BEGINNER'S GUIDE TO BS 10012 : 2017

Personal Information Management System (PIMS) Requirements Explained

QMS

INTERNATIONAL

What is BS 10012 : 2017?

All organisations work with personal data, whether it concerns their employees or their customers, and one of the best ways that a company can show that they are taking the management of personal information seriously is through the BS 10012 framework.

BS 10012 allows businesses of any size and within any industry to control risks to data privacy, and ensure that the data they hold is managed according to industry standards and both UK and European legal requirements concerning data protection.

Why use it?

With the publication of increasingly more stringent legislation, higher fines for companies who do not adhere to legal requirements and increased concern from interested parties, businesses are finding that they need to pay extra attention to data protection and personal information management.

A certified organisation will be able to support and promote good data protection practices and balance these with their business needs – financial or otherwise. They will be rewarded with an enhanced reputation for taking the security and privacy of their customer’s data seriously, whilst reducing the likelihood of being fined for not following data protection regulations.

In statistics published by the Information Commissioner’s Office (ICO) for the year 2017/18:

£5.6 million
Total fines issued by ICO

£400 thousand
Maximum fine issued by ICO

£125 thousand
Average fine issued by ICO

3.3 thousand
Reported data security incidents

Source: ico.org.uk

How does it work?

BS 10012 : 2017 is built around 7 areas...

1 Context

What?

You need to outline and communicate your organisation's responsibilities.

Why?

By setting out your organisation's goals, commitments and responsibilities you are proving that your business is committed to ensuring personal data is protected and used responsibly.

How?

Start by identifying the individuals whose personal information your organisation will hold or use. Knowing who is impacted will identify potential areas to focus on. Don't just think about staff, consider potential customers and visitors to your website/office too.

With the affected individuals identified, you will need to work out your legal responsibilities toward them, their needs and their expectations. Make sure to think about how future projects or changes to your business will affect your plans.

It is important that you document and communicate this information throughout your organisation.

2 Leadership

What?

Leaders at all levels should establish a unity of purpose and direction.

Why?

A good leader will set an example for those below them by actively participating in and caring about the PIMS. By doing this they will be creating an atmosphere where everyone feels they can and should contribute to the company's data protection goals.

How?

As a business leader, you should take accountability for the safety and responsible use of the personal data you hold. Do this by understanding their needs and expectations in the first instance, and creating a PIMS policy based on these.

A PIMS policy should be your company's mission statement for data protection issues – a vision and strategy for responsible use and preventing loss or unauthorised access. Communicate this to all staff, visitors and contractors to ensure everyone knows what is expected of them then they can act with one purpose.

Review your policy periodically to ensure that it remains appropriate to your business and still meets legal obligations.

3 Planning

What?

You need to establish, implement and maintain processes and objectives.

Why?

Planning shows how forward-thinking and proactive your business is while allowing you to react quickly to any risks and opportunities that may arise.

How?

