BEGINNER'S GUIDE TO ISO 27001 : 2013

Information Security Management System Requirements Explained

QMS INTERNATIONAL

What is ISO 27001 : 2013?

ISO 27001 : 2013 is an internationally recognised Certification that sets out and standardises methods and processes for securing, recording, storing, transmitting and handling data. It is a model that sets out industry best practice and allows you to manage your processes, people and resources effectively to minimise the risk of losing or mishandling data, accidentally or otherwise.

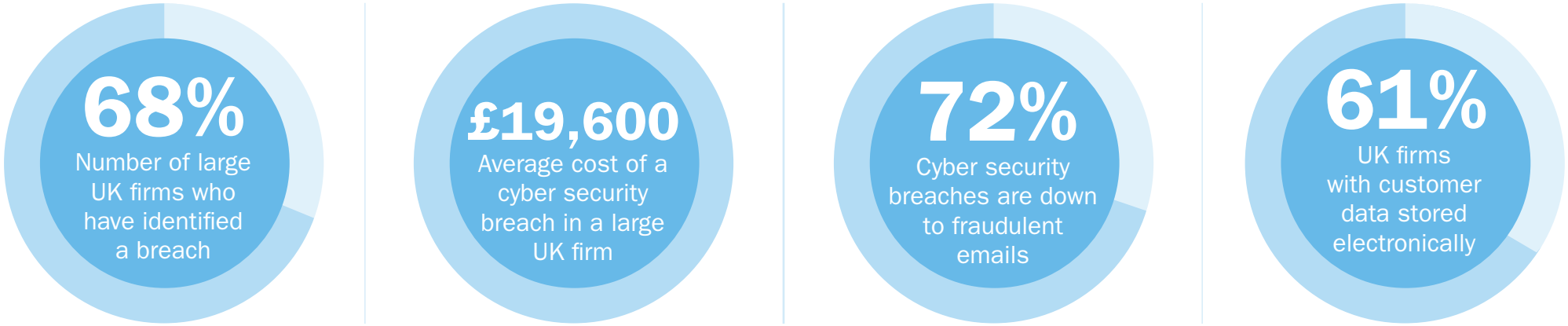
In addition, the ISO 27001 Standard focuses a certified business on continually reviewing and improving upon their processes, assuring its customers, staff and external stakeholders that it takes the security and use of their data seriously.

Why use it?

From bank details to addresses, purchasing behaviour to browsing habits, from client names to deal details - all this information is recorded. And with the increase in what types of information a company gathers and holds, comes an increased need to secure that data.

What is valuable to you is also valuable to hackers and competitors, so it goes without saying that the security and integrity of the information you hold is of vital importance. Reduce the risk to your organisation's reputation, its staff, partners and customers by ensuring you have taken all steps possible to protect your data from misuse, loss, corruption or theft through an ISO 27001 Certification.

Statistics published by Ipsos MORI and the Institute for Criminal Justice Studies at the University of Portsmouth in April 2017:



Source: gov.uk

How does it work?

ISO 27001 : 2013 is built around 7 areas...

1 Context

What?

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

Why?

By setting out and communicating your organisation's approach to information security, you are increasing positive brand recognition. In an age where customers are increasingly aware of the dangers of data loss and consequences of data misuse, you are showing that your company is doing everything it can to prevent this.

How?

Start by creating your organisation's information security policy. It should cover legal regulations, contractual requirements, and current/potential information security threats.

It is important that your policy aligns with your business strategy so that it can easily be incorporated into day-to-day operation.

Try to identify how you will handle any deviations from the policy or if there are exceptions. Such things do occur, so preparing for them now is good practice.

Document your policy and review it periodically to ensure that it remains appropriate to your business.

2 Leadership

What?

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

Why?

When the leadership of an organisation sets an example by actively participating in and encouraging those under them to care about the information security management system, they are creating an environment where everyone is working towards achieving the organisation's information security objectives.

How?

Start by communicating your organisation's information security policy. If everyone knows what your organisation is about and how it aims to go about it, then they can act with one purpose – especially if your leadership is setting a positive example in this regard.

Promote the importance of effective information security management and explain how your management system allows your staff to do this. You should also encourage a focus on continual improvement.

It is up to your leadership to take full responsibility for the information security management system but to also delegate and assign responsibility to individuals who will be in charge of specific areas.

3 Planning

What?

You need to establish, implement and maintain the processes needed to meet your goals.

Why?

By planning your processes in advance your business will be able to react quickly to any information security risks and opportunities that may arise. It also shows that you are a forward-thinking and proactive business, not a reactive one.

How?

