You're not alone: QMS is by your side

One of the things that sets us apart, here at QMS, is our commitment to stripping away the hassle and making things work for our customers on a day-to-day basis. We don't want to see our manuals sitting on shelves. We believe in simple, practical ways of working to bring reduced costs, improved efficiency and enhanced reputation.

The best part is that even after you've gained certification, we'll continue to support you at every step. We also offer a range of support, training and certification services, to help you:

Training

Internal audits, Management Reviews, handling non-conformances and keeping your manual up to date can all seem a bit daunting. Don't worry. We'll help you and your team to manage every aspect of your Information Security Management System in a way that gets the results you need. We offer on site training courses, nationwide, throughout the year.

Support

QMS can offer support to any organisation with an existing Information Security Management System in operation. Our support packages start from £49 per month and include an annual on-site visit as well as telephone and email support. In addition to the standard support package, you will gain membership to 'LAUNCHPAD', our online client portal for digital management of your Information Security Manual and Certificates.

Manual Compliance

If you have drafted your own manual, or used a consultant to draft it on your behalf, we offer a FREE desktop review. Subject to passing the review, a compliance audit will be arranged to ensure that the manual has been implemented correctly. If all goes to plan, we'll then present you with your certification.

QMS
INTERNATIONAL
A CITATION COMPANY

Contact us today

☎ 01603 630345

enquiries@qmsuk.com

qmsuk.com

QMS International, Muspole Court, Muspole Street, Norwich, NR3 1DJ

Understanding **ISO 27001**

Implementing an Information Security Management System

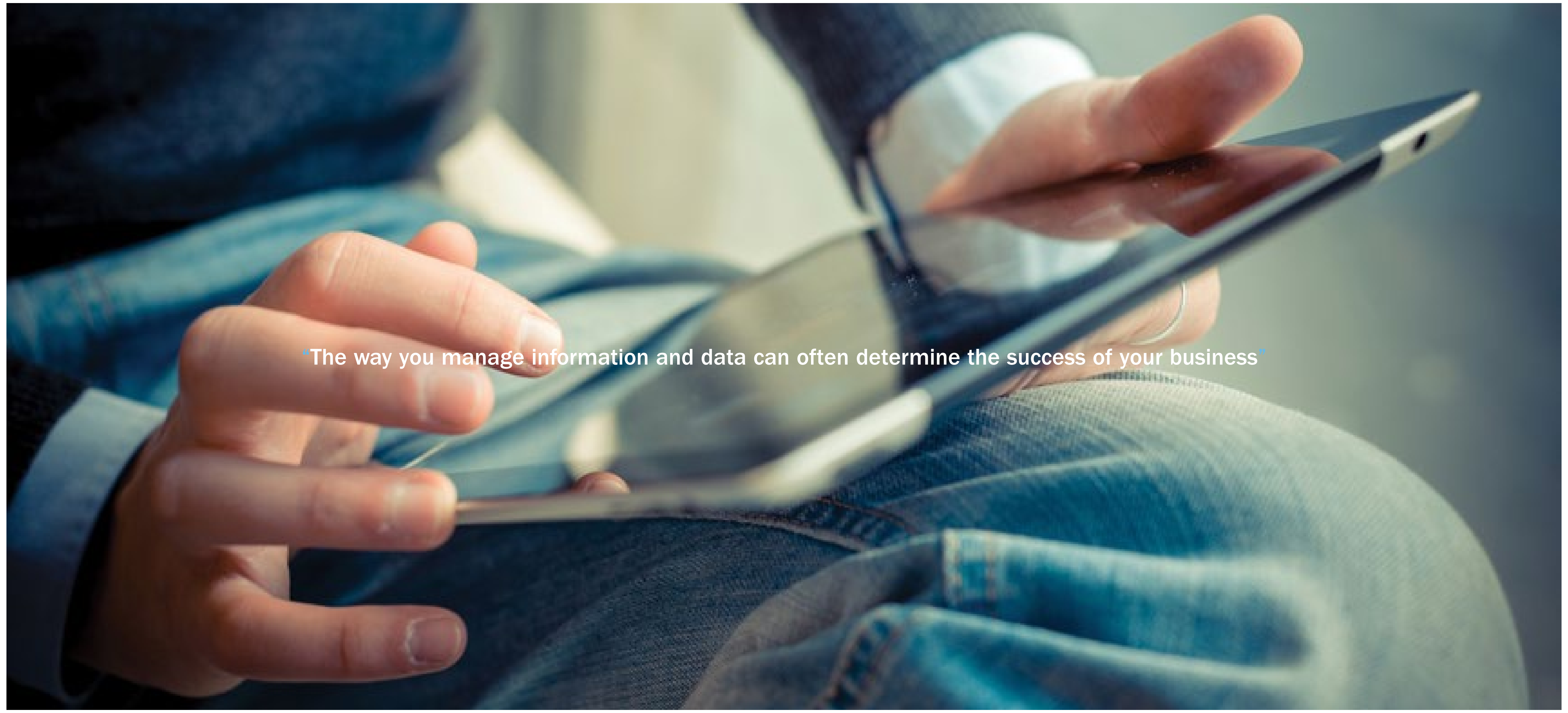
QMS
INTERNATIONAL
A CITATION COMPANY

What is ISO 27001?

