







# Recognize the factors to Consider when hiring an ISO 27001 ISMS Consultant

## Recognize the factors to Consider when hiring an ISO 27001 ISMS Consultant

The most widely used universal standard for information security is ISO 27001. It was released in collaboration with the International Electrotechnical Commission (IEC) by the International Organisation for Standardisation (ISO). Both are top international organizations that produce global standards. The goal of ISO 27001 is to safeguard the availability, confidentiality, and integrity of information within a firm. This is achieved by first determining what potential incidents could affect the information (i.e., risk assessment), and then specifying what needs to be done to avoid such incidents from occurring (i.e., risk mitigation or risk treatment).

The time it requires to establish an ISMS should be accelerated by an ISMS consultant. The [ISO 27001 consultant](#) must provide all the necessary expertise and support in avoiding the project's numerous hazards. Throughout the project, a consultant should guide a company step-by-step and provide specific guidance on what the certification auditors will be looking for.

A consultant can frequently conduct essential analyses, give the best solutions, make relevant documentation, train the employees with proper [ISO 27001 ISMS awareness training](#), and many more things. In other words, the consultant may reduce some of the employees' workload. Additionally, managing ISO certification domestically may out to be unexpectedly costly. Training staff to become familiar with the requirements can easily be more expensive than using a consultant. A consultant can identify minor process problems that the employees might notice or write off as "just the way we do things." An outsider's viewpoint can add new value to how the company functions. So, which criteria should you use while hiring an ISMS consultant?

1) Experience & skills: In addition to researching the consulting firm, find out if the person performing the consulting has any relevant certifications, such as the Certified ISO 27001 Auditor Training or the ISO 27001 Lead Implementer training course. How many different jobs has this individual completed, and how long has worked in this industry? For what kinds of businesses did work? They might be a poor choice for an IT business, for instance, if she primarily worked with banks.

2) Reputation: Calling the clients, the consultant claims to have worked with is by far the best option – very often, you'll be startled that the assignment individual was working on was significantly less in scope than you were likely to assume, and sometimes the customers won't speak favourably about the service they received. Also, if a consultant has written books or articles on a particular topic, or if she is a regular conference speaker, chances are the organization makes a solid pick.

3) Customized service: Avoid "copy-paste" consultants; they will offer executed templates and add nothing to them. During the bargaining process, you will discover a lot about a consultant's willingness to adjust the service to your demands. If you believe that is not adaptive enough, or if you dislike her communication approach, walk away from this offer.

4) Language: Choosing a consultant who does not speak (or talks poorly) in a native language is an invitation for disaster. Don't expect a translation to assist you with this issue; the goal of a consultant is to grasp all the complexities of your operations, which cannot be accomplished through a third party.

5) Conflict of interest: Hire a consultant who exclusively sells consulting services. Avoid those who

