Johner Institute

ISO 27001 (not only) for medical device manufacturers

With Dr. Andre Baumgart, Prof. Dr. Christian Johner

Transcript

00:00:05 Speaker 1

Medical Device Insights, a podcast by the Jona Institute for medical device manufacturers, authorities and notified bodies.

00:00:17 Speaker 2

At the latest with the DiGA Regulation, ISO 27001 and information management systems in general are in focus

00:00:28 Speaker 2

medical device manufacturers.

00:00:31 Speaker 2

However, not only these DiGA manufacturers should deal with this standard and what this standard is about, what exactly it requires, how to introduce it, such as an information security management system.

00:00:46 Speaker 2

This is exactly what I would like to talk about today with my colleague, Doctor Andre Baumgart.

00:00:51 Speaker 2

Hello Andre, how are you?

00:00:53 Speaker 2

Would you like to introduce yourself very briefly?

00:00:55 Speaker 3

Thank you very much, Christian, for the introduction.

00:00:56 Speaker 3

My name is André Baumgardt.

00:00:58 Speaker 3

At the UNI Institute, I deal with medical device approval and information security management, especially in the context of DiGAs, and am myself a lead auditor in the field of 27001 and lead auditor in the area

of ISO 13485 and have already supported several 100 manufacturers in the approval of medical devices.

00:01:23 Speaker 2

Of course, this makes you exactly the right man when it comes to this topic.

00:01:27 Speaker 2

Let's start with the beginnings or with the basics.

00:01:30 Speaker 2

What is an information security management system?

00:01:35 Speaker 2

What does this regulate and how does it differ from a quality management system?

00:01:42 Speaker 3

An information security management system, as the name suggests, deals with the issue of security with information and data in the organization

00:01:51 Speaker 3

And in principle, it is a systematic, risk-based and targeted approach to shaping the management of information in the organization and thus supporting and achieving the business goals of the company.

00:02:10 Speaker 2

What does ISO 27001 require in concrete terms?

00:02:15 Speaker 2

goes from the manufacturers, do you have to implement procedural instructions, as with a 13485?

00:02:24 Speaker 3

The standard prescribes some processes, significantly fewer compared to ISO 13485,

00:02:35 Speaker 3

which usually surprises manufacturers, but these are partly similar topics as the 13485, which also provide points of contact.

00:02:46 Speaker 3

Topics such as description of the area of application, the context of the organization we also know from ISO 13485 The whole topic of leadership, leadership responsibility, obligation of the company management also plays a role.

00:03:04 Speaker 3

Then a risk-based approach now with regard to values and information, which we know from ISO 13485 with regard to the risks of medical devices.

00:03:16 Speaker 3

So it's a bit different here, but similar in approach.

00:03:21 Speaker 3

And the whole topic of support, resources in the organization, that's also something that's very similar compared to 13485.

00:03:32 Speaker 3

then we also have a management review, internal audits and the popular Kappa process, which also works here.

00:03:41 Speaker 3

So you can already see or hear from it that there are many points of contact in the main articles of the standard.

00:03:50 Speaker 2

Now you have just described that we have many similar procedural processes.

00:03:55 Speaker 2

You have now spoken of management reviews, of corrective measures, preventive measures of internal audits.

00:04:01 Speaker 2

Where do you see the biggest differences?

00:04:04 Speaker 2

In other words, what additional processes would companies have to implement in order to meet the requirements of 27001?

00:04:14 Speaker 3

The differences lie because the focus of the standard is different in the area of safety and information and protection of values in the organization, especially in Annex A1.

00:04:30 Speaker 3

it mentions many requirements that shed light on another aspect of the organization, such as ISO 13485.

00:04:42 Speaker 3

So, you can take examples.

00:04:44 Speaker 3

There is an information security policy that one needs to implement to determine what these information security management systems relate to.

00:04:58 Speaker 3

And everything else is then derived in the area, for example, mobile devices, teleworking, personnel security, access authorizations, management of information values, protection of data carriers, buildings.

00:05:14 Speaker 3

These are all responsibilities that have to be defined here and there are specific procedural instructions needed, but then probably also

00:05:26 Speaker 3

Work instructions in detail to give employees tools and also instructions on how to implement them.

00:05:35 Speaker 2

Now you've talked a lot about ISO 27001.

00:05:40 Speaker 2

Now there are a few sister standards in this series, especially one for health applications or healthcare.

00:05:50 Speaker 2

Would you recommend to manufacturers,

00:05:52 Speaker 2

to look at these other norms as well, and perhaps a question before that, what are these sister norms about?

00:06:00 Speaker 3

There is a whole family of standards of the 27 thousand series.

