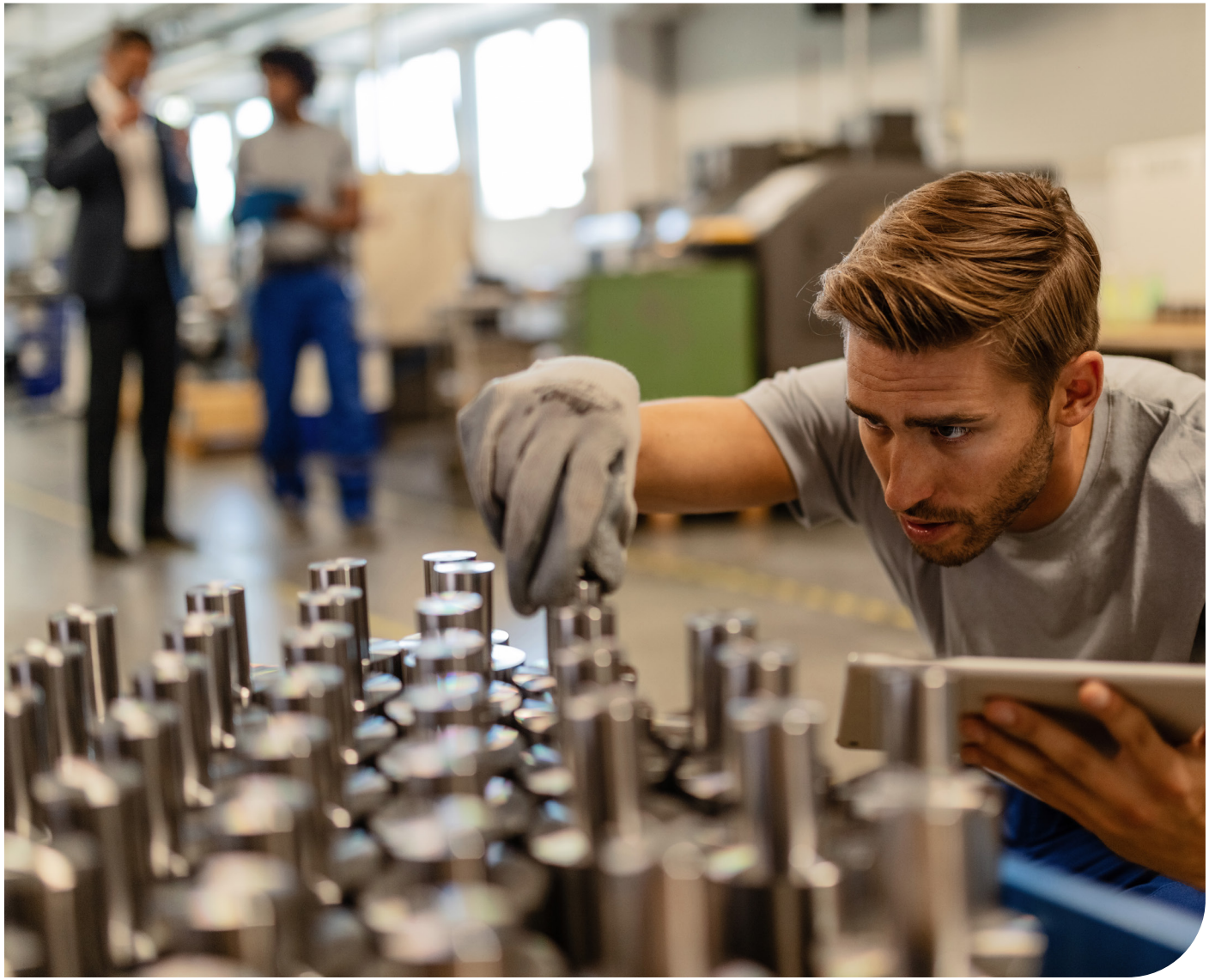
Your ISO/IEC 27001 journey: A step-by-step guide to implementation

Protecting your data is more important than ever before, as so much of our personal and professional lives take place in the digital world. Adopting ISO/IEC 27001 can help keep your business' valuable data safe.