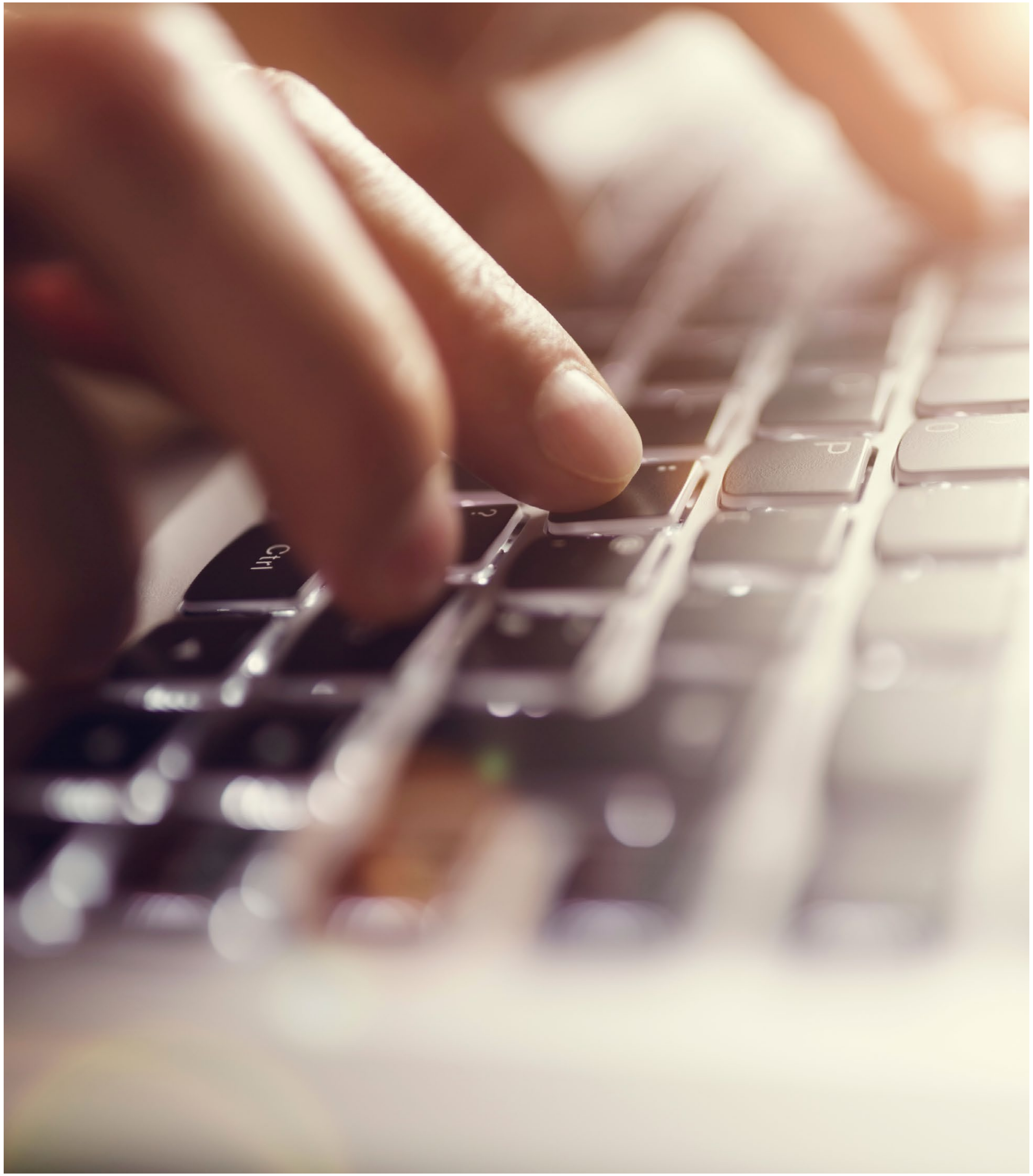
Start by defining a set of data protection objectives. A specific list of goals sets the expectations of your staff and any interested parties. Think about how you will measure the success – or failure – of these objectives, what resources will be required and who will be responsible for them.

Next, create a data inventory and flow which will identify key business processes that use personal data and how it is used. For each piece of information, categorise it and decide why you are holding it.

It is important to establish procedures for, and controls to eliminate, risk. Use Privacy Impact Assessments and risk treatment processes to facilitate this.

Finally, work out which legal data protection regulations your organisation must follow and determine a method to keep up-to-date with any changes.

Make sure to record all of these areas and keep your documents up-to-date.



4 Support

What?

Determine and provide the resources needed to fulfil your goals.

Why?

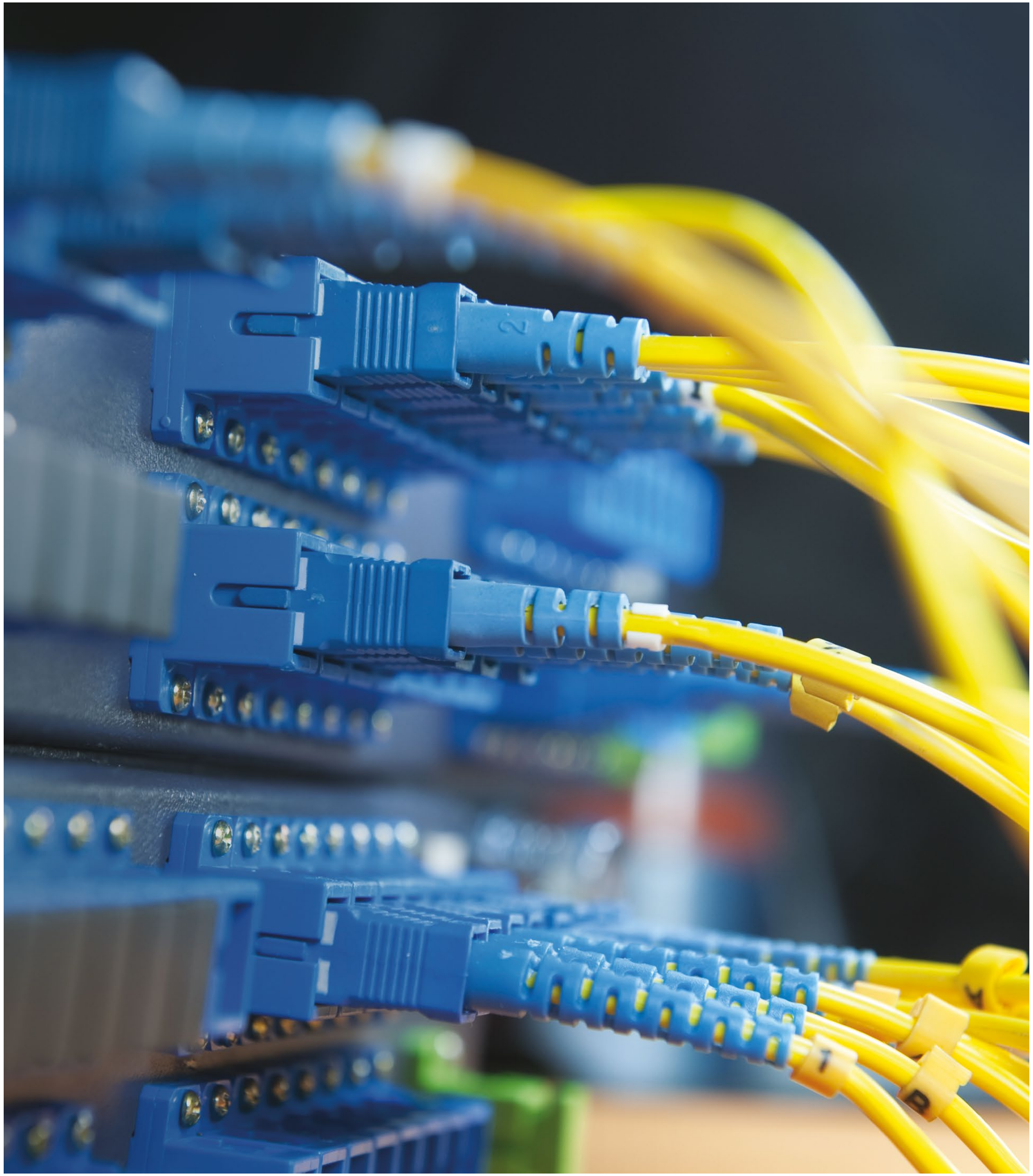
By allocating the correct resources for the task you will ensure that your business is in the best position to achieve your data protection goals.