For each relevant function in your business, establish a series of information security objectives and plan how you will achieve them. For each goal, determine: what will be done; what resources will be required; who is responsible; how long it will take and how the results should be evaluated.

It is an important part of the management system that your goals can be evaluated so that continual improvement can be achieved.

Determine any risks and opportunities related to information security and plan how you will address these. Also consider potential changes to your business that may affect these plans such as new products/services and abnormal conditions/ emergency situations.

4 Support

What?

Determine and provide the resources needed to fulfil your goals.

Why?

Without support, it is unlikely that your information security goals will be achieved. A fully supported management system shows that your organisation is committed to information security, not just paying lip-service.

How?

First, focus on your staff. Provide training and education to ensure all staff are aware of the information security policy and the consequences for themselves and the company should it not be followed.

It is important to empower your people by giving them the resources, training and authority to act with accountability in information security matters. In addition, inspire, encourage and recognise their contributions to encourage their participation.

Document all processes, cases of non-conformity with the Standard, audits and reviews. Make sure to keep these documents up-to-date with any changes that may occur.

You should ensure that your organisation's documented information is controlled appropriately, ensuring that they are protected against loss, improper use or theft.

5 Operation

What?

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

Why?

Information security should be thought of as part of business operations – not an afterthought. By thinking of it in this way you are more likely to prevent issues before they occur – saving you time and money.

How?

Check that you have covered four principal areas of security: people, location, systems and network. Do this by providing training for staff, securing your premises and network to prevent unapproved access, keeping systems secure with software updates and installing antivirus protection. Make sure these steps are applied at every stage of the business life cycle, including any outsourced work.

As well as the processes built in to day-to-day operations, you should also schedule regular risk assessments, audits and reviews to ensure everything is working as expected – and adjust the management system or provide training if not.

Be prepared for unusual situations and circumstances that aren't covered by the documented management system, training your staff so that they feel confident to report and, if necessary, respond to such incidents.

6 Performance evaluation

What?

You should monitor, measure, analyse and evaluate performance.

Why?

By evaluating your performance, you are ensuring that your goals and legal obligations continue to be met. This step also allows you to identify and rectify issues early on, before they become a problem.

How?

Firstly, determine what needs to be measured. You should set out a series of guidelines to allow consistent measurement – especially where measurements can be subjective.

Data shouldn't just be collected but be analysed, not only to see if a goal has been reached, but if improvements can be made.

You should perform regular audits and management reviews to ensure that your targets and measurements are still fit for purpose.

Everything within this section needs to be documented.

7 Improvement

What?

Successful organisations focus on continual improvement.

Why?

To ensure that a business does not stagnate, constantly look for opportunities to improve. From small, incremental alterations to large breakthrough changes, all improvements can increase the success of your information security management system.

How?

Regularly tracking and reviewing processes and making improvements will ensure they are always fit for purpose.

As part of your improvement efforts, all staff should be trained to spot non-conformities – where documented processes do not match the reality. When looking at any type of non-conformity, consider the root cause as well as addressing the consequences. This will allow you to introduce preventive actions and even allow you to spot and prevent similar issues in future.

Who can help?

Implementing an ISO 27001 Information Security 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 ISO 27001 Standard can bring to your business, and are looking for a common sense and 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, for businesses in a wide range of industries, QMS's market-leading services include everything from drafting a compliant Manual, to offering on-site Training and Certification.

Figures shown are taken from the QMS customer survey 2016.

Hassle Free Certification Process

From the first visit with a QMS consultant, right through to certification, you could potentially gain your ISO 27001 certification in as little as 45 days.

99%

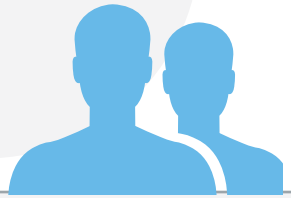
of clients were pleased with the speed of our certification process.

Experienced Consultants

With over 25 years' in the industry, you can be confident that our consultants have the knowledge and experience required to help any organisation, in any sector, achieve Certification with minimal hassle and cost.

97%

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

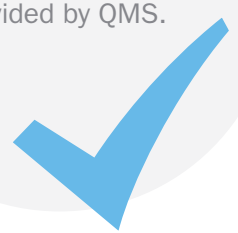


Accredited Certification Body

QMS are audited annually against ISO 17021 by the Accreditation Services for Certifying Bodies (ASCB). ISO 17021 is the international Conformity Assessment Standard which outlines requirements for bodies providing audit and certification of management systems.

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 straight-forward and efficient as possible.

Contact Us

If you would like QMS to support you on your route to ISO Certification, then get in touch today:

0333 344 3646 enquiries@qmsuk.com qmsuk.com