bsi.

Standards at the Heart of Information Security

A guide to protecting your business information

By Royal Charter

Enabling better business

Contents

Your guide to information security and how an Information Security Management System can add value to your business

Information security: What is it and why does it matter?

Whether you're a small independent retailer or a larger corporate organization, your business handles lots of data every day. This could be confidential business information, personal details of your staff or even just files and documents that shouldn't be seen by people outside of your business. Any data breach, large or small, can have a significant reputational or financial impact on your business, whether from a cyber-attack, hacker or disgruntled employee. Securing your data is essential.

Types of data your business might handle

Customer contact information

Sales and prospecting data

Website traffic statistics

Budgets and forecasting documents

Personnel data

Medical records

Payroll and HR information

Intellectual property

3.1 billion potentially malicious emails are sent every day – yet 83% of SMEs aren't equipped to recover from a cyberattack.

Information security is the method of taking care of your data and making sure only approved persons can access or change sensitive documents. This can take many forms: you might keep confidential files on a hard drive under physical security (e.g. a safe), you may use software and digital security methods like encryption (scrambling a document's contents so it's impossible to read) or you may hold records in the cloud.

Laws like the General Data Protection Regulation (GDPR) aim to monitor and standardize – on an international level – how businesses in the UK and the EU store and handle data. But with so many different businesses and different ways to protect data, it can be difficult to know the best way to protect your business information. That's where ISO/IEC 27001 can help.

Information security: What is it and why does it matter?

Understanding data breaches

The phrase “data breach” might make you think of hackers and scams, but it can actually refer to any data being accessible when it shouldn’t be. While effective information security protects against direct attacks from malicious outsiders, it should also be able to guard against human error which is a frequent cause of data breaches.

Causes of data breaches

- Out of date anti-virus software
- Weak passwords
- Loss or theft of devices
- Downloading malicious software (malware)
- Aggrieved staff or ex-staff members
- Phishing emails

The British adoption of the ISO, BS EN ISO/IEC 27001 is a UK standard for information security. It’s an approach to protecting business data that can be applied by any size organization, in any sector, to continually improve how data is stored, managed and used.

Information security standards: Enabling better data security

Standards bring together knowledge and experience from across an industry, academia, the UK government and other sources to create a best practice approach to doing something. For information security, there are many standards that can show you how to identify, manage and mitigate risks to your business, prevent vulnerabilities and better protect your data.

Standards can show you how to:

- Assess your existing processes and the potential impact of adopting a standard
- Identify, prevent and manage potential risks by creating an ISMS (Information Security Management System)
- Create new information security policies and protocols
- Communicate new information security processes and systems to staff
- Continually evaluate and optimise your new information security processes

Information security: What is it and why does it matter?

Certified and non-certified

There are two ways to use a standard: certified and non-certified. To achieve certification, you'll need to follow all the recommendations in the standard, before being externally assessed on how well you've implemented it. This is the most beneficial way, as you'll not only reap all the benefits of every part of the standard you will also be able to tell your stakeholders you are doing so with third party assurance.

However, you don't have to get certified to enjoy benefits from the standard such as process enhancements and business improvements. You can still take on board the best practice outlined in the standard and apply parts of it to your business; the more recommendations you incorporate into your business, the more you'll benefit.

Information security in a remote working world

Many of us are now working remotely, be that in cafes, shared workspaces or from home. But the convenience of opening up a laptop and connecting to free Wi-Fi can disguise many potential information security risks.