00:06:05 Speaker 3

The core standard, 27001, which we have now primarily talked about, describes the requirements of the I.S.M.S.

00:06:16 Speaker 3

for general organizations.

00:06:19 Speaker 3

Now, if you look at 27,799, as you mentioned, which was also designed specifically for health care facilities, it deals with the specifics that exist in care facilities or even with operators, if you speak generally, and in some cases tightens the requirements in

00:06:46 Speaker 3

really concrete requirements that must be met with regard to the implementation of these information security requirements.

00:06:56 Speaker 2

Could you give us an example of these tightenings?

00:06:59 Speaker 3

One example is that the guideline on information security must contain a concrete reference and concrete design of personal health information.

00:07:14 Speaker 3

This means that this guideline defines at the highest level how I handle this sensitive information and

data in the organization.

00:07:24 Speaker 3

At the different levels, in the different areas, for example a hospital or even if I am a DIGA manufacturer, how do developers approach potential data that may train an AI and how does customer service handle this customer data?

00:07:40 Speaker 3

I have to

00:07:41 Speaker 3

even at the top level in my information security management system.

00:07:50 Speaker 2

With that, you've now brought in another exciting thought here, namely the topic of products.

00:07:56 Speaker 2

We have talked a lot, now about organizations that have to protect their information, information technology.

00:08:03 Speaker 2

This would probably affect the operators in particular.

00:08:07 Speaker 2

Now, however, many DiGA manufacturers are not only operators, but above all manufacturers of medical devices.

00:08:13 Speaker 2

And the MDR explicitly requires these medical devices to take state-of-the-art information security into account.

00:08:25 Speaker 2

Is ISO 27001 helpful to us in meeting this requirement of the MDR?

00:08:34 Speaker 3

ISO 27001 as a system standard can indirectly help to derive requirements for the products, because of course, when I think about the operation and also the product realization later, I check

00:08:55 Speaker 3

whether I can be operated safely in my application context afterwards.

00:09:00 Speaker 3

So, it's more of an indirect reference, if you want a direct reference, then the standard helps you to systematically derive these requirements through the systematic approach in the organization as a manufacturer.

00:09:16 Speaker 3

So whether this is a cryptographic method or the topic of authentication for

00:09:23 Speaker 3

for such an app, I can then systematically derive requirements, but today they often link to more specific product standards or requirements, such as from the Federal Institute for Information Security, which has issued requirements for digital products, for example, at least in a draft version.

00:09:50 Speaker 3

Or of course, we also have our guide, the

00:09:53 Speaker 3

who supports us very well in consulting, but above all also supports the manufacturers in deriving requirements for the products.

00:10:03 Speaker 2

I'll summarize very briefly so that you can check if I understood it correctly.

00:10:08 Speaker 2

I understood you to mean that ISO 27001 can ultimately also be used to define the product requirement, i.e. the System Requirements Specification or Software Requirement Specification.

00:10:21 Speaker 2

so that afterwards from the customer's point of view you also have products that can be operated in accordance with 27001, but that we as manufacturers also have to explicitly refer to other standards and best practices.

00:10:39 Speaker 2

and for those for whom this is too much work, to have to go through many standards, such as IEC 62 443 again, you recommend our guide, in which we have already consolidated all this.

00:10:51 Speaker 2

Is that true?

00:10:52 Speaker 3

That's true and supports each other and of course that brings a lot of efficiency if you refer to the existing documentation.

00:11:01 Speaker 2

Let's go back to the topic of information security management systems.

00:11:07 Speaker 2

and to the question of how to proceed now to introduce something like this.

00:11:12 Speaker 2

Most manufacturers don't start at 0, according to M.D.R.

00:11:16 Speaker 2

already have a quality management system in place.

00:11:20 Speaker 2

What steps do you recommend now to meet the requirements of ISO 27001 in addition?

00:11:29 Speaker 2

There is also a bit of a question in it, will we have 2 management systems and

00:11:35 Speaker 2

The other question is also involved.

00:11:38 Speaker 2

So, what steps do I take now to move from a Q.

00:11:41 Speaker 2

M.

00:11:41 Speaker 2

system to achieve 27001 compliance.

00:11:48 Speaker 3

First of all, I have to ask the organization, what do I want with this information security management system as a manufacturer

00:11:58 Speaker 3

And in principle, this is a strategic question and the requirement to have something like this usually comes either classically from regulation, legal requirements, as we now have in the area of DiGAs, or often from customers.

00:12:15 Speaker 3

So the first thing you have to do is to ask yourself, is it worth doing the whole thing, do I even have to do it in order to be able to survive in the market at all?

