ISO 27001 : 2013

What can you expect from the certification process?

Information Security Management System Checklist

This checklist will provide you with a detailed understanding of what you can expect to have in place, and be doing, by the time you complete the ISO 27001 certification process. If you don't have any of this in place already, don't panic; QMS are happy to provide you with the necessary templates and guidance, during the QMS 3-stage certification process, until you do.

Planning

This means: understanding the areas that the ISMS will cover, as well as what it needs to achieve and the associated risks

- ○ The scope of our Information Security Management System is clearly set out and written down.
- ○ The options we have for how we manage and address risk have been identified and we've thought about how effective these might be within our organisation.
- ○ We've put in place a formal, written Information Security Policy (ISP) that is not only relevant to us but regularly updated and communicated to employees and interested parties.
- ○ The ISP includes clear objectives that we are committed to working towards and considers all the legal and regulatory obligations that we have.
- ○ We've set out a document considering all the information security risks to our business and covering all the ways in which we'll assess risk, as well as the levels of risk we consider acceptable in our organisation.
- ○ We have also thought about and set out the assets we have, as well as their ownership. We have considered areas of vulnerability, and threats, and the impact that could come from any loss of confidentiality and access to these assets.
- ○ We have thought about the impact, on our business and to our customers, that a loss of confidentiality, integrity and availability of this information could have. We have also thought about the security controls we have in place and need.
- ○ We are satisfied that the anticipated levels of risk are within boundaries we consider acceptable. If they are not we have set out plans to remedy this.
- ○ We have set out the security controls needed and, where necessary, implemented them, to ensure we meet the requirements identified in the risk assessment and risk treatment process.
- ○ The people responsible for our business have accepted the recommendations set out in the ISMS, as well as the associated levels of risk.
- ○ We have a Statement of Applicability that shows which controls (from ISO/IEC 27001 Annex A) have been selected, the reasons we have selected them (or not) and the status of their implementation.

Implementation and Operation

This means: understanding what you need to do and the foundations you need to put in place to be successful.

- ○ We've identified the things we need to do, resources required and the necessary funding, responsibilities and priorities for managing information security risks.
- ○ We've agreed how we will measure success and scope for improvement with this plan.
- ○ We have arranged the necessary training.
- ○ A senior person, within our organisation, has been appointed to manage this process.
- ○ We have set out controls that allow us to identify and respond to any security events and risks, promptly and efficiently.

Monitoring, measuring and evaluating

This means: making sure we know what's working, what isn't and what we need to do to change.

- ○ We have a framework for the ways in which we monitor activities to highlight errors, breaches, performance, prevention of security events and to assess whether the action taken was appropriate.
- ○ A formal reporting framework has been set out to assess effectiveness, using the results of audits, incidents, measurements and feedback from interested parties.
- ○ We've set out a programme for reviewing all risk assessments and acceptable levels of risk. We review these at planned points throughout the year and we take into account all the external and internal factors (such as personnel changes, changes to business activities, and legal or regulatory changes) when doing so.

- We run regular, formally planned internal audits of our ISMS. The results are reported and we put any changes necessary, as a result of these findings, into action in a timely way.
- We understand what we need to monitor and measure. The people responsible for our business conduct regular management reviews, at planned intervals, to make sure the ISMS continues to meet our objectives, needs and expectations.

Maintaining and improving

This means: **committing to a programme of constant improvement so that your ISMS always meets your objectives.**

- We've reviewed how well our ISMS is meeting our organisational objectives as well as the needs and expectations of all interested parties.
- We do this on a regular, planned basis.

Documents and records

This means: **how you handle any documents, records or information concerning your ISMS.**

- All the documents and records that relate to our ISMS are kept and managed in line with agreed procedures and risk standards.

Leadership

This means: **the role your key management will play in leading, not just managing, your Information Security Management System and any actions required during the certification process.**

- The people responsible for our organisation have understood the certification process and have taken responsibility for the effectiveness of our ISMS.
- We have clearly set out who is responsible for making each part of the ISMS a success, as well as what is expected of them, what they'll do and by when. We have made sure that they have the competence required and provide training if necessary.
- We are committed to ensuring that the resources required to be successful for each stage of our ISMS have been set out and made available.

Security control examples

This section includes some of the security controls you might have selected during your risk assessment and risk treatment processes.