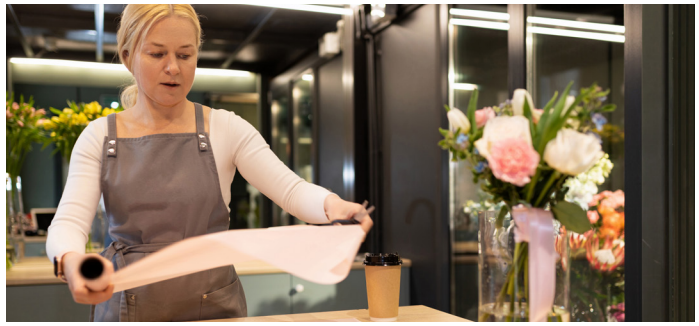
Once you're ready to implement ISO/IEC 27001, it's time to start planning how you'll embed the standard into your organization. This step-by-step guide will help you create and plan your implementation strategy and get you ready to start your ISO/IEC 27001 journey.

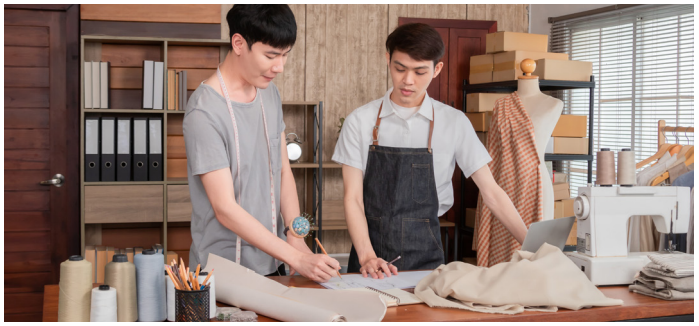


1 Make sure it's a team effort

Implementing any standard needs buy-in at every level of your business and ISO/IEC 27001 is no different. To successfully adopt it, you'll need the buy in of your stakeholders, staff and management teams.

- Tell everyone about the standard: why it's being adopted, what will be improved and how it will benefit both individuals and the wider organization.
- Invite open and honest discussion to talk about any doubts or concerns people may have about the changes being made.
- Create workgroups involving staff from across the business. Establish defined roles so people are responsible for the adoption of the standard, meeting deadlines and ensuring the implementation process goes smoothly.





2 Create a time and cost budget

Understanding and planning the resources you'll dedicate to adopting ISO/IEC 27001 can prevent unexpected costs and, naturally, the more time and resource you can devote to implementing the standard, the faster things will progress. Consider who should be involved in implementing the standard and what kind of support you think you'll need.

Try BSI's simple to use Impact Model tool to see how ISO/IEC 27001 could benefit your business

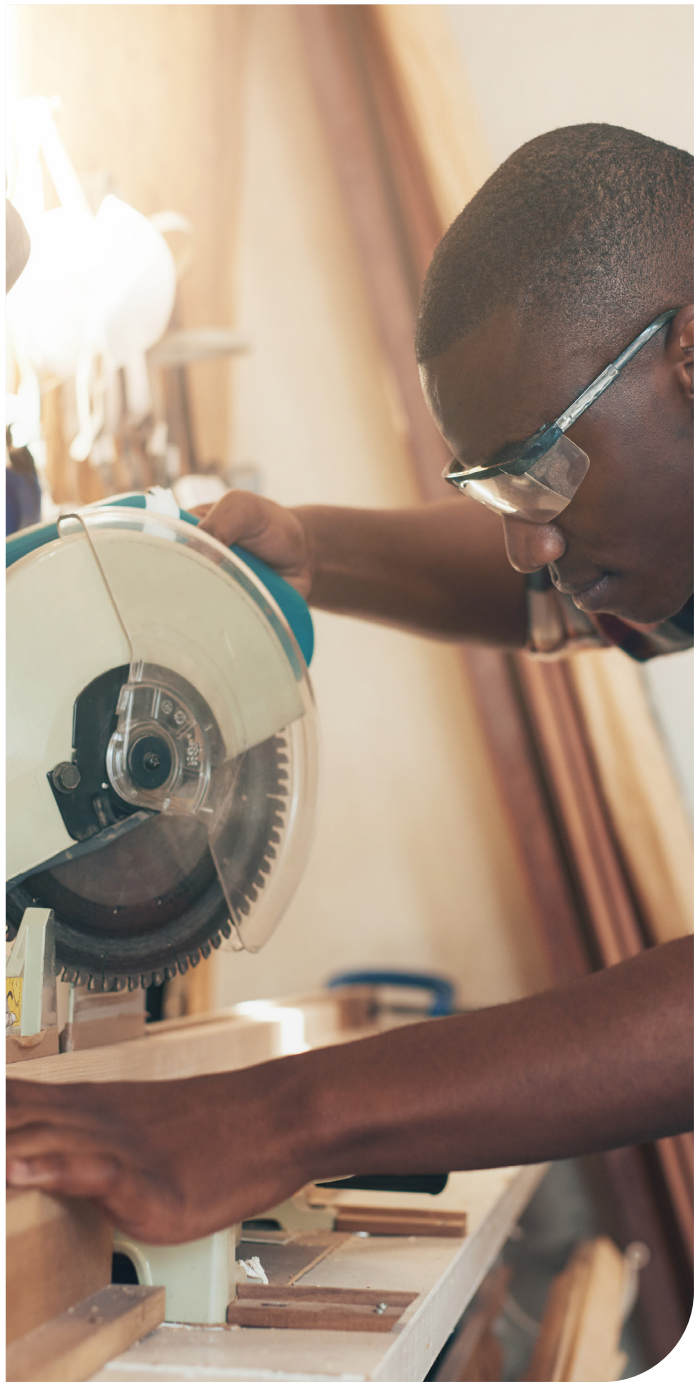
Organizations recognized by the UK Accreditation Service (UKAS), like BSI, can help at every stage of the implementation process; look for training courses or seek out advice about the standard.

