27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

Implementing ISO 27001 with a consultant vs. DIY approach

WHITE PAPER

Advisera
Making certification simple.

Table of Contents

Executive summary

In the past, there were two main routes to implementing ISO 27001: create the documents and gather information needed from a variety of sources, or hire a consultant to hold your hand through the process. The first option is cheaper, but often ends in failure. The second is very expensive and results in the valuable knowledge and expertise gained from implementation not being retained in the business.

The situation with ISO 27001 implementation has fundamentally changed. Custom-built online tools now provide budget-savvy IT or security managers with the high-quality information and advice they need in one place. This is drastically reducing the cost of implementation, while ensuring a project is quickly and effectively completed. The benefits these tools bring (large cost savings compared to hiring consultants, high-quality ready-to-use document templates, retained knowledge in the business, step-by-step guidance and community support) make this new approach to ISO 27001 implementation a compelling option.

Introduction

All companies are in pursuit of making bigger profit and avoiding losses and financial mismanagement. Among other benefits that ISO 27001 brings to the company, it can be one of the tools that will help companies to enhance their image and expand their market by being qualified to apply for tenders and meet customer and legal requirements. Consequently, more and more companies worldwide are deciding to implement ISO 27001, and the number of certificates is growing every year, but the road toward the certificate is not always easy. (Read this article to learn more: Four key benefits of ISO 27001 implementation.)

At the very beginning of ISO 27001 implementation, you're probably overwhelmed with various approaches on how to start and finish such a project successfully. One of the biggest problems is the fact that the company doesn't even know what to expect from the implementation, what the deliverables are, or how much work it takes. Even before the implementation project starts, the company must become familiar with the standard to get some idea of what to expect at the end of the project. There are two basic options to implement these standards: (1) use a consultant, or (2) implement the standard with a Do-It-Yourself approach – but taking advantage of external know-how.

The implementation with a consultant

Pros. With this option, you hire an expert from outside (usually, this is a local consultant) who has experience with the implementation of the standard. This person then performs the analysis of your company, does the interviews, writes the documentation, and everything else – basically, he is implementing the whole standard on your behalf. Here are some benefits of hiring a consultant:

- A consultant can do all the work for you, so it seems like you save your time for other things.
- The consultant ensures your compliance with ISO 27001 by reviewing and correcting all the documents.
- A consultant can show you the ISO 27001 certification criteria, and tell you what you need to get ready for certification.

Cons. Consultants obviously cost money, so this is the most expensive option. Further, you are opening access to almost all of your company secrets (e.g., how the company is organized, its main processes and key competitive advantages, who the most important people are, where the company is vulnerable, etc.) to an outsider. Finally, when someone from outside is writing the documentation, the employees might feel those policies and procedures are imposed on them, so often they look for ways to bypass them. In addition to this, here are some of the most common weaknesses of this approach:

- Hiring a good consultant is expensive, due to the time they have to spend onsite in your organization. Unfortunately, a bad consultant costs even more.
- An on-site consultant learns your weaknesses, knows your strategies, and has easy access to company secrets.
- At the end of the project, the consultant leaves – and takes all that expert knowledge with him. Often, employees don’t even understand how to maintain the documentation, leading to declining use and eventual abandonment of all those documents you paid for.
- Consultant fees are usually fixed and encompass the entire project. If you don’t like his work, you’ll probably still have to pay for his services.

The DIY implementation

Do-It-Yourself implementation of the standard means that you will be relying primarily on the work of your own employees and external know-how. With this option, your employees are doing all the analysis, performing all the interviews, writing the documentation, etc., but the knowledge for all this comes from external experts and online tools.

There is no "one-size-fits-all" solution, and this method might not be right for every business. Actually, there is no one solution that will do everything for you. Nevertheless, online solutions can be a valuable trump card for the efficient completion of ISO 27001 implementation without the high price or high stress.

Pros. This is probably the most cost-effective option because online tools are far cheaper than hiring a consultant on site. You're also not allowing anyone from the outside to learn anything about your internal processes or documentation. Finally, creation of your own documentation expands the engagement of your employees towards the required changes. Additional benefits of this approach are:

- Online tools have more extensive experience incorporated in them, since they are accessible worldwide and get feedback from clients everywhere throughout the world.
- You keep all that knowledge inside your organization. Employees learn how to maintain the documentation, improve upon it, and use it on a daily basis.
- You pay only once, only for what you need, and you can use the templates as many times as you like.

Cons. Your employees will even now need to learn about the implementation, so this is not the speediest approach to implement the standard. Likewise, this option does not resolve the issue if your employees are totally overwhelmed with different tasks and have no time for anything new.