Loss/theft of items

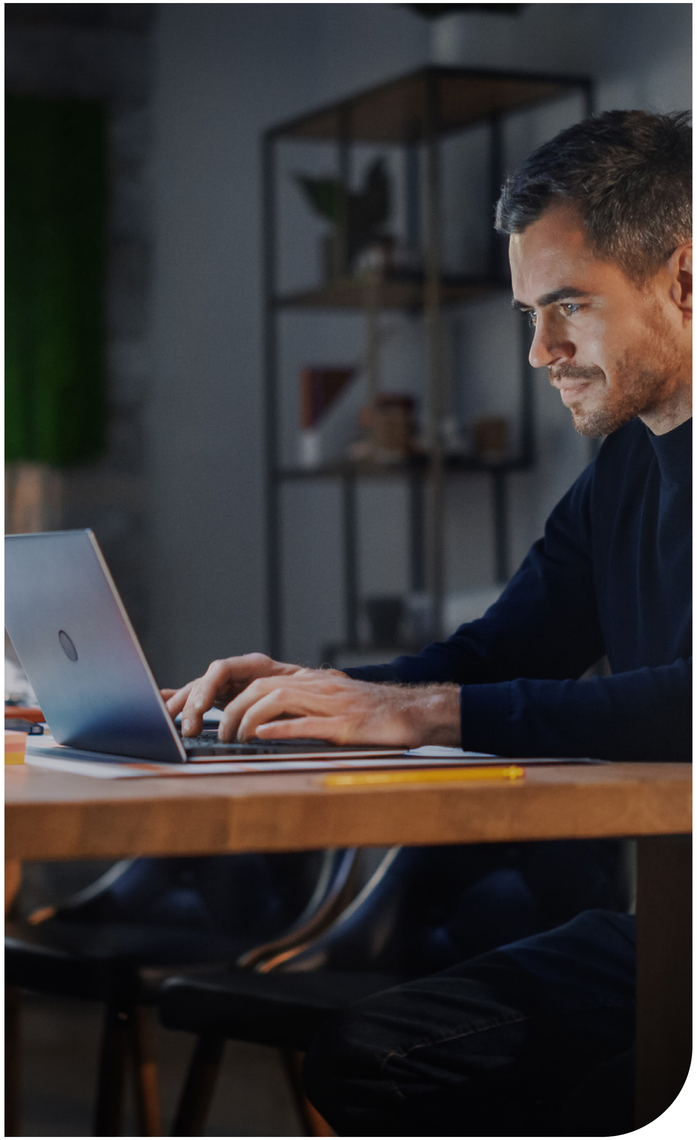
If you're travelling with mobile phones, laptops, memory sticks and other equipment you run the risk of accidental loss or the theft of these items. Any data stored on these devices is then potentially unsecured and in the public domain – that's a data security breach.

Connecting to public networks

Using your internet or mobile device to access the web via any connection other than your home or office setup can pose a threat to data security. It's impossible to know who else is using that network and, on public networks, your device and files may be visible to others.

Keep passwords secure

You can't be certain who else is looking at your screen – or if you've been targeted by keylogging software. Changing passwords regularly – even if you always work from home – can help keep information safe.



The benefits to your business

How information security standards can transform your organization

Taking steps to protect your data offers a wide range of benefits to your business - including some you might not expect.

Establishing an ISMS and improving data security positively impacts your business at every level, from its reputation to efficiency and productivity.

Increase trust in your business

80% of businesses using the standard report that customers feel reassured when they see that the business is adhering to information security standards.

Boost your reputation

Letting customers and staff know that you have taken measures to keep their data safe inspires trust and confidence in your business. Many business owners add their accreditation to all communications, so everyone can see their commitment to data security and quality standards.

Gain confidence

Enjoy the knowledge that you have taken a comprehensive, expert-informed approach to ensuring your ISMS is in order and your data is safe.

Reduce the risk to your business

75% of businesses which have adopted the information security standard ISO/IEC 27001 agree that it has helped them to identify and address potential security risks.

The benefits to your business

Get peace of mind

The recommendations laid out in the standard make data security lapses less likely. A big part of standards is the focus on continual improvement, even after accreditation – a standard is, at its core, an evolving approach to doing something in the best possible way.

Minimise mistakes and incidents

With a system in place designed to protect against human error, as well as malicious cyberattacks, you're less likely to spend time fixing potential breaches due to staff errors. That means you'll reduce costs and free up time to focus on more important aspects of your business, like growth or training.

Improve awareness of information security

Offering your team the opportunity to learn more about a topic as important and relevant today as information security is a great way to keep your team motivated and learning.

Get the advantage over competitors

Adopting a standard allows you to bid for projects or take on customers that might previously have been out of reach. With strong information security credentials, your customers will find you much more appealing than your competitors.

See the financial benefits that your business could achieve by using our ISO/IEC 27001 Impact Model.