- Don't skate over the details - create a realistic plan that puts aside time for the audits, takes into account holidays and includes even minor costs, like the price of the standard.
- Do your research to see how other companies have implemented ISO/IEC 27001 and how long it took them, but remember every organization is unique.

3 Review existing processes and start planning

With a budget and timeframes in place, you can start planning how you'll adopt ISO/IEC 27001; it can take between 3 and 12 months (source), depending on how quickly you want to implement it. Begin by looking at what you already have in place; this'll give you a clear view of how the standard will slot into your business and any areas that might be more complex.

- Review your existing information security processes and record everything you find - you can use this as a benchmark to monitor progress against. You may already do much of what's in the standard, but make sure it's adding value to your business - not just being done for the sake of it.
- Establish the threat landscape, the risks it poses to your business and the scope of your ISMS. It can just cover a specific service you offer or your entire organization.
- Use the steps in the standard document to plan effectively. Followed correctly, ISO/IEC 27001 walks you through identifying your information assets, carrying out a risk assessment and developing your ISMS policy.



4 Keep motivation levels up

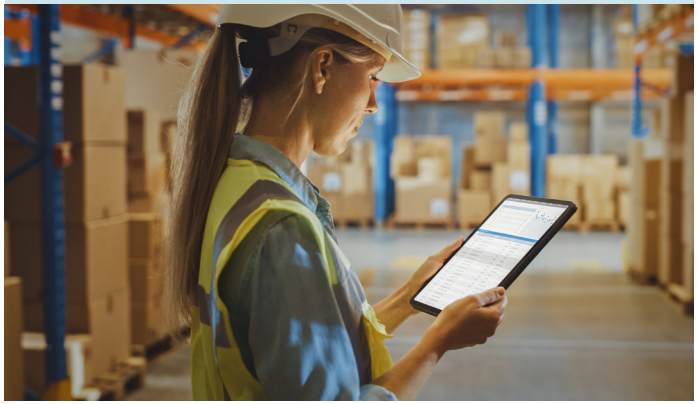
Although an end goal of certification may give you the ability to tender for bigger, more profitable projects, maintaining motivation throughout the implementation process is essential if you want to get the best results.