For more information, please take a look at this useful handbook: Preparations for the ISO Implementation Project: A Plain English Guide.

What does a good online solution include?

Much the same as consultants, online tools come in various shapes and sizes, and it can be difficult to figure out which tool is the best for you. The primary thing to be considered is what you are getting for your cash – would you say you are getting just a cluster of folders with documents, or does it include some extra support? Here are some examples of criteria that can help you determine whether the solution is right for you:

Content of the documentation package – This is the first thing to look at. Does the documentation package contain all mandatory documents? Furthermore, does it contain documents that are not mandatory, but are useful for the implementation and operation of the ISMS?

Quality of the documents – This doesn't enter your thoughts until you begin filling in the documents and tailoring them to your needs. Is the document formatting consistent throughout the entire package? Are documents appealing? Do they include comments to help you navigate through the documents and help you fill them in?

Additional helping tools – Need for such tools arises later in the implementation, and it is not entirely obvious at the moment when you are buying the package. Are your suppliers offering some extra tools that may help you when you stall out or want to make an estimate of the timeframe? Such tools might include a Gap Analysis tool or video tutorials that will help you fill in the documents.

Know-how for the implementation – This is a fundamental criterion, because the knowledge is what remains in the company and will ensure that you yield benefits from ISO 27001. Do your providers offer online courses so your employees can learn about ISO 27001 basics and the internal audit? Are there any articles or webinars that explain different parts of the standard?

Personal interaction – The online solution cannot completely replace the insight from an expert. Does the online solution include expert help at critical stages in the process? Can you ask a question via email or schedule an online consultation? Can they review your documents so you are sure that your documentation is compliant with the standard? This element of the online solution can have a great impact on your decision, since it enables you to get the consultant's knowledge and advice at the moments when you need them the most, and to get the consultant's help only when you really need it.

Availability in your language – Using a solution that is not translated to the language that the employees use might significantly expand the timeframe for the implementation. What every company wants to avoid is translation of the documents, especially when it comes to some professional matter where translation mistakes can have a profound effect.

Scalability of the online solution – Although the requirements of the standard are the same for every company, the way in which those requirements are met will depend on the size of the company and the complexity of its processes. Using documentation created for a big company in a small one will cause problems, and vice versa. See if they have different packages for different purposes.

Having every one of these criteria as a primary concern will keep you from purchasing something that won't help you or wouldn't fit your needs. Ensure you get a good value for your cash and abstain from wasting it on an item that doesn't work for you.

To summarize, which implementation approach is best for you?

Which path you take to ISO 27001 implementation depends on your unique situation. So, to help you decide which approach is best for you, here is a quick guide to your options:

Hire a consultant if:

- Time is a major concern for you. Hiring a consultant will help you achieve success in a short timeframe.
- You don't have people who can allocate time to an implementation project. A consultant can act as that person on the ground.
- Cost is not your primary concern.
- You're sure you will get a top-level consultant, as this is the best way to ensure they bring added value to the table.

Do it yourself if:

- You have enough time to put into your project.
- You want to cut the implementation expenses.
- You have some spare time, but don't want everyone's daily routines to be overly impacted.
- You want the knowledge of ISO 27001 implementation to be retained in-house.

Conclusion

Where once the most likely route to a successful ISO 27001 implementation was to hire a consultant, the options available to you have now expanded. Rather than having to locate all the information you need from a range of online sources, you can now utilize dedicated one-stop shop online services.

The rise of these new online tools has, for the first time, made the do-it-yourself approach to implementation a feasible one.

Before embarking on an implementation project, it's vital to choose the method that best suits your needs. And that very much depends on your unique situation. For some, hiring a consultant will be the best option; for others, the new online tools provide an attractive choice.

One thing is for sure: the rise of online services has changed the landscape of ISO 27001 implementation.

Check out ISO 27001 compliance software

To learn how to implement ISO 27001 without the help of a consultant and automate the creation and filling out of documents, sign up for a 30-day free trial of Conformio, the leading ISO 27001 compliance software.

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

Advisera Expert Solutions Ltd
for electronic business and business consulting

Our offices:
Zavizanska 12, 10000 Zagreb, Croatia
Via Maggio 1 C, Lugano, CH-6900, Switzerland
275 Seventh Ave, 7th Floor, New York, 10001, U.S.

Email: support@advisera.com
U.S. (international): +1 (646) 759 9933
United Kingdom (international): +44 1502 449001
Toll-Free (U.S. and Canada): 1-888-553-2256
Toll-Free (United Kingdom): 0800 808 5485
Australia: +61 3 4000 0020
Switzerland: +41 41 588 0722

EXPLORE ADVISERA

Advisera
Making certification simple.