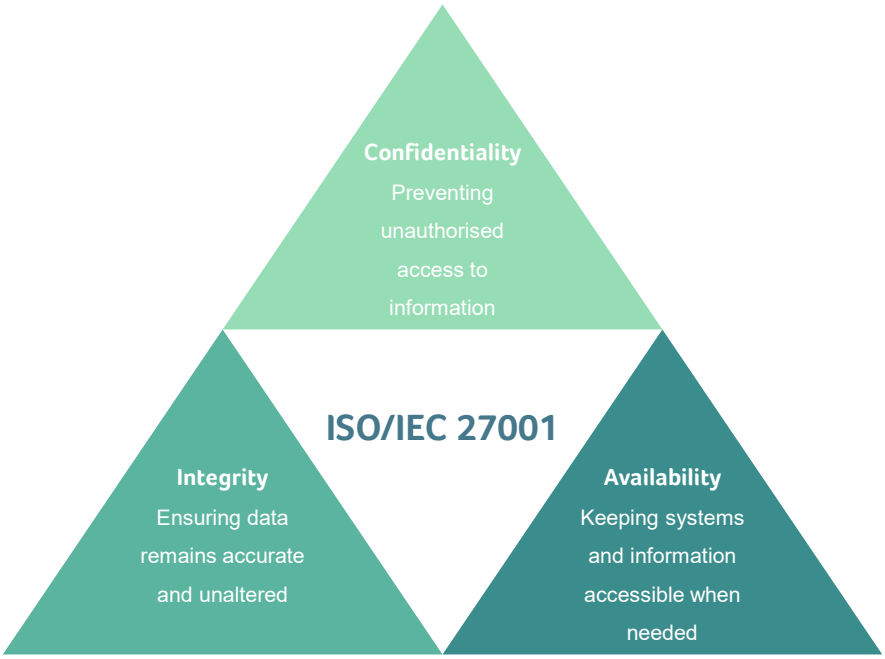
Position the ISMS as a **quality and business enabler**, not just an IT compliance task.

Link security to **real MedTech scenarios** (e.g. protecting clinical data, ensuring availability of devices).

Start with a **short internal kick-off** workshop to align stakeholders and clarify the business value.

Step 2 | Know the core principles of ISO/IEC 27001

ISO/IEC 27001 is centred within the triad of confidentiality, integrity, and availability:



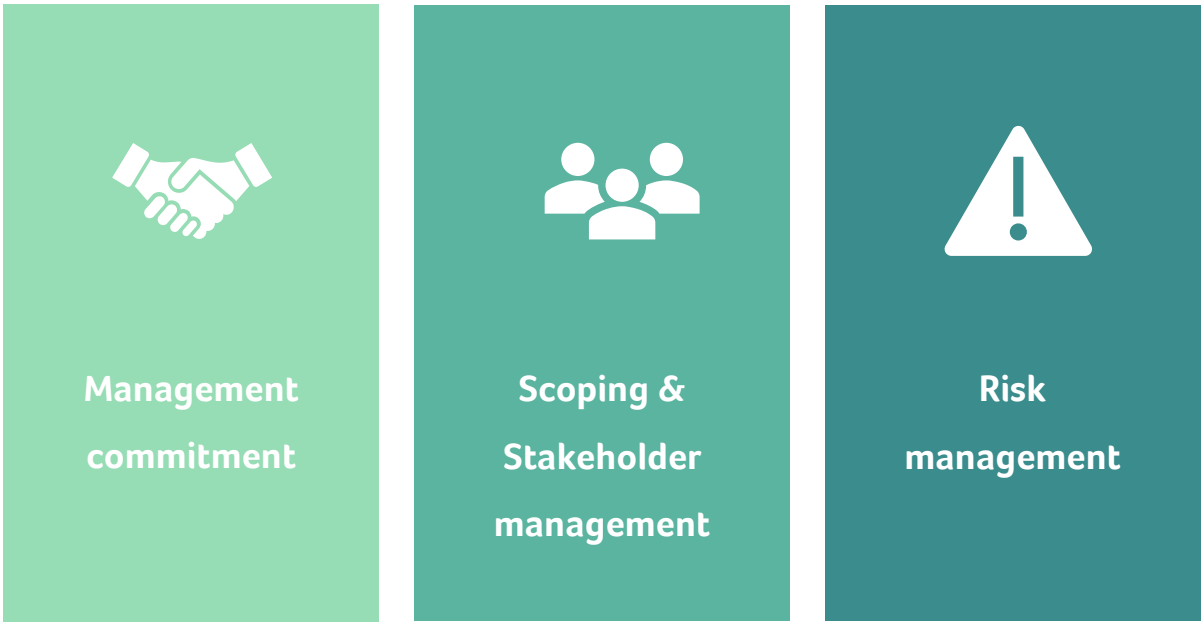
It's built upon the High-Level Structure (HLS), enabling alignment with ISO 13485. ISO 27001 requires organisations to define their security objectives, understand internal and external context, evaluate risks, and implement appropriate controls (as per Annex A) - supported by regular review and continuous improvement.