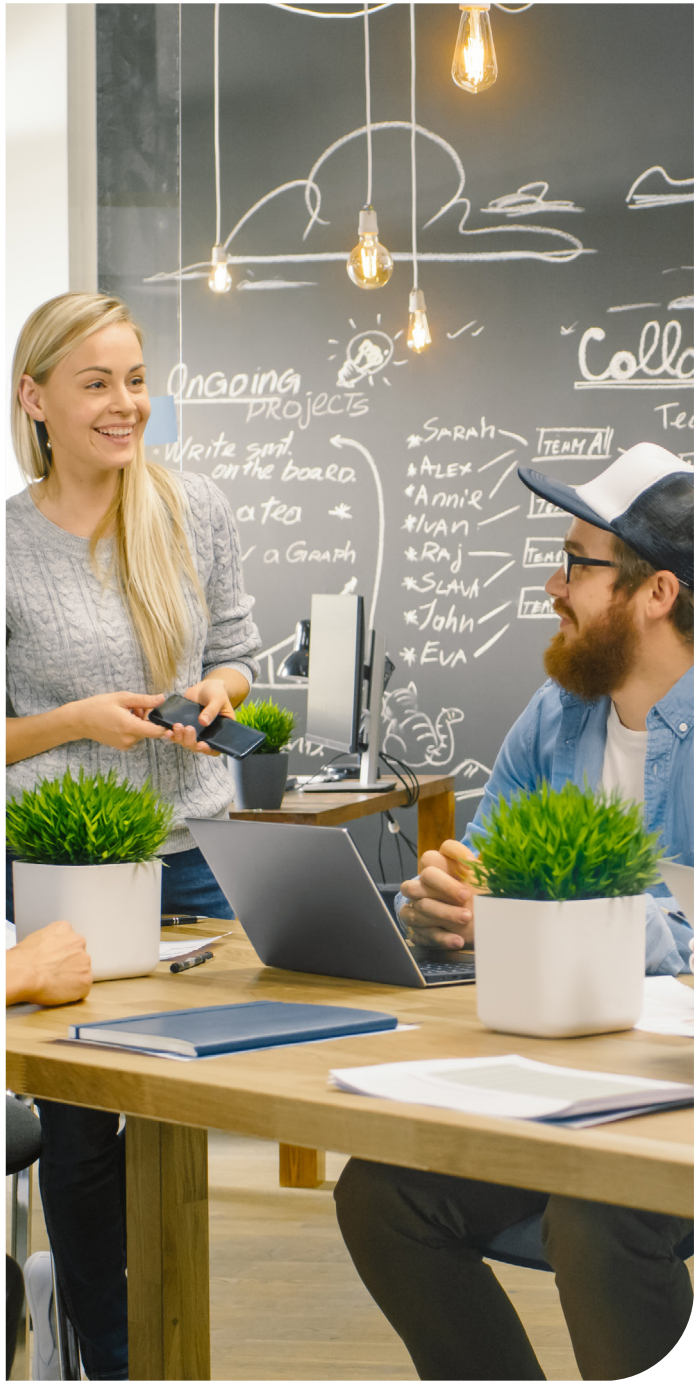
- Acknowledge small wins, celebrate major milestones and share progress with the wider organization to keep everyone in the loop and ensure the adoption process is a positive one.
- Get regular feedback from customers and suppliers, as they can offer fresh insights into how you operate. Ask for suggestions and feedback on your service which you can work into your implementation strategy.
- Encourage staff to take up any available training opportunities and learn as much as they can about ISO/IEC 27001. This can provide useful skills and training, such as individuals becoming internal auditors.
- Communicate the additional benefits achieved with each recommendation you adopt to team members, helping them to understand the incremental differences each action has upon the organization.

Certification or non-certified?

There are two ways to use a standard: certified and non-certified. You can get all the process enhancements, efficiencies, and risk reduction benefits from implementing the recommendations in a standard without certification. You don't even need to implement all the recommendations.

If you are looking to make business improvements, you can select the parts of a standard that best suit your needs and adopt them. But remember, the more recommendations you follow, the better your business will run. However, if you want to be able to demonstrate to your customers and stakeholders that your business can be trusted and is running with optimal process, then adopting all the recommendations in a standard and getting certified by a UKAS accredited organization, such as BSI, is the most effective way of doing this.





