Top Tips to Prepare for an ISO 27001 Audit

Preparing for an audit can be incredibly stressful, and ISO 27001 is no exception. Months of hard work and preparation, all come down to just a few meetings with an auditor, where the proverbial magnifying glass is put to your organization, and used to scrutinize your efforts. This process can be even more stressful if it's your first time, and you don't know what to expect. Well, take a deep breath, and let out a sigh of relief, because after hundreds of audits we have come up with the 5 top tips and best practices that you need to know to make sure your audit goes smooth, and stress free!

Upload/send evidence as early as possible

While being the auditee can certainly be stressful, the job the auditor has is no walk in the park either. Speaking and answering questions on behalf of the International Organization for Standardisation requires vast amounts of knowledge, expertise, and an exceptional eye for detail. Between planning, performing audits, reading pages upon pages of policy documentation, reviewing hundreds of evidence items, drafting reports, and much more, an ISO 27001 audit is far more than just an easy day in the office for your auditor. This is why providing your auditor with necessary evidence items sooner rather than later is such an important step. This gives the auditor more time to review your evidence, which in turn makes their responsibilities easier to manage, which means a happier auditor! Not only this, but providing your evidence early can significantly reduce the amount of time the audit itself may take, as there is more time before the audit to search for answers to questions they would otherwise have to ask you. By having evidence organized and given to the auditor around 2 weeks before the audit is scheduled, we've seen audit times cut down to as much as half their original schedule!

Complete a readiness assessment

While these will vary from firm to firm, reputable and experienced compliance auditing firms such as A-lign, often provide a tool for you to self-assess whether or not you have all your necessary documentation and evidence ready before the audit begins. These assessments do a fantastic job of highlighting details you might have glossed over, and helping you avoid common gaps and pitfalls. These assessments are more than worth the time and effort to complete, and we highly recommend completing them before finalizing and sending your evidence.

Ensure all relevant parties are engaged and present

While this may seem a little obvious on the surface, it is vitally important to ensure you have all of the correct members of your team involved and engaged in the audit process. It's very likely that a singular person in an organization can give detailed answers to questions around everything from technical controls, software development procedures, HR functions, building security, and even cryptography and asset management. Always review your audit schedule, which will include what controls are being covered on which days, and ensure that you have the best people available to answer questions, and help the auditor understand your organization's context.

Stay organized! Ensure you have controls mapped to their location within your policies

Just as, if not more effective at streamlining your audit than tip number 5, mapping your controls within your policies BEFORE the audit is a crucial step missed by almost every first-time auditee. An ISO 27001 audit is conducted by flowing through all the applicable Annex A clauses, of which there are 14 total. Each clause has a series of accompanying controls, in which specific measures are outlined that must be followed, and have evidence provided for during the audit. Many of the controls are elements required within your organization's policy documentation. With each of these controls being reviewed during the audit, you could imagine how much time would be wasted, and how embarrassing it could be to be asked about a control, and having to fumble around, searching for the corresponding clause within your dozens of policy documents in real time while the auditor sits there waiting for you. By mapping the controls to the corresponding policy, and location within that policy before time, you can move quickly and easily through the process and be infinitely more prepared to answer additional questions from the auditor without hesitation.

Answer all questions clearly and concisely

While these tips aren't necessarily in any particular order, this one undoubtedly is the most important to remember. Some more experienced auditors have been reviewing these same clauses, and asking some of the same questions for years or maybe even decades. It is critical to very carefully listen to an auditors questions, and ensure that you are answering in the clearest, truest, and most concise way possible (emphasis on concise). The auditor does not need a 15 minute anecdote when the answer could be as simple as 'yes' or 'no'. Now, this isn't to say you should only answer yes/no or never give additional context to your answers, but consistently giving more information than is necessary can very easily make things hard for the auditor to understand, and more often than not, opens the doors to even more questions that would otherwise not have been asked. With a potential for a grueling week of inquisition and

scrutiny, being sure to answer the question that was asked, and ONLY the question that was asked, with clarity and concision will help ensure a fast, and painless audit for all involved!

These are just a sample of some of the most important things we have learned over our years of experience and 100’s of audits. While there is still far more to know, if you follow these 5 tips, you’ll be well on your way to a smooth and successful ISO 27001 certification. Still feeling overwhelmed or need more help? Contact us for a free consultation!