Regardless of size or type, all organisations collect, process, store and transmit information, in many forms - and this information is valuable to your business and operations. An Information Security Management System sets out the things you need to do, within your organisation, in order to keep both your own and your customers' information assets secure.

By meeting the requirements of ISO 27001, and through certification, you'll able to demonstrate to your customers and stakeholders that you are managing and controlling information security risks as well as protecting and preserving the confidentiality, integrity, and availability of information - reassuring them that their information is secure.

With an ISO 27001 Management System in place you'll be able to reduce the chances of incurring fines, by eliminating incidents and improving compliance with relevant laws and regulations.



"The way you manage information and data can often determine the success of your business"

What does ISO 27001 include?

The Standard is backed by a great deal of theory and was drawn up by a number of experts from around the world, within this field. It defines a set of information security management requirements which include:

1

Context of the Organisation

For you to be successful you need to be able to demonstrate that your Information Security Management System is inline with your organisation's strategy, purpose and objectives. In plain English this means making sure the people responsible for it understand the Information Security Management objectives you've set; how they relate to the strategic goals you have, internal and external issues that might affect your success, the needs and expectations of interested parties and the ways that they plan to review your Information Security Management System.

2

Leadership

The next step is ensuring that someone takes a leadership role in this and is prepared to be accountable for making it a success. That means taking personal responsibility for setting objectives; considering the risks that could prevent success; implementing an Information Security Policy (i.e. your statement of what you're going to do and how you're going to do this) and generally ensuring that the standards agreed are met; as well as relevant, every single working day of the year. This could mean establishing an Information Security Management System Forum – where you allocate specific responsibility to people throughout your business.

3

Planning

Whilst we don't want things to go wrong, it's important that you have considered the potential for things to change. This might include plans to prevent or reduce undesired effects, setting out a clear plan for assessing, addressing and managing these risks (such as processes, policies, procedures, programs, tools, and much more), as well as reviewing the ways you identify them. This includes the means you have in place for the communication of this activity to key contacts and the ways you manage documentation relating to this process.

4

Support

This is all about practicing what you preach. That means providing the necessary resources to implement, run and control your Information Security Management System. This may mean the training of key staff or setting out a statement of your Security Policy and Objectives, and Information Security Management System Manual. It can also include Risk Assessment Methodology and Risk Assessment Reports including threats and impacts analysis, Risk Treatment Plans and a summary report of controls implemented.

5

Operation

You will need to set out the ways in which you are going to manage risks and implement the promises made in your Information Security Management System. This means performing information security Risk Assessments regularly and addressing any risks they highlight. Importantly this also applies to suppliers of outsourced (products and) services, many of whom may not be ISO 27001 compliant.

6

Performance Evaluation

This means continually monitoring, measuring, analysing and evaluating your Information Security Management System through Management Review Meetings and other means of achieving this.

7

Improvement

Most importantly, it's not just about measuring performance but about identifying areas for change and improvement and being able to prove that you're going to act on all of this information.

How can I get an ISO 27001 Management System to work in my business?

We understand that you've entered into this process because you're aiming for certification. To achieve this you need to be able to prove that you have the correct structure in place to meet the Standard's requirements.

By working with a QMS Consultant, you will be able to achieve certification in less than 45 days. That's regardless of whether you have done this before or not.

We have developed a simple, three stage certification process:

Stage 1: Manual

We start by visiting your organisation to conduct what's called a 'Gap Analysis'. This will highlight any changes that need to be made so that your policies and procedures meet the requirements of the standard. We will issue a detailed report for you and, with the information we gain on this visit, your ISO 27001 compliant manual can be created. One of our expert consultants can do this for you, or you can do it yourself using a QMS template.

Stage 2: Implementation

Now it is time to make sure those changes highlighted in the Gap Analysis are all in place (if applicable). We can help you do this by providing templates and tutorial videos. We also offer unlimited telephone support, from 9.00am-5.00pm, Monday to Friday.

Stage 3: Certification

In order for you to gain certification an accredited auditor must now visit your Organisation. They'll check that the documented processes in the manual are being followed, and that the necessary changes have been made. Providing all is in place you will be presented with your certification.

With QMS this process can take less than 45 days

To ensure that your certification remains valid, your manual and processes must be checked on an annual basis. Therefore audits will be carried out around the anniversary of your certification date and during the agreed certification period, by an accredited auditor.