xtention
IT with care.

Setting up an ISMS in a hospital

How do you approach an ISMS project in a hospital?

The ISMS project

What do I have to look out for?

Setting up an ISMS is not a project that is implemented once and is then complete. An ISMS needs to be managed, updated and enhanced constantly because the threats and risks are always changing, too.

What level of detail is required at the beginning?

It is important not to get lost in the details when you first set up an ISMS. Start the ISMS as a 'basic setup' and add more details as you go along.

Tip

Less is often more, especially in the early stages of setting up an ISMS. If you overwhelm your organization from the beginning with a "fully grown" ISMS, it is likely that people will not be on board, and it will fall by the wayside.

What is the scope?

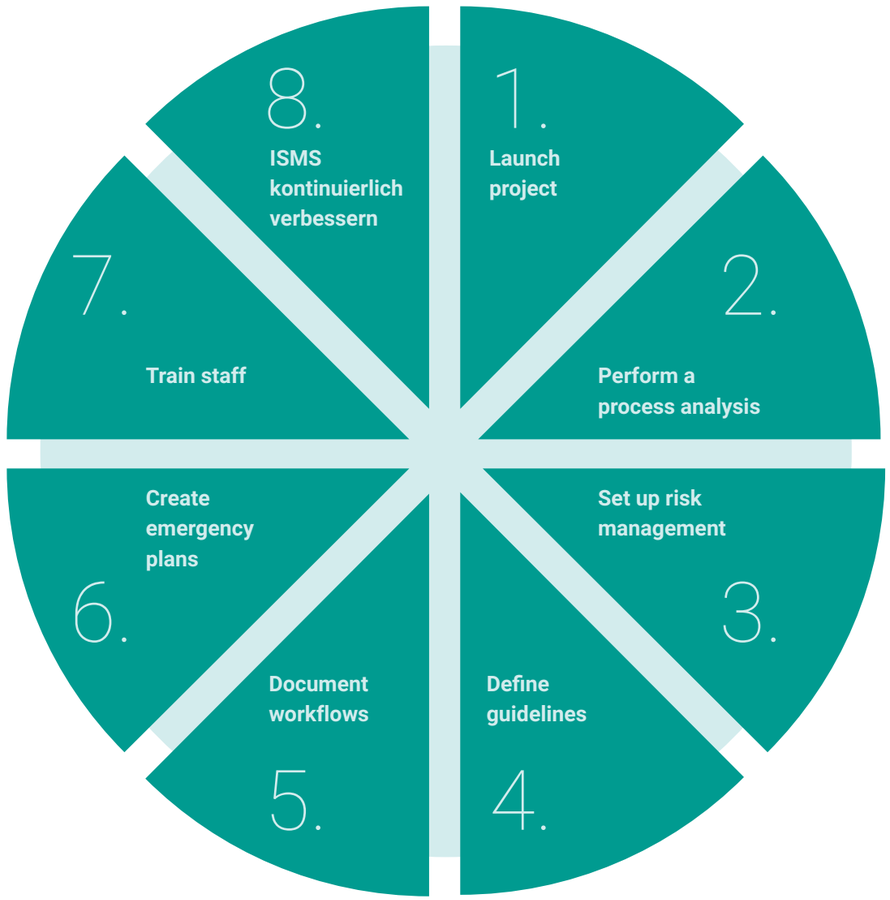
In hospitals, the scope reflects the core processes relating to treating patients. The five core processes are usually admission, diagnosis, treatment, care and discharge. All guidelines, process descriptions and documentation must be aligned with this scope, making it clear that IT alone cannot provide all the solutions for this kind of undertaking.

PROJECT IMPLEMENTATION

Implementing the project

What are the specific steps when setting up an ISMS?

An ISMS project concerns more than just IT; it affects almost all areas of a hospital. As well as IT specialists, the core team should include medical and facility technicians as well as data protection and HR specialists. For a project like this to succeed, it is vital that senior management actively supports the project and that others are made aware of its importance. You should also remember to involve the works' council at an early stage when creating employee guidelines.



1. Launch project

The project starts with a joint kick-off meeting where senior management is joined by representatives from all relevant specialist departments (IT, medical and facility technology, data protection, HR, etc.). The project goal and plan are presented at this meeting, along with the various tasks.

Tip:

Setting up an ISMS can only be successful if senior management clearly communicates the importance of such a project.