Implementation tips

- ✓ Create a one-page "ISMS Overview Map" to visualise how the standard's key components link to your business
- ✓ Highlight overlapping areas like document control, training, internal audits, and management review
- ✓ Use your map to brief executives, auditors, and employees to make the system more tangible and less abstract
- ✓ Display the map in your meeting rooms or on your quality dashboard

Step 3 | Implementation strategy

Your implementation strategy involves three key aspects:



The following pages dive deeper into these three areas, including some tips for practical action to take.

Step 3 | Implementation strategy

Management commitment

ISO 27001 requires clear leadership engagement (as per Clause 5). As such, management must define security objectives, assign roles and responsibilities, and provide sufficient resources. This means:

- **Aligning** the ISMS with the business and product strategy
- **Defining** specific, measurable information security goals
- **Allocating** budget and skilled people
- **Supporting** integration with the QMS and day-to-day operations

Leadership must lead by example - not just sign policies, and security must be visible in decision-making.

Implementation tips

✓ Have top management record a 2-minute video message on why security matters - then screen it in all-hands meetings and onboarding activities

✓ Define “Security KPIs” that link to business outcomes (e.g. zero data loss in product development, 100% incident response rate)

✓ Assign an executive sponsor for the ISMS to drive visibility and decision power

Step 3 | Implementation strategy

Scoping & Stakeholder management

Before you build anything, you need to know what you're securing and for whom. ISO 27001 requires you to understand:

- Your internal and external environment (technology, legal, customer expectations)
- The relevant stakeholders (regulators, patients, partners, service providers)
- What these stakeholders expect from you regarding information security

This lays the foundation for setting the scope of your ISMS. In MedTech, this usually covers R&D, production, clinical trials, supplier systems, regulatory data, and the maintenance of digital systems or infrastructure for connected devices on the market.

Implementation tips

✓ Use a whiteboard session to map out your key processes, stakeholders, and information flows - this creates early buy-in and awareness

✓ Turn this mapping into a simple "ISMS Scope Document" with clear boundaries (systems, teams, countries)

✓ Align this with your existing QMS scope to simplify audits

Step 3 | Implementation strategy

Risk management

Risk management is the engine of your ISMS, allowing you to identify where something could go wrong, how bad it would be, and what to do about it. Key steps include:

- **Identifying** key information assets (e.g. technical files, source code, cloud systems, patient data, IP)
- **Analysing** potential threats and vulnerabilities
- **Rating** risks based on likelihood and impact
- **Deciding** on risk treatment options, i.e. reduce, accept, transfer, or avoid
- **Assigning** risk owners and tracking treatment actions

Ideally, use the same structure or tool you already use for ISO 13485 and ISO 14971 product risks.

Implementation tips

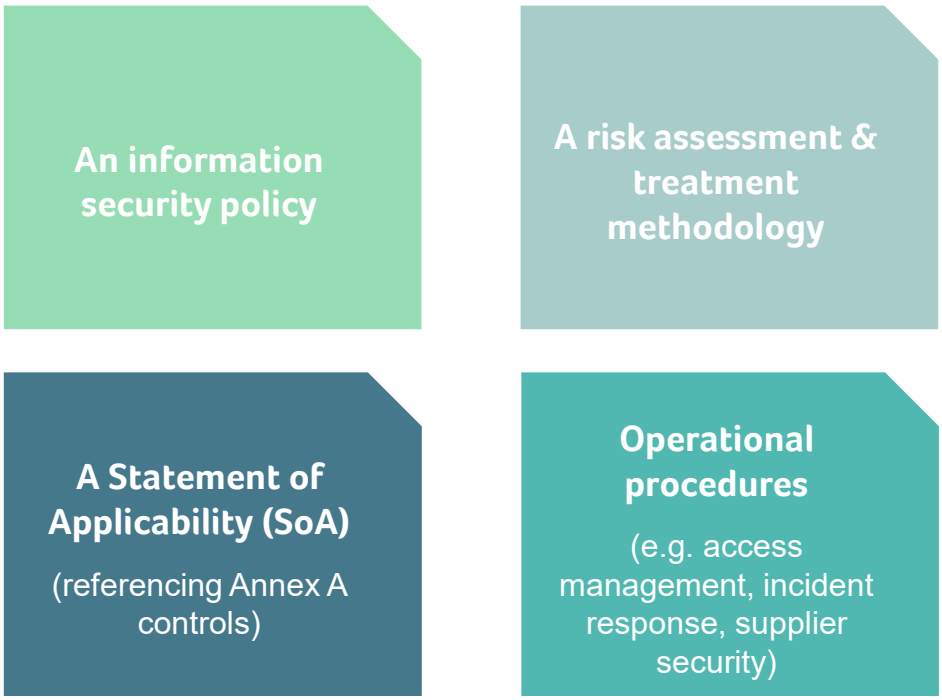
✓ Use existing templates (e.g. FMEA) to identify and score ISMS-related risks

