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 maintaining your manual so it is in 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, whether you need help on-site or off-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.

You’re not alone: QMS is by your side

Understanding ISO 27001
Implementing an Information Security Management System

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

01603 630345 enquiries@qmsuk.com qmsuk.com
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 both your own and your customers’ information assets secure.

By meeting the requirements of ISO 27001, and through certification, you’ll be 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.

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 the 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 do is to demonstrate that your Information Security Management System is in line with your organisation's strategy, purpose and objectives. In plain English this means making sure that the people responsible for it understand the Information Security Management objectives you 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 play a role in your Information Security Management System.

2. Leadership

The next step is ensuring that someone takes a leadership role in this field is prepared to be accountable for making it a success. That means being personally responsible for setting objectives, controlling 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 it); and generally ensuring that the stakeholders agree are met, as well as ensuring they’re regularly reviewed on a day-to-day basis. The role must involve key people and must be supported by a Board of Directors - where you allocate specific responsibility to people throughout your business.

3. Planning

While we don’t want things to go wrong, it’s important that you have considered the potential for things to change. This might involve plans to prevent or reduce unwanted effects, setting out a clear plan for assessing, achieving and managing these issues (such as processes, procedures, programs, tools, and rules) and ensuring you’ve reviewed the ways you manage documentation relating to this process.

4. Support

This is all about practicing what you preach. That means providing the necessary training to key people, working with your ISO 27001 consultant, creating your Information Security Management System. This may mean the training of key people, setting out a statement of your Security Policy and Objectives, including threats and impacts analysis, Risk Treatment Plans and a documented Information Security Management System. It can also include Risk Assessment Methods and Risk Assessment Reports, including threats and impacts analysis, Risk Treatment Plans and a summary report of current procedures.

5. Operation

You will need to set out the ways in which you are going to manage risks and uncertainties for people, assets, and In your Information Security Management System. This means performing information security that measures are in place, and that those managing this activity to keep contacts and the ways you manage documentation relating to this process.

6. Performance Evaluation

This means continually monitoring, measuring, designing and evaluating your Information Security Management System through Management Reviews and other means of auditing this.

7. Improvement

Next important, it’s not just about measuring performance but about identifying where, how, and on what basis to prove that you’re going to get out 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 the ISO 27001 Management System and ensure that your certification remains valid, your manual and processes must be checked on an annual basis.

With QMS this process can take less than 45 days