DACHS

Document Management for Life Science

# ISO 27001 COMPLIANT MANAGEMENT SYSTEM IMPLEMENTATION PROJECT

(WHITE PAPER)



**Our latest ISO 27001 consultancy project was special. Clients in many cases have a QMS (Quality Management System) already and want to integrate it with an ISMS (Information Security Management System), but that was not the case in this instance. Instead, they had an aborted ISO 27001 implementation project, and, while they didn't know exactly what they wanted, they knew very well what they didn't want. The purpose of this paper is not to provide a complete and detailed process of implementing a management system but to highlight the experience of a given ISMS implementation project and to provide useful hints.**



## The Client

Our client was a medium-sized international IT service company. They didn't want to implement the ISMS for the whole of their operations but for services where only about 10–12 people were involved. It was clear for them that they needed preferably one expert (not a bunch of consultants who might be contradicting each other in some cases), and they wanted to see progress. They already knew that implementing an ISMS needs time and effort.



## Setting Up the Project

So our task was to support them in restarting their project and keep momentum. The very first task is always to set up the implementation project. We agreed on a commonly acceptable schedule, identified stakeholders, and set up communication channels. **It is indispensable to have a single contact on the client side who receives all written communication** and possibly participates in all meetings with stakeholders to have a general view of the progress and support client-side activities. This time we had an excellent, agile client-side project manager. **It is important – and this was also an expectation from the client – to have regular status meetings.** It was agreed that these would be held weekly, which is good for projects with at least medium intensity.

**Another key element is to obtain top management buy-in.** In this project there was no need for a management kick-off meeting, as the project was already initiated before our arrival.

It was clear immediately that restarting the implementation would waste the work our client had already invested. So we asked for access to the ISMS documents already created, to reuse as much as possible.



## Interested Parties

Earlier versions of the ISO management system standards were talking about management-related requirements. The current ones refer to top management. By definition of the standard, the term “organization” is used for that part of the company that is covered by the ISMS and “top management” means those who direct and control the organization at the top level (which is not necessarily the same as company top management). Requiring top management involvement emphasizes the strategic nature of an ISMS: it requires resources to establish and implement the management system. Actually, the burden is the same whether the organization sees the certification as only a marketing tool or it is considered a strategic tool to strengthen information security.

**IT security is not the same as information security but is a major part of it.** This means that the IT manager (or somebody with a good understanding of the IT environment) is a key player in the project. But IT managers tend to be busy and not the best friends of writing and executing procedures. The passive resistance of an IT manager can significantly extend the project schedule. This is one point where a good project manager and top management support is indispensable. We were lucky with our client, as the IT manager saw the value in the project, participated in almost all the meetings, and did his best to keep internally agreed deadlines. **Even though it is true that “fate leads the willing and drags along the reluctant”, the importance of a supportive IT manager cannot be overstated.**



## Defining the Scope

The review of the documents showed that the approach applied in the first run didn't really fit the size of the organization. They had, for example, a lengthy scope document. This was legally perfectly correct and defensible, but this is not what people at an organization of that size expect and auditors search for. **The standard requirement that the scope must be documented doesn't mean that the scope has to be in a separate document.** It just means that what is included (and optionally what is excluded) has to be clearly defined in writing.

Let us stop here for a few thoughts:

- No company works without policies and procedures. Some of these are relevant from an information security point of view. Although some additions may be required based on the standard requirements, existing controls should be kept as intact as possible, as those reflect the organization's inherent view on processes and controls. **Some of the existing documents will need to be referred by, others embedded into new documents to be practically included in the big picture of the ISMS.**

- It is possible that not all of the processes of a company are covered by the ISMS. The definition of the management system scope is always the decision of the organization.

- The ISMS scope is defined in terms of processes and information assets. If any characteristics (location, purpose, type…) of assets is relevant, it can be included in the wording of the scope; otherwise, listing processes is enough.

- Some say, that anything excluded from an ISMS scope must be treated as if it were external to the company and doesn't need to be dealt with. This is true for many management systems (like a Quality Management System or a Service Management System) but not always for an ISMS. **Excluded assets and processes may pose risk for assets and processes in scope and that may need to be treated.**

- Lastly – even if it is pretty uncommon – t**he certification scope may be smaller than the ISMS scope.** The organization may decide to have only a part of its ISMS audited by a certification body, but most companies want to pick all the fruits of their work.

## Quick Look at the Standard

The ISO 27001 standard has two clearly separated parts, both of which are mandatory. I used to see them as a tennis racket:

- The standard body is the racket frame, which sets up a management system framework. This doesn't contact the ball, but still it makes it possible to play the game.
- Annex A of the standard corresponds to the tennis string, which lists grouped control requirements, directly influencing information security.

