Adopting ISO/IEC 27001 - Your next steps

Introduction

With more and more of our daily lives taking place digitally, managing your data is more important than ever before.

ISO/IEC 27001 provides a best practice approach to help organizations manage information security, look after commercially sensitive data and keep their business safe and secure.

Standards set out approaches that can be adopted by any size business; to successfully implement and embed a standard it's important to plan how your business will use this expert knowledge to best effect. Follow these steps to discover how your organization can benefit from the adoption and implementation of the best practice advice found in ISO/IEC 27001.

Step 1 - Get everyone involved

Discuss the possibility of adopting ISO/IEC 27001 with stakeholders, team leaders and staff to ensure it will add value to your organization and that everyone is on board with the implications of adoption – an ISO/IEC 27001 training session provided by BSI or other UKAS members, or an external consultant can help with this.

Benefits of ISO/IEC 27001 experienced by BSI customers (source)

75%
Reduces business risk

80%
Inspires trust in our business

71%
Helps protect our business

Step 2 - Plan, prepare, preview

There's plenty of information about ISO/IEC 27001 within the BSI website and you can also preview the standard at BSI Knowledge. Take time to read these and check that ISO/IEC 27001 is right for you and your business needs.

Your choice: Certification or non-certification?

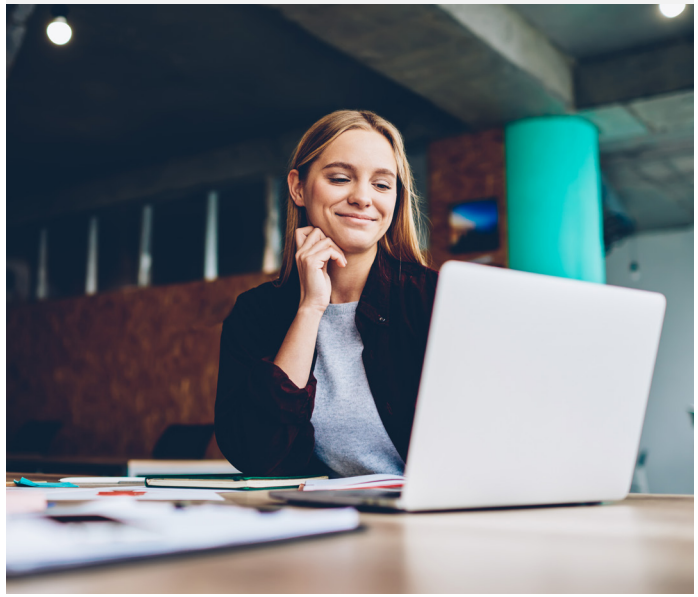
It's up to you whether you take the assessments that will help you achieve ISO/IEC 27001 certification or prefer to pick and choose the elements of the standard that have most relevance and impact upon your organization. There's no right or wrong way – it just depends on what's right for your business.

Top tip

When planning your implementation strategy, ask customers, stakeholders and suppliers for feedback on your current information security setup.

Step 3 - Get your copy of ISO/IEC 27001

ISO/IEC 27001 is inexpensive to purchase from BSI Knowledge. You can download a PDF of the full standard in minutes and start reading it, which will help you to understand the value it will add to your organization. You can now start planning your implementation strategy, thinking about how you will adopt the standard's recommendations and embed them into your business.