5 facts you need to know about information security and standards

1 It's more important than ever to protect your company's information

Every business holds more data than ever before; in fact, over 90% of all the data in the world was created in the last two years. And yet for many organizations, IT and data security aren't a central focus. It's essential that you have a robust information security system in place; without one, you run the risk of a data breach that could cost you thousands of pounds in fines, lost businesses and reputational damage.

2 Information security standards give you a guide to protecting data

Standards are used by millions of businesses every day to improve productivity, efficiency, sustainability, product quality and more. Standards make this possible by bringing together experts in a field (for example, information security) and combining their knowledge in a document which can then be used by any other organization to improve how they do things.

3 Information security isn't just about your IT system

Hackers stealing data is what we tend to think of when we hear "data security", but many seemingly harmless actions can be a data security risk. Using a password that is too simple and can be easily guessed or sending an email to the wrong person are everyday things that can be potentially dangerous – and that an ISMS can help prevent.

4 You don't have to implement every recommendation to benefit from a standard

A small business will operate very differently from a much larger organization with multiple offices, and they'll have different data security needs, too. A business can start benefiting from an information security standard as soon as it implements the first recommendation – and those benefits only increase the closer you get to certification.

5 An ISMS can benefit the whole company

An effective ISMS can change your organization's entire data and IT culture for the better. As well as protecting you from cyber threats, an ISMS can help everyone work more efficiently by storing documents in one place; improve company culture by involving and educating everyone about data security; and reduce costs by minimizing risk and being more selective about data security methods.

Ian Waterhouse
Information Security Programme Manager, Legal Ombudsman for England and Wales

"ISO/IEC 27001 certification allows us to provide our clients with confidence that their information is being protected."

Next Steps – Implementing ISO/IEC 27001

To successfully implement and embed a standard, it's important to plan how your business will use this expert knowledge to best effect.

Follow the steps below to discover the best course of adoption and implementation for the information security standard 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 accredited organizations, or an external consultant can help with this.

Step 2 - Plan, prepare, preview

There's plenty of information available 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.

Step 3 - Get your copy of ISO/IEC 27001

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

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

To demonstrate your commitment to managing information safely and securely, there are various organizations, including BSI, who can help with this.

- **Get ready:** Find a third-party to provide certification such as BSI or other organizations recognized by the UK Accreditation Service (UKAS)
- **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. You only have to implement the standard once, but you'll protect your data and reap the rewards well into the future.

Certification and beyond

Starting your standards journey

When you've chosen a standard, one important decision you'll need to make is whether or not you want to get certified. It's not compulsory and, while many businesses choose to go for certification, other organizations find they can benefit from using the standard more informally.

Certified

Certification is a gold standard that shows your clients, customers and stakeholders that you have gone the extra mile – it demonstrates your commitment to something, for example keeping the data your business holds safe.

For many businesses, once they've started implementing a standard and begun to see the benefits, they're encouraged to keep on going to certification. Once certified, it's reassuring to know that best practice is in place and that you have the knowledge and skills to keep optimising and improving.

Certification is when an external auditor assesses how accurately and effectively you have implemented a standard. You'll have to contact a certification body such as BSI or any other organisation accredited by UKAS, to organise this process and ensure you keep up with the standard to remain accredited.

> **Senior Operations** IT industry
>
> “[Information security] is what we do, so we had a lot of [the standard's recommendations] in place already. Having the certification keeps clients spending with us – it's worth it just for that. I think it's good that one personcan't do it alone, it has to be a joint effort and commitment and that's why it gets embedded and you're always improving.”

Non-certified

Adopting a standard more informally (non-certified) simply means that you don't have to go through the certification process. You can still achieve all the process and business enhancement benefits implementing the recommendation in the standard brings. Or you can choose the recommendations that will have most impact on your business and only implement them.

For example, with a standard like ISO/IEC 27001 you could choose to undertake the risk assessment and identify any vulnerabilities, create an ISMS and come up with new data security policies, but you may not want to conduct an internal audit yet. You'll still reduce the risk of data theft and increase awareness of data security, but you'll not have the third-party assessment which will enable you to prove to your customers and stakeholders you are adhering to the recommendations in the standard.

You can always start adopting a standard informally and gradually build up to certification when you're ready – there's no time limit.