00:12:25 Speaker 3

That would be the first step.

00:12:27 Speaker 3

the second step, if I have decided to do it, we classically do a detailed gap analysis, where we meet all the requirements of the main chapters and Appendix A.

00:12:40 Speaker 3

1 and record what is going on in the organization.

00:12:46 Speaker 3

This also allows us to determine how well existing procedural instructions cover the requirements of ISO 27001.

00:12:56 Speaker 3

And

00:12:57 Speaker 3

at the same time, we also get a good picture of how much effort is behind implementing the whole system, i.e. in the case of man-days or then also costs that are added to it.

00:13:11 Speaker 3

And based on this comes the third step, the implementation planning and the implementation planning is then a multidisciplinary undertaking in the organization in order to

00:13:24 Speaker 3

not only the developers or not only the I.

00:13:26 Speaker 3

T.

00:13:27 Speaker 3

department, but really everyone to live the topic of information security.

00:13:32 Speaker 3

Because in the end, it's not just about I.

00:13:35 Speaker 3

T.

00:13:35 Speaker 3

Questions on this topic, but also on real physical elements that contribute to information security here in the organization.

00:13:44 Speaker 3

And that's what I have to build up, implement, live and to a certain extent

00:13:53 Speaker 3

The fourth step is to audit this internally, use this internal audit to identify gaps in the implementation and then present the whole thing in a management evaluation.

00:14:06 Speaker 3

And once you've gone through that, then you can say that I think you've checked how the whole thing should be lived.

00:14:16 Speaker 3

And if I am sure that I will meet all or essential requirements in the standard and in Annex A.

00:14:23 Speaker 3

1 and have implemented it correctly, then I register for the audit by an independent testing body, which

will then issue an ISO 27001 certificate after successful testing.

00:14:39 Speaker 2

You have already mentioned a sentence or a word that made me stop.

00:14:43 Speaker 2

It was now the

00:14:44 Speaker 2

Effort.

00:14:45 Speaker 2

I think many of the manufacturers are interested in it, what does it mean now in terms of time, what does it also mean in terms of costs, what are your experiences, how much effort do you have to expect as a manufacturer to be ready for certification in 27001?

00:15:02 Speaker 3

The effort that we have now seen in the large number of projects fluctuates between 60 and 100 man-days, you can roughly say.

00:15:09 Speaker 3

So, if you take the middle of 80 man-days, then you can count that as an expense for the organization, the company.

00:15:17 Speaker 3

These are internal man-days or women's days, which are needed accordingly to set up the whole thing, operate it and implement it in the organization, including training.

00:15:31 Speaker 2

Yes, I think we have a pretty good overview.

00:15:34 Speaker 2

Let me briefly summarize.

00:15:35 Speaker 2

So we talked about what such an information management system regulates in the first place.

00:15:41 Speaker 2

Have recognized that there are many operating instructions that we already know from an ISO 13485, but that further work and procedure instructions are necessary to specifically meet the requirement of this Annex

00:15:56 Speaker 2

A.

00:15:57 Speaker 2

1, where it is also about very concrete things, such as access authorizations you have described, also hi-

ring staff, access to systems and much more.

00:16:08 Speaker 2

We had taken a quick look at the norms family.

00:16:12 Speaker 2

You reported that there is another standard for operators of healthcare facilities, namely ISO 27 799 in this family of the 27 thousand series.

00:16:24 Speaker 2

We have

00:16:25 Speaker 2

had talked about the fact that the M.D.R.

00:16:28 Speaker 2

information security demands that a 27001 will not be sufficient now, but rather actually provides information on the specification of these products and that other product-specific standards are still needed.

00:16:42 Speaker 2

And at the end you reported that we can finally get to certification with just 4 steps and what that means in terms of effort.

00:16:50 Speaker 2

Oh, I think there was a lot in that good quarter of an hour,

00:16:54 Speaker 2

André, thank you very much for being there for us, for giving us this insight.

00:16:59 Speaker 2

Yes, and for all those who want to know more about this topic, we have linked technical articles here below in the description.

00:17:07 Speaker 2

You know our contact details anyway.

00:17:09 Speaker 2

So, if we can help with the introduction or testing of certification readiness, so to speak, just let us know so that

00:17:20 Speaker 2

Your system meets the requirements of the DiGA Regulation, for example, or

00:17:25 Speaker 2

Your products are also MDR-compliant.

00:17:28 Speaker 2

André, thank you for joining us again.

00:17:31 Speaker 3

Thank you very much.

00:17:32 Speaker 2

See you soon.

00:17:32 Speaker 2

Bye.

00:17:34 Speaker 3

Bye.