Best Practice Advice for SMEs

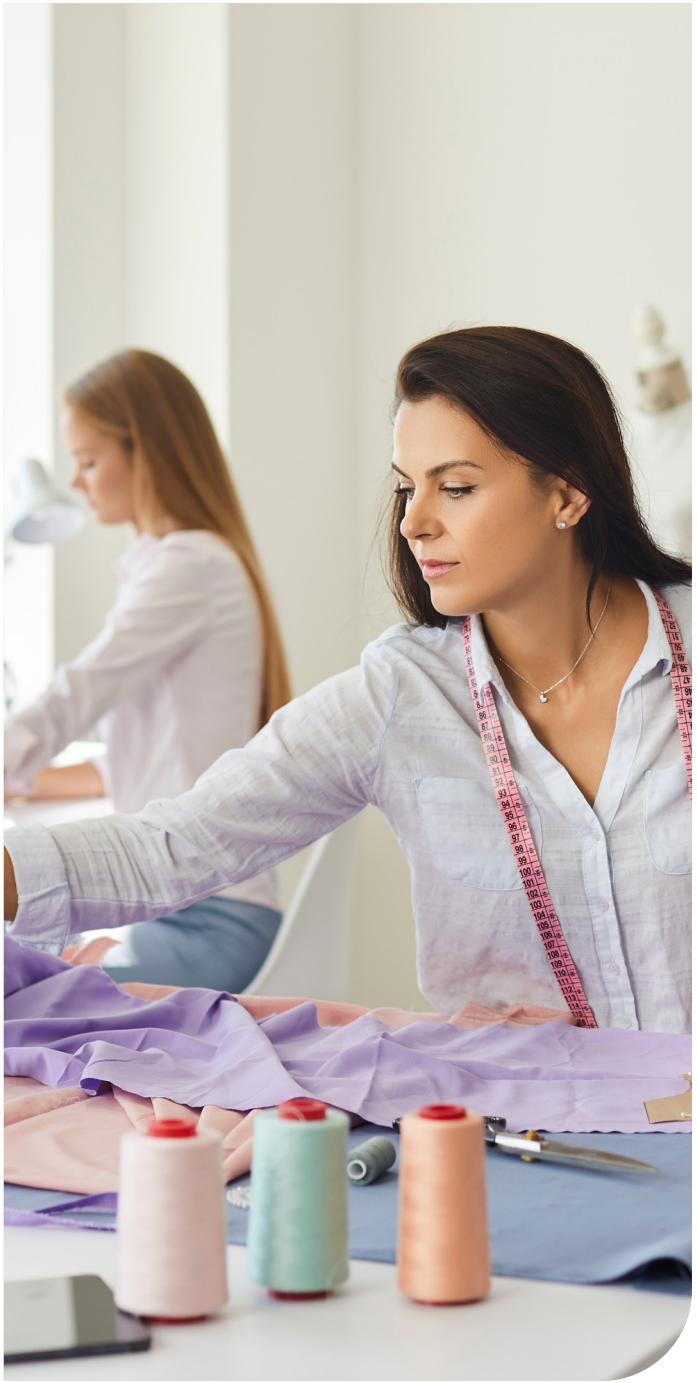
It doesn't matter how large or small your organization is, there are benefits to better protecting data for any size business.
ISO/IEC 27001 contains best practice approaches that improve productivity, effectiveness and data protection at every level.

Step 4 - Starting the implementation process

Once you've started implementing the processes and writing the policy recommended by ISO/IEC 27001, remember to review your existing processes and keep records as a benchmark to monitor your progress and positive change.

During implementation:

- Get commitment and support from senior management
- Create workgroups with defined roles, responsibilities and deadlines
- Compare your current system with ISO/IEC 27001 guidance



Step 5 - Time to get certified

If you wish to gain full certification, and demonstrate that you're meeting with industry best practice and your commitment to managing information safely and securely, there are various organizations, including BSI, who can help with this.

Get ready

Find a UK Accreditation Service (UKAS) approved third-party, such as BSI, to provide certification

Gap analysis

Maybe use an optional pre-assessment service to examine your existing ISMS and identify which areas need improvement to meet the requirements of ISO/IEC 27001.