Certification and beyond

Do it your way

How you choose to adopt and work with standards is up to you. Make sure the standard you choose adds value to your business, offering tangible improvements to how you operate – don't adopt a standard just because you feel you ought to. There's no right or wrong way – it depends on what works best for your business.Now that you're familiar with information security and have a better understanding of how to implement a standard like ISO/IEC 27001, it might seem like receiving your certification is the end point – but it's just the beginning of your standards journey.

Data Protection Manager marketing and branding agency

> "As you work through it, you realize it all makes perfect sense. I felt so much more aware of risks to our enterprise but in a much better position to address them... It's allowed us to reach more clients and that has to be a benefit for every single person there."

Standards to suit every size

How standards can have a big impact on smaller businesses

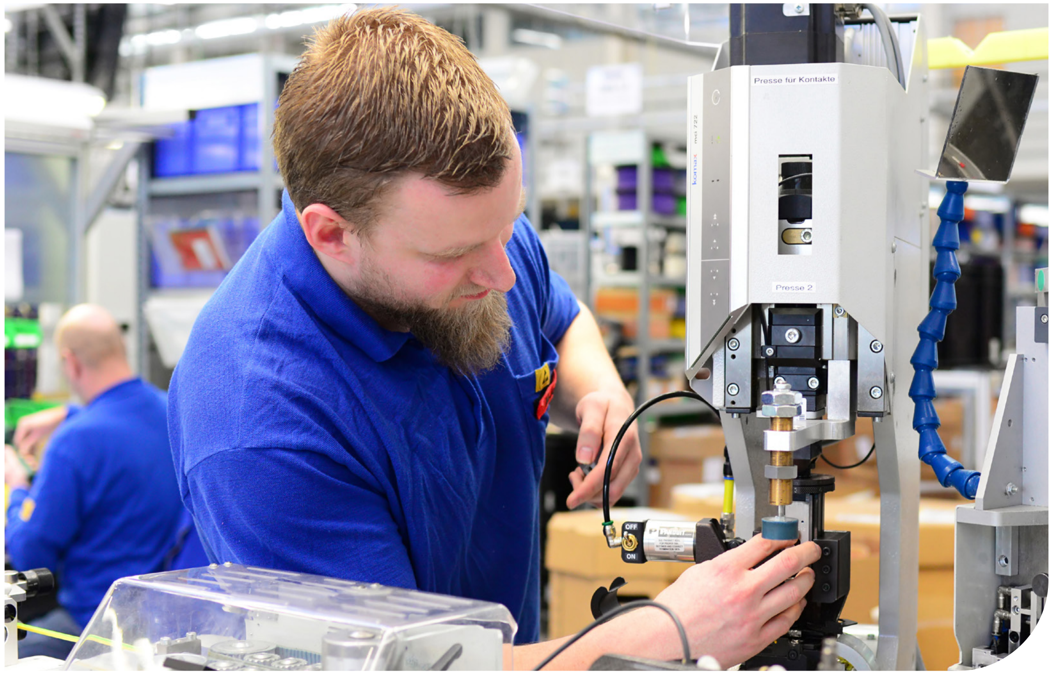
For any size business, standards can improve the quality of your products and services, make your entire organization more efficient and ultimately boost your bottom line.

Standards offer a tried-and-tested best practice methodology for doing things. By providing an expert-led approach to a process, system or product, standards can save small businesses a lot of time in the testing and trial-and-error stages, meaning that you don't have to reinvent the wheel. Standards are, in essence, one of the most affordable forms of consultancy available.

> “
> **Paul Brazier** Commercial Director, Overbury
>
> Don't try and change your business to fit the standard. Think about how you do things and how that standard reflects on how you do it, rather than the other way around.”

For example, ISO/IEC 27001 gives you a practical framework to examine, review and continually improve your information security. Rather than outsourcing your ISMS, or learning through trials what works and what doesn't, the standard gives you everything you need to do to meet the highest levels of data protection.

> “
> **Lyndon Wild** MD, Laminar Medica
>
> Having the standard in place plays an important role when we are bidding for work and it has almost certainly brought us new business. When we tender for contracts I'm sure we gain points because we comply.”



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.