- We have confidentiality and/or non-disclosure agreements within all employment contracts and contracts with suppliers.
- We have contact with external authorities, special interest groups and/or run a regular independent review of our information security arrangements.
- We have set out a study of the information security risks that come from external parties. We have addressed these in any relevant contracts or agreements.
- We have compiled an inventory of our organisational assets, and set out who owns them and the rules for their acceptable use.
- We have set out a framework for information classification, as well as guidelines and procedures for putting it into practice, labelling and handling information.
- We perform legal and proportionate background verification checks on all candidates for employment.
- There is a formal disciplinary process for employees that have committed a security breach.
- There is also a formal process for when employment terms change or employment is terminated, that sets out how assets are to be returned and access rights removed/adjusted.
- We have set out secure 'physical' security areas, with entry controls on relevant facilities, offices and sensitive areas. These include delivery and loading access.
- We have identified areas of external and environmental threats and put in place a framework for protecting against them, as well as reducing any associated risk.
- All equipment is protected against the failure of supporting utilities and cables are protected from damage or interception.
- We make sure equipment is maintained and tested to ensure availability and integrity within the context of information security risk.
- This same level of security is applied to any equipment being removed from our premises or used off-site. We've also put in place a procedure for disposing of this equipment securely.
- We have set out clear operating procedures and all changes are controlled and recorded.
- We have analysed tasks that have security implications and thought about ways to segregate duties so as to protect against risk.
- Any development, test and operational facilities have been separated so as to reduce the risk of unauthorised access to operational systems.
- We are clear about the requirements we have for third parties, concerning security. We have set these out in formal agreements, which are monitored and reviewed within the context of change and risk management.
- The people responsible for our organisation are tasked with anticipating future requirements and maintaining system performance.
- When we change our systems we set out criteria for success and test these changes both during development and before we accept them.
- We have set out controls that allow us to accurately detect, prevent and recover from malicious code. We have also launched communications to raise awareness of this risk.
- We make regular backups of information and software, and we test these. This is all underpinned by a formally set out Backup Policy.
- Our networks are managed and controlled so as to protect our organisation (and customers) from the threat of security breaches. We have a clear agreement that sets out the standards we expect and how these will be maintained.
- Any media that needs to be removed or moved is managed according to clear procedures we have set out, to include handling, transport and storage.

- We have set out formal procedures for exchanging information and software with third parties.
- We have procedures in place that protect information when it is included in interconnected business systems, for example email.
- We have clear controls in place to protect interested parties during any online transactions, ecommerce and in using publically available information.
- An audit log of user activities, system events and system administration activities is kept, retained and protected against tampering.
- All faults are logged and systems monitored, as well as being reviewed regularly. We take any necessary action, as a result of this process, quickly and efficiently.
- We have set out an Access Control Policy, based around our business and security requirements.
- There is a formal user registration procedure. We manage privileges and passwords centrally and review, regularly, access rights.
- All users are required to follow good security practice where passwords, leaving equipment unattended and using facilities are concerned.
- We have set out a policy on the use of network services, which includes strict guidelines for good practice concerning use and connection of equipment.
- Access to operating systems is controlled by secure log-on procedures. All users are uniquely identified and use of system utilities is restricted.
- We have a formal policy setting out security measures and procedures for mobile computing and teleworking.
- The security requirements surrounding new and changed information systems have been set out formally.
- We have set out formal processes for the validation of data input and output, processing controls and integrity checks, where all applications are concerned.
- We have a clear policy for the use of cryptographic controls. If appropriate, cryptographic key management is in place.
- We have set out controls for the installation of software. These include the selection and control of system test data.
- Change control procedures have been considered and, where relevant, put in place for application software. This is source code protected.
- We conduct a technical review of business critical applications, following upgrades to operating systems.
- Any outsourced software development is supervised and monitored.
- All security events and weaknesses are reported and recorded so that an orderly response can take place. We use this learning to reduce future events and weaknesses.
- We have considered the security aspects of business continuity. We have set out a robust, tested plan for maintaining and restoring operations as well as making information available.
- We have identified all of the legal, statutory and contractual requirements that impact on our ISMS and are committed to making sure we stay current, where these are concerned.
- We test, regularly, how well we are doing against our security policies and standards, as well as our technical compliance. Access to these information system audit tools is restricted and controlled.

Implementation and Certification takes only **45 days**

QMS have assisted with the implementation of over 20,000 Management Systems. Our mission is to help organisations, of any size, in any industry sector to become certified in the most straight forward and cost-effective way possible. That is why our customers' benefit from a simple 3-stage certification process, free templates, unlimited telephone and email guidance and access to LAUNCHPAD, our on-line Management System portal.

If you would like to find out more about this Standard or how QMS can help your organisation to become certified, then get in touch today on 0333 344 3646.