How?

Supporting a management system covers many areas from providing the resources needed to achieve company goals, to training staff in how to handle specific issues. For data protection this is no different.

Make sure that everyone in your organisations is trained to respond appropriately to, and actively looks out for risks and emergency situations. Even if someone is not trained to handle a risk, they should know who to report it to.

Be sure to empower your people by giving them the resources, training and authority to act with accountability. Encourage them further by recognising and rewarding their contributions.



5 Operation

What?

The management system should be part of your day-to-day operations.

Why?

Data protection issues should be thought of as part of business operations – not just an afterthought once an issue has already occurred.

How?

Consider how your data protection goals can be met at every stage of your business life cycle and use your findings to design a series of controls to address them. Your controls should be aimed at ensuring privacy by design and reducing risk.

In addition, you will need to establish, implement and maintain a plan to address changes in your business, unforeseen issues and emergency situations.

Don’t forget to document and communicate your processes. Documents should be reviewed and updated regularly, and any changes communicated to relevant parties such as customers, employees and visitors.

You may need to assign a Data Protection Officer (DPO) if your organisation is large enough or there is a business need for one. This person needs to be qualified to perform this role and will be responsible for ensuring your PIMS is compliant with all legal regulations and will report to the relevant supervisory authority.

6 Performance evaluation

What?

You should monitor, measure, analyse and evaluate performance.

Why?

Evaluating your data protection performance allows you to identify and rectify issues early on, before they become a problem.

How?