5 Understanding certification

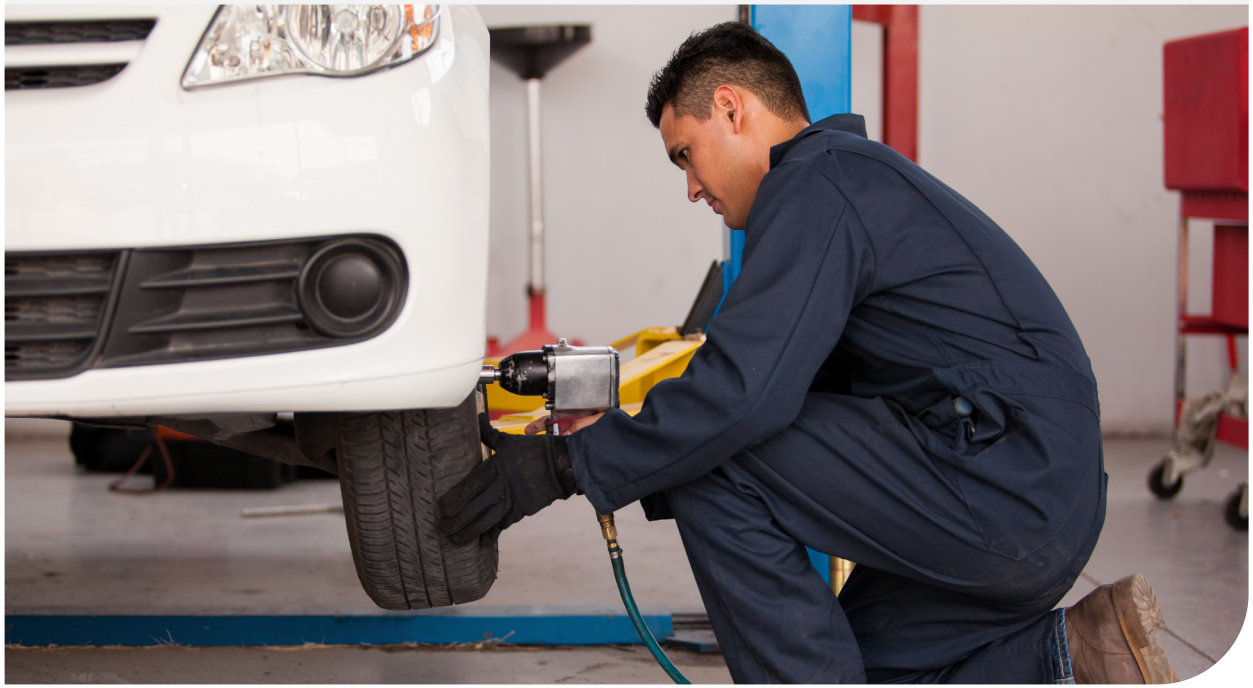
Whether you implement the whole standard, and apply for certification by a third party, or just implement some of the recommendations in the standard, the implementation process is really just the beginning of your journey. Adopting the standard gives you the tools and knowledge to keep reviewing your ISMS and ensure your data is secure, as the standard continues to change with the latest best practice advice and expert guidance.

- To be certified, you'll need to apply through BSI or another third-party certification body. The assessment is broken down into two stages:
  - **Formal assessment:** This is a two-stage process. First you (or a third party) will need to review your organization's readiness for assessment by ensuring the necessary ISO/IEC 27001 procedures and controls have been developed in your organization.
  - **Stage 2:** Next, if all the requirements are in place, the assessment will examine the implementation of the procedures and controls within your organization to check that they work effectively. If they pass, you'll receive certification of ISO/IEC 27001.
- Check your mindset! Instead of seeing each audit as a hoop to jump through, focus instead on how you can ensure your processes and systems are as safe and robust as possible - and that they're continually improving.

Start your standards journey...

The certification process isn't compulsory - if you want, you can choose to follow the standard and adhere to its guidance without ever receiving formal certification. However, while this offers the benefits of the standard, including improved processes, reduced risk of data breaches and therefore reduced risk to reputation and financial penalties, many businesses find certification gives them an edge when marketing, pitching and bidding for contracts.

However you choose to adopt ISO/IEC 27001, your journey begins with implementation. By communicating clearly with stakeholders, customers and staff and thoroughly planning the adoption process, you can start your standards journey on the right foot and ensure your information security is robust and effective well into the future.



Start your standards journey

Visit the BSI Shop to explore over 60,000 standards. To find out more about ISO/IEC 27001 contact our customer service team on 0345 086 9001.