Formal assessment

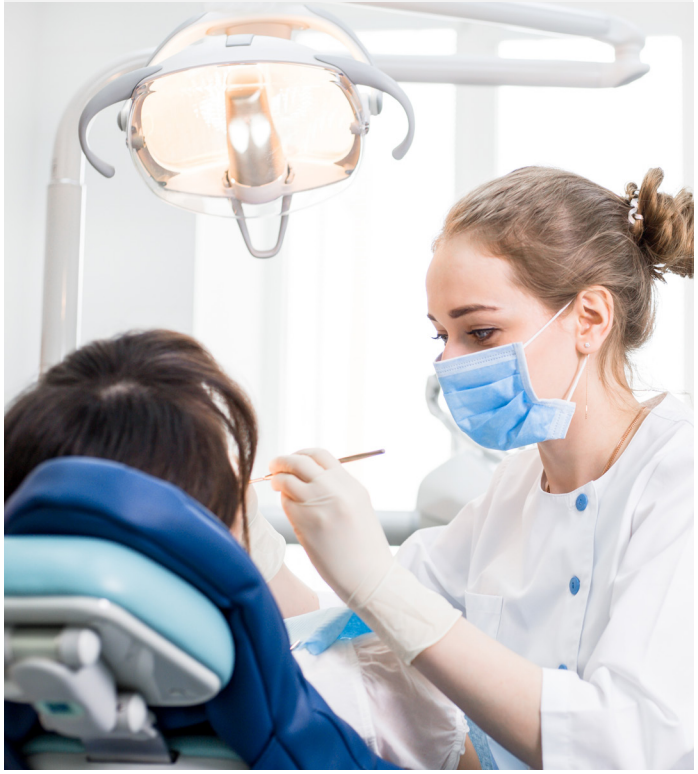
A two-stage assessment is carried out by a representative of the certification body who will examine how you're applying the standard and check necessary procedures and controls are in place.

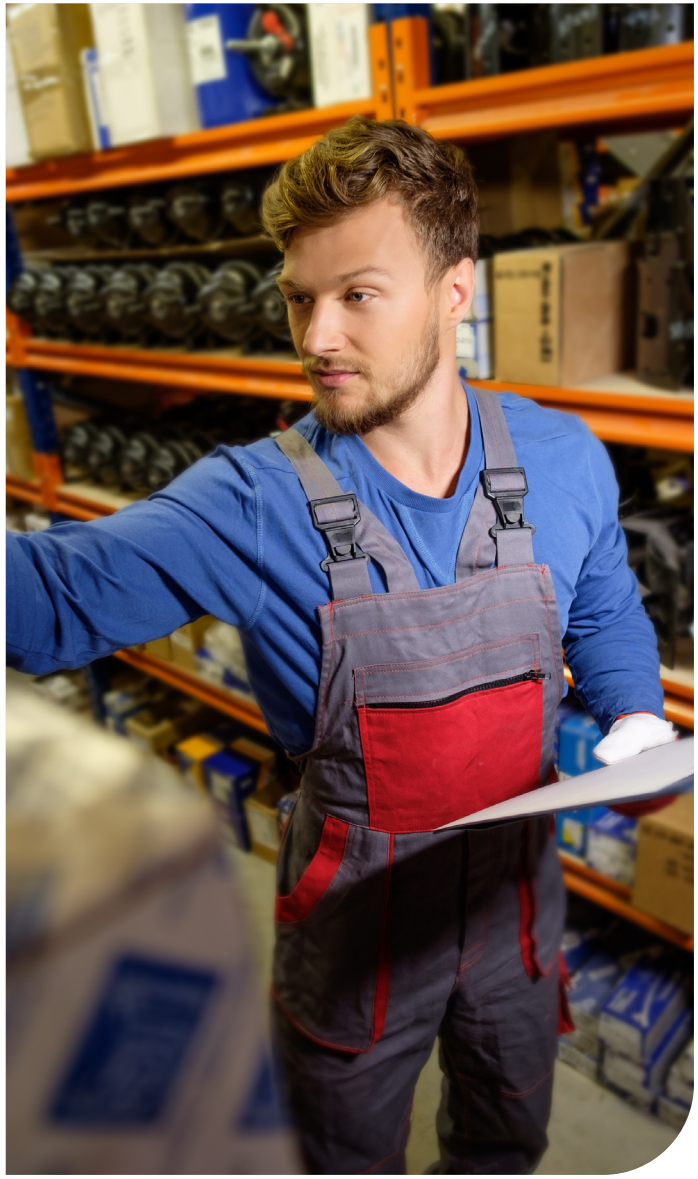
Certification

When you achieve certification, your ISO/IEC 27001 certification is valid for three years.

Step 6 - The journey begins

Getting certified is just the beginning of your standards journey. Once you're accredited, you'll have the skills and knowledge to continue assessing data security risks, identifying your business' vulnerabilities and improving your information security. With or without certification, ISO/IEC 27001 helps protect your data, your business and your reputation well into the future.





Start your standards journey

Visit BSI Knowledge to explore over 60,000 standards or, for more information around standards, contact our customer service team on 0345 086 9001.