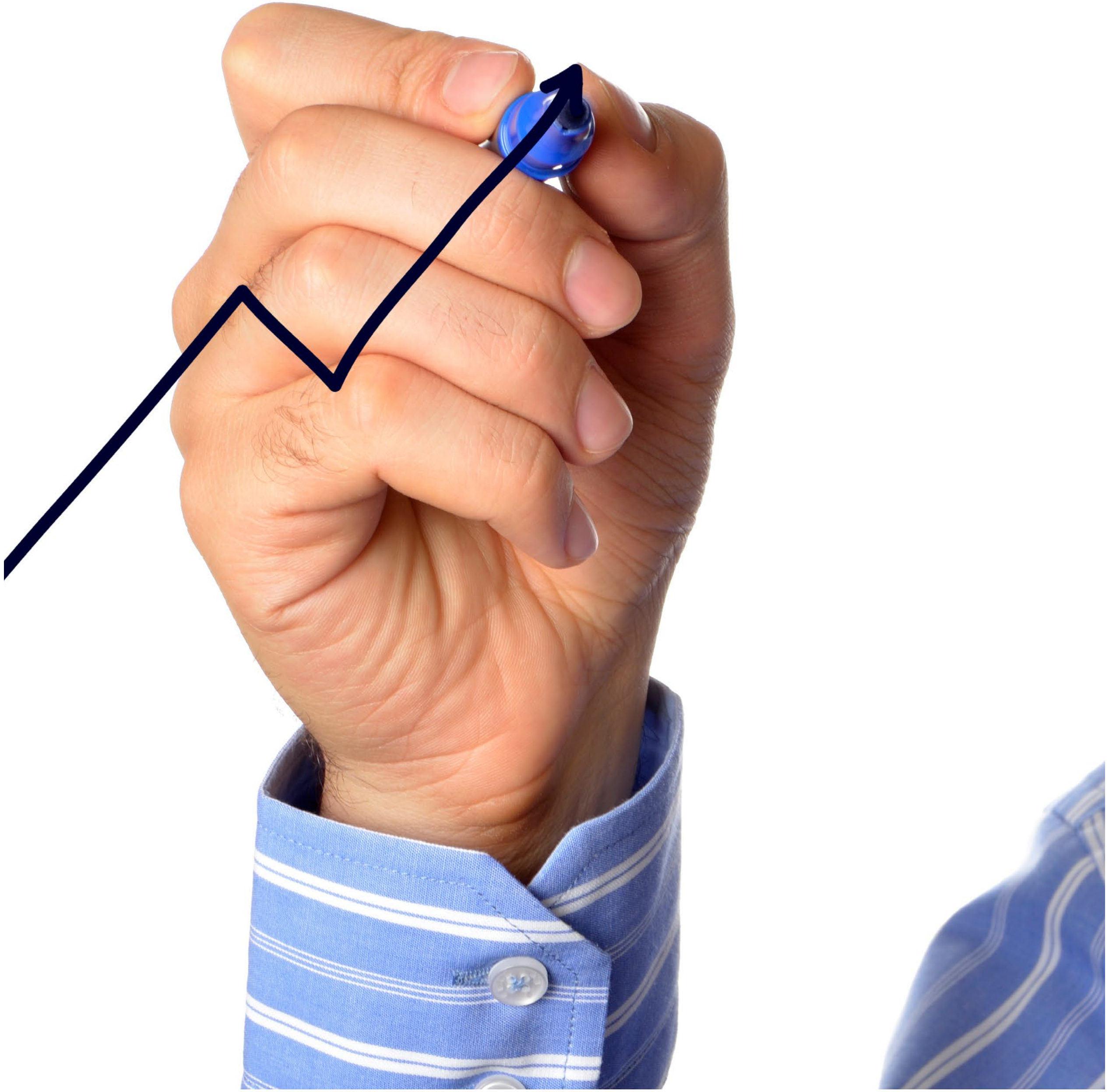
For all your identified controls, determine what needs to be measured to assess their success. Set out guidelines that will allow consistent measurement – especially for subjective areas.

As well as collecting data, analyse it to determine if a goal has been reached and if any improvements can be made to the process.

Internal audits are the best way to gather this data and assess individual departments on their adherence to the Standard.

Make sure to document everything from start to finish, not just your data but how you will collect and analyse it.

Communicate this to the relevant parties.



7 Improvement

What?

Successful organisations review their successes and failures.

Why?

The best way to learn how your business can repeat its successes and avoid past mistakes is to review and evaluate performance.

How?

It is important to create a plan for analysing your business' performance. Make a schedule as part of this which will ensure that reviews are held regularly.

Reviews should look at the results of internal audits, the general data protection performance of the organisation and any changing circumstances such as new legislation being introduced.

Make sure to take minutes of the items discussed and note any agreed actions. You should make sure to follow up on these actions in the next review which will ensure that your processes are always fit for purpose.

Who can help?

Implementing a BS 10012 Personal Information Management System is not something you have to do alone, and certification doesn't have to be expensive or complicated. If you are interested in the benefits that the BS 10012 standard can bring to your business, and are looking for an efficient approach which doesn't break the bank, QMS International can support you every step of the way.

Having helped implement thousands of Management Systems across the UK, QMS's market-leading services include everything from drafting a compliant Manual, to offering on-site training and Certification.

Figures shown below are taken from the QMS customer survey 2016.

Hassle Free Certification Process

Gain your certification in as little as 45 days.

99%

of clients were pleased with the speed of our certification process.

Experienced Consultants

With over 25 years' experience in the industry, our consultants have the knowledge and experience to help any organisation, in any sector.

97%

of clients were satisfied with the support given by QMS Consultants.

Accredited Certification Body

We are accredited by ASCB, and audited against ISO 17021, so you can be confident of our competence as a certification body.

96%

of clients are satisfied with the overall service provided by QMS.

By teaming up with QMS you can be confident that you are working with a consultancy & certification provider that puts quality and satisfaction first, whilst making the Certification Process as simple, efficient and cost effective as possible.

Contact Us

If you would like QMS to provide you with a straight forward and cost-effective route to certification, then get in touch today:

☎ 01603 630345 ✉ enquiries@qmsuk.com 🌐 qmsuk.com