✓ Keep it simple: focus on your top 10-15 information assets first (e.g. source code, DHFs, patient data)

✓ Use real-life past incidents or industry examples to reinforce relevance

Step 4 | Establish ISMS policies & procedures

A robust ISMS requires structured documentation. According to Clause 7.5, you must maintain:



The level of documentation can reflect your existing QMS structure, which you should leverage – there's no need to reinvent the wheel.

Implementation tips

✓ Integrate ISMS procedures into your QMS document framework

✓ Avoid "paper ISMS" - write for real users using practical examples

✓ Include simple flowcharts, quick guides, and decision trees for everyday reference

Step 5 | Implement relevant security controls

Annex A of ISO/IEC 27001 contains 93 controls categorised into:

Organisational	People
Physical	Technological

Control selection should be driven by your **risk assessment** and **business context**. For MedTech, key areas often include:

- Encryption of patient or trial data
- Roles-based access controls for product design files
- Secure communication with cloud platforms and external partners
- Logging, backup, and monitoring of critical systems
- Supplier agreements with information security clauses
- Secure software development practices for SaMD or digital health tools

You don't need to implement them all - only those relevant to your risks. But auditors will require a strong argumentation for all controls you have defined as not applicable.

Implementation tips

✓ Conduct a "controls workshop" with key IT and compliance staff to define which controls apply

✓ Maintain a lightweight but clear SoA spreadsheet, mapping each control to risk items - this will be your main audit artefact

✓ Ensure that awareness and behaviour are embedded - not just technology

Step 6 | Operationalise & train

Once processes and controls are defined, operational implementation begins. This includes:

Training & Awareness	Everyone must understand their role in information security.
Technical controls	Secure passwords, firewalls, endpoint protection.
Monitoring	Keep an eye on logs, access attempts, and vulnerabilities.
Incident handling	Know what to do when something goes wrong.

At this stage in the process, policies become practice - and culture starts to shift.

Implementation tips

- ✓ Launch a Security Awareness Campaign: posters, short videos, games, FAQs (make learning fun, not fearful)
- ✓ Add “Security Minutes” to team meetings: each month, share one practical tip (e.g. “how to spot phishing”) or ask employees for ISMS relevant incidents, news or experiences (e.g. a sophisticated phishing mail)
- ✓ Include security behaviour in performance reviews and onboarding checklists

Step 7 | Evaluate performance & prepare for certification

ISO 27001 requires regular performance evaluation through:

Regular internal audits

(Clause 9.2)

Structured management reviews

(Clause 9.3)

Ongoing performance evaluation & corrective actions

(Clause 10)

These prepare you for certification audits and demonstrate real operational maturity.

Implementation tips

- ✓ Use your QMS audit schedule to integrate ISMS audits – utilise the same structure and share resources
- ✓ Conduct a “friendly audit”: let selected staff shadow and learn
- ✓ Use findings to prioritise future actions and track them in existing CAPA tools
- ✓ Treat the external audit as validation of your progress, not judgement day

Step 8 | Integrate with your existing QMS

Many processes required by ISO 27001 already exist under ISO 13485, such as document control, risk management, training, and supplier evaluation. Instead of duplicating effort, unify systems – for example:

- **Align** ISMS risk methodology with ISO 14971 hazard analysis
- **Extend** document templates to cover both standards
- **Harmonise** internal audits, SOPs, and CAPA processes

This not only saves time - it creates a unified, streamlined compliance culture.

Implementation tips

✓ Conduct a gap analysis between ISO 13485 and ISO 27001 to identify overlaps and deltas

✓ Create a combined management system manual to reflect both frameworks

✓ Use one integrated training plan, covering both quality and security topics

Final thoughts...

Building an ISMS in a startup, SME or corporate MedTech company is not just a regulatory project - it’s a strategic investment in resilience, trust, and operational excellence. And with ISO 13485 already in place, you're halfway there.

Security is not a project. It’s a mindset.

The key to success? Start small. Be pragmatic. Focus on people. Embed security into your existing quality mindset - and it will stick.

Congenius

mdeg
we do medtech!

Should you have a challenge related to your ISMS, please do get in touch – our MedTech experts are ready and happy to help.

Congenius AG
Riedstrasse 1
CH - 8953 Dietikon

E: info@congenius.ch
T: +41 44 741 04 04

congenius.ch

Revision 1 – May 2025