Some consultancy companies create documentation sets to support organizations establishing their ISO management systems. My decade-long auditing experience showed that it is easy to spot the use of these documentation sets, as they tend to be lengthy (to support all sizes and types of organizations) and never fit perfectly. They can be used, of course, but customizing them is about the same amount of work as creating a custom documentation set. You can save the cost of a consultant, but you will never know what you do due to the standard and what because of the specifics of the documentation set (some processes may be simplified or even omitted at certain organizations).

## Top-Down Approach

**It is a proven approach to start establishing the ISMS with an ISMS policy and an initial asset inventory.** This is a good warmup to establish cooperation. Documenting an inventory is extremely useful for both parties: organization stakeholders gain an understanding of what is in the scope (and what is not and why), and the consultant receives a view of what the organization has, including the most important existing controls.

We like to work with the ISMS manual next, while the initial asset inventory keeps client reps busy. This is possible because interviews to gather information on the content of the manual are relatively short. Management system manuals tend to be similar to each other between organizations; this is where a template with pre-prepared content is the most useful. It is a clear advantage if a company has any ISO management system operating already (typically a QMS, which is the most widespread standard), because **all ISO management system standard framework requirements are identical.** This means that one need only add a few standard specifics to an existing manual, and one is done. This was not the case with our client, so we suggested a template that follows the standard body structure. This is irrelevant for the few users of the manual (typically the CISO, the internal auditor, and a few managers), but auditors love it.

## Control Definition

The most cumbersome and lengthy part of an ISMS implementation is writing the policies and procedures. **There are many control requirements, and all of them need answers that cover all assets in scope and are specific to the organization.** Here we followed a few simple rules:

- Standard requirements are based on best practice. However, they don't contain the method for covering them; that is up to the organization. The consultant should not emphasize that something is a standard requirement but try to focus on organizational value and support the organization's finding a control that fits best.

- It is a mistake to think that all controls must be implemented by a technical solution and thus heavy investments are needed. The implementation of controls must be tailored considering customer and legal requirements, the size and type of business, and the organization's risk appetite.

- If an area or function impacted by the ISMS has no written procedures, it is time to create them. It is practical to write documents that cover the whole company and not just the organization, but it is up to the company to decide.

- The purpose of the ISMS documentation is not to provide an overly comprehensive demonstration of compliance with the standard requirements. It has to document an environment to implement, maintain, and improve security. Don't write anything just because you think it would look good on an audit. Keep documentation simple but clear (e.g., avoid passive terms like "will be done," because if it is not clear who will do it, when, and how, it won't be done) – your colleagues will appreciate it.

- If the standard requires a written procedure on a topic, it doesn't mean it has to be a separate document. Short procedures can be merged into more general documents to avoid a regiment of tiny documents, where nobody will be able to find the relevant controls.

- Consultants should suggest, but let the organization decide on documentation structure and controls. It is their management system; they know what they want and what they can accept.

- Structure the documentation content according to reader groups. This will help colleagues to find controls they must observe more easily.

- High-level policies and procedures can be drafted by the consultant based on interviews. But for low-level documents and lists it is not effective; they are better be prepared by the organization.

Our client had a lot of small policies, created organically as they felt the need for them. Some even contradicted each other at some points. In this phase – based on standard requirements – they could largely extend the scope and coverage of their existing controls without increasing the number of documents they already had.

**It is not easy to maintain momentum while writing policies, but this is the price of a comprehensive approach where all the important aspects of information security are considered and fit into a single system.** It took us – besides other duties on both sides – about three months to get through this phase.

**Writing policies and procedures always brings up topics that were uncontrolled.** This was the case in our project as well. If a control requirement is irrelevant for the organization, it can be excluded with proper justification. But it is a delicate question since control exclusions will be given a close look by the auditors. If you don't currently apply the best controls you would use, do what you can and set it as an objective to improve. As long as the objective is clear, actions are planned and realistic, and progress is visible, it will not hinder certification.

**"There are many control requirements, and all of them need answers that cover all assets in scope and are specific to the organization."**

**"Writing policies and procedures always brings up topics that were uncontrolled."**

## Implementing the ISMS

Once procedures and policies are ready and approved, they need to be communicated to the interested parties. As we stated before, practically everyone in a company is involved in an ISMS, even people or entities outside the scope (e.g., out-of-scope departments, suppliers, service providers). **They need tailored communication on relevant requirements of the ISMS so as not to pose risk to the assets in scope.** People in scope need a deeper knowledge of policies and procedures; a presentation for them and a knowledge test is advised.

From this point on, the ISMS is established and implemented, and proofs of operation of controls are being collected. It is important to know that certification bodies require typically at least three months of management system operation to gather proofs of operation to be sampled during the audit. It is also important to **have an internal audit and a management review before certification, as certification bodies need to see these processes working.**

When an organization aims to implement a management system that complies with multiple management system standards, there are other aspects to be considered – you can read about those in this paper.

June, 2022
© DACHS GmbH., Basel/Switzerland