Iseo Blue.

Top Tips For ISO 27001 PLAN 2024

My Key Advice

Setting off on the wrong foot can be a painful learning experience with ISO 27001, so I've wrapped up some of my biggest learning experiences here.

Explore The ISO Toolkit

Understand Your Scope and Avoid the Goat Rodeo

One of the biggest challenges organisations face is defining the scope of their ISO 27001 implementation.

Aiming too broad initially can lead to chaos, particularly in larger, more complex organisations. Instead, consider adopting a phased approach.

Begin with a simple, reduced scope in the first year, focusing on a specific service, business function, or team. This approach allows you to establish a solid foundation before gradually expanding the scope in subsequent years. This strategy helps avoid the 'goat rodeo'—a chaotic, unmanageable situation with diverse stakeholders pulling in different directions.

Don't Try to Do It in Isolation

Attempting to achieve ISO 27001 certification single-handedly is a recipe for disaster.

This process requires collaboration and support from various parts of the organisation. Engaging others not only distributes the workload but also brings in different perspectives and expertise.

ISO 27001 is a team effort; leverage the knowledge and skills of your colleagues to build a robust Information Security Management System (ISMS).

Set Up a Project Team or Steering Group

Having senior support and a dedicated project team or steering group is essential. This team should be cross-functional, including representatives from HR, Legal, IT, and other key areas.

Their role is to make crucial decisions, such as policy approvals and risk mitigation options. With senior backing, your project will have the authority to implement necessary changes effectively and swiftly. Leaving out key areas can result in resistance and undermine the changes you are trying to implement.

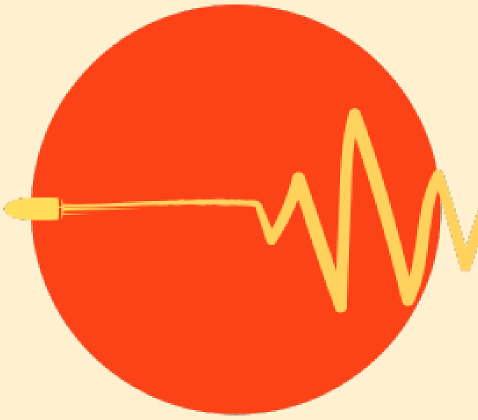
Ready – Fire - Aim

Perfection is the enemy of progress. ISO 27001 certification is not about achieving perfection from the outset but about continuous improvement.

The 'Ready – Fire – Aim' approach encourages you to take action, learn from the outcomes, and adjust accordingly.

This iterative process helps identify areas for improvement and implement changes that bring the most significant benefit to your organisation's information security. Every business is unique, and what works for one may not work for another.

Embrace a mindset of continuous learning and adaptation.



Engage with External Experts

Bringing in external experts can provide invaluable insights and guidance throughout your ISO 27001 journey.

While internal knowledge is essential, external consultants or auditors bring a fresh perspective and expertise that may be lacking in-house. They can help identify gaps, offer best practices, and ensure that your approach aligns with industry standards.

Engaging with experienced professionals can streamline your certification process and mitigate potential risks early on.

Remember, leveraging external expertise doesn't undermine your team's capabilities; it complements and enhances them.

Work out Why You Want It

You'll find plenty of organisations promising 'ISO weeks' if you search the internet. It's entirely possible, but...

Ask yourself what the primary reason you want ISO 27001 is? Is it for the certificate (so you can wave it at potential customers) or is it so you have confidence in robust security around your data?

If it is the former, then fine, take the rapid route to ISO, and I wish you every success.

If however, it's the latter, and you want better information security practices, that doesn't come in a week or two. Like any worthwhile change It's a long haul, takes time and constant reflection and improvement.

Being honest with yourself allows you to identify the pitfalls. A rapid approach to 27001, throwing out documents every few days, and then forgetting about it all until the next ISO audit might get you a certificate, but isn't going to get you strong security practices.

In Conclusion

ISO 27001 can be as tricky as you allow it to be. There's the easy way and the hard way. The recommendations here are about identifying the easy way.

Start with a manageable, reduced scope to help you avoid the chaos of trying to do too much too soon. A phased approach allows you to build on a solid foundation and expand your scope methodically over time. Adopt a continuous improvement mindset, rather than seeking perfection, will keep you moving forward.

Engage various parts of your organisation ensures diverse perspectives and expertise, making your Information Security Management System (ISMS) more robust and effective.

Establish a dedicated, cross-functional team with senior support to enable swift and authoritative decision-making.

And don't be afraid to get help; a coach, a consultant – someone who's been there, done it and got the t-shirt and scars. Their help can be invaluable.

Iseo Blue.

The ISO 27001 Toolkit

Written by Alan Parker

June 2024