2. Perform a process analysis

Next comes an analysis of business processes and core medical processes. You identify all in-house support processes that are necessary for securing the core processes (admission, diagnosis, treatment, care and discharge).

Based on that information, the next step involves pinpointing critical processes. For every process that is evaluated as critical, you determine what IT support is necessary to maintain it uninterrupted (considering both IT applications from the users' perspective and IT components from the perspective of the IT-infrastructure). Typical IT applications in hospitals that are considered in this context include HIS, LIS, RIS, PACS, DMS, surgery scheduling systems and transport logistics.

Tip:

As well as the usual core hospital applications, you need to consider IT systems and components from medical technology, utility technology (e.g. water and energy supply), communications technology (e.g. call systems and telephones) and information technology (e.g. domain controllers, IP data networks and printers).

3. Set up risk management

Based on the business process analysis previously carried out, you can now perform a risk analysis for critical processes. You create risk catalogues derived from the requirements of common standards (e.g. ISO/IEC 27001 or 27002) and specific service processes (e.g. securing transfer routes to and from the service).

All identified risks are transferred to a central risk management system for information security. After comprehensive analysis and evaluation, you develop appropriate risk-mitigation measures.

Tip:

When setting up an information security risk management system for the first time, it is usually enough to use simple tables to document and evaluate risks. What is more important is that you develop a transparent risk-evaluation system, justifying each evaluation, the consequences and the likelihood of occurrence in your own words.

4. Define guidelines

Every ISMS needs principles and guidelines. These should cover general requirements (e.g. roles, responsibilities, management commitment, etc.) and define specific rules (e.g. an employee's decision-making power).

Tip:

Rather than trying to achieve the impossible, principles and guidelines like this should be based on truth and reality. Guidelines should be practicable for employees and remain compatible with common practice. Please note that you should also monitor regularly whether guidelines are being observed.

5. Document workflows

You document processes and workflows alongside the process analysis. Normally there are processes that are already being followed, but they are often insufficiently documented or not at all. Many of the processes to be documented mainly affect IT, for example access management (e.g. Active Directory), security systems (e.g. firewall, virus protection, encryption, logging, monitoring), requirements and procurement management (e.g. inventory, IT systems), backup and recovery, change management (e.g. checking and releasing changes), infrastructure documentation (e.g. data centre, network and central components), patch and vulnerability management (e.g. testing and rollout of security patches), handling of security incidents and personnel management (e.g. authorization adjustments when employees join or leave the organization).

Tip:

Hold workshops for small groups in the various specialist departments, and start by documenting the current status. Note possible deviations in the information security risk management system and continue working on them there.

6. Create emergency plans

Emergency plans must be created in a hospital because patient care must be guaranteed whatever happens (e.g. power cut or a pandemic). That is why you are not only required to create plans, but also to hold regular drills. In addition to standard emergency scenarios such as a fire, you should also cover IT-related emergencies (e.g. outages at all data centres).

Tip:

Don't forget to have your emergency plans readily available as hard copies at several locations on your premises because if your IT goes down completely, you will not be able to access digital documents.

7. Train staff

The most important requirements must be known within the organization. All members of staff must know what they are allowed to do and what is forbidden, as well as understanding why something is forbidden. Without a practical training concept, you will not be able to reach a consistent level of security in your organization or maintain it in the long term.

Tip:

Given the large number of employees in the healthcare sector, e-learning has proven to be a practical choice for the majority. This allows employees to decide for themselves when and where they take the course, and they are not "dragged" away from their work when they do not have time for training. E-learning systems also allow you to track attendance easily (instead of getting people to sign a list). Managers can be given extra training in the form of workshops, so they can share the knowledge in their specialist departments.

8. Continually improve your ISMS

Once you have successfully implemented your ISMS, you must continue to use, improve and enhance it. You should adopt multiple measures, such as defining measurable key performance indicators (e.g. how many employees participate in training courses) or specifying audits (e.g. checking authorizations in the HIS). By evaluating key performance indicators and audits, you can monitor, control and continually improve your ISMS. Senior management should also be actively involved in improving it. The best way of doing that is to hold an annual management review, in other words a yearly ISMS status report with the results of all audits, plus key performance indicators and suggestions for improvement.

Tip:

Try to make key performance indicators measurable, and plot the data on graphs. Informative visualizations provide management with a useful basis for making decisions.

EXPERIENCE &
TESTIMONIALS

Tips and experience

Real-life examples

- The German Hospital Federation's 'Industry-specific Security Standard for Healthcare Provision in Hospitals' (B3S) is a very useful foundation for setting up an ISMS in a hospital.
- In practice, the greatest challenges are usually setting up an information security risk management system and creating emergency plans. In many cases information security risk management is non-existent and has to be built from scratch. As a result, it is usually a new topic for management, too. Although emergency plans are available much of the time, they are often incomplete, out of date or are not followed.
- Due to the large number of hospital staff, employee training on information security and data protection is often neglected. With the GDPR transition period coming to an end, the significance of training courses has become more apparent, leading organizations to rethink. E-learning platforms have emerged as an ideal and practicable solution.
- Embedding the defined guidelines, workflows and processes in day-to-day hospital operations is a bigger challenge and requires careful handling.
- Although setting up an ISMS is not purely an IT matter, many of the related tasks do affect IT directly and need to be implemented by IT staff. Human resources are often focused on technical IT operations, but ISMS mainly affects organizational aspects. In many cases, IT departments do not have the human resources to operate an ISMS in the long term. We therefore recommend that you appoint an internal or external chief information security officer (CISO) who reports directly to management.

Selected customer testimonials

Leopoldina Hospital Schweinfurt

'We worked with x-tention to integrate an ISMS into our critical processes in a permanent and organized way. Right from the start this project had tight deadlines, so x-tention's quick and straightforward cooperation was really helpful. The ISMS templates provided by x-tention allowed us to considerably reduce the amount of work required to create an ISMS as the documents were adapted and put into action by the specialist departments themselves. X-tention's wide-ranging practical experience and their flexible approach to the particular setup in our hospital meant that we could quickly create an ISMS that meets our needs perfectly. The commitment of all participants was rewarded with an excellent compliance audit result from the auditing body.'

Thomas Balling MSc | Head of IT

SRH IT Solutions GmbH

'The x-tention templates were a great help with setting up a long-term ISMS in our OES organization in Gera. The extensive content was extremely well structured by sector, and the templates saved us lots of time and effort. They enabled us to provide the verification documents required by Section 8a of the BSI Act in time for the deadline on 30 June 2019.'

Dr Stefan Müller | CISO

Marienhospital Stuttgart

'x-tention's expertise and template package allowed us to quickly and efficiently define requirements and processes in the organization and build an effective ISMS.'

Stephan Rühle | Head of IT/MTECH

Hanau Hospital

'In line with the NIS Directive, we created an ISMS at Hanau Hospital to meet the new regulatory requirements. We called on x-tention as an expert ISMS consultant. Thanks to the templates they provided, we were able to minimize the amount of work spent on implementing an ISMS. The positive result we received from the compliance audit was a testament to our effective cooperation and the success of the project.'

Hüseyin Gökceoglu | Head of IT

The complete template package

Our years of experience ensure your success

x-tention provides customers with templates for guidelines, process descriptions and other necessary documents, tailoring them to the requirements and circumstances of each organization.

Security guidelines

Creation of central ISMS documents (e.g. information security policy and usage policy)

Process descriptions

Definition of required information security processes (e.g. backup concept, patch management and security incident management)

Roles and responsibilities

Creation of role definitions, role assignments, provisions for substitutes, etc.

Information security risk management

Methodology for identifying, evaluating and handling risks; documentation of risks and countermeasures

Awareness programme

Creation of an awareness concept; staff training on information security topics

Audit planning

Creation of an audit programme and a template for audit reports; definition of internal and external audits

Key performance indicators

Definition and regular monitoring of key performance indicators; implementation of improvement measures

Management review

Regular reporting to management; implementation of improvement measures

x-tention group

How to get in touch

x-tention Informationstechnologie
AT +43 7242 2155 office@x-tention.at
DE +49 6221 360550 office@x-tention.de
CH +41 43 222 60 22 office@x-tention.ch
UK +44 203 983 9860 office@x-tention.co.uk

soffico
DE +49 821 455 901 00 info@soffico.de

FAKTOR D consulting
DE +49 821 455 9021 00 info@xd-consulting.de

it for industries
AT +43 7242 2155 0 office@itforindustries.at

Cloud21 Limited
UK +44 845 838 8694 info@cloud21.net

Michael Punz
Process & Quality Management

Telephone +43 7242 2155 6325
Mobile +43 664 80009 6325
E-mail michael.punz@x-tention.at