BS 10012 : 2017

What can you expect from the certification process?

Personal Information Management System (PIMS) 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 BS 10012 certification process. If you don't have any of this in place already, don't panic; QMS will provide you with adequate time to address the areas of non-conformance, ahead of certification.

Context of the Organisation

This means: understanding external and internal issues, as well as the needs and expectations of interested parties, and where you sit in all of this.

- We have thought about and set out the external and internal issues that are relevant to our organisation's vision, purpose and strategic direction, and usage of Personal Information.
- We've set out a way of reviewing and checking these as well as the timescales for doing so.
- We have identified the parties that may be interested in our Personal Information Management System (PIMS) and understand their needs and expectations.
- Our PIMS addresses the external and internal issues, the needs and expectations of all parties, as well as our strategic vision, objectives, products and services.
- We've carefully set out the processes, actions and requirements at each stage within our PIMS.
- We've also set out how each of these stages will be managed, who is responsible, how they need to action things and how success will be measured.
- We understand how to adjust our PIMS as the context of our organisation changes.

Leadership

This means: the role your top management will play in leading, not just managing, your PIMS and actions required during the certification process.

- Our top management have understood the certification process and have taken responsibility for the effectiveness of our PIMS.
- Our PIMS is structured to reflect the strategic vision and the priorities of our organisation.
- We are able to integrate the policies and procedures set out in the PIMS into our day-to-day operations.
- We have defined and communicated a PIMS Policy that describes how we aim to comply with data protection requirements and best-practice.
- We have a framework for communicating our objectives clearly at all levels of the organisation – strategic, functional, departmental and individual.
- Our managers understand the importance of communicating the processes set out in the PIMS and the role that risk-based thinking will play in our success.
- We've considered both the risks and opportunities that exist within our own processes, taking the appropriate steps to act on these findings.
- We have clearly set out who is responsible for making each part of the PIMS a success, as well as who is responsible for making decisions.

Planning

This means: evaluating success, measuring risks and opportunities, and planning the steps needed to increase desirable effects, prevent unwanted effects and achieve improvements.

- We have a framework for identifying the risks and opportunities that affect our processes and the PIMS.
- We regularly perform a data inventory for all areas of our business that records what data we hold, what it is used for and why we collect it.
- We have defined and documented a data flow process that covers all sources and categories of personal information.
- We have identified, defined and documented the legal basis for which we hold or process personal information in our business.
- We have a defined procedure for, and regularly perform, Privacy Impact Assessments (PIA).
- We ensure that all personal information is protected by default and by design in all of our projects and processes.

- We have planned what we need to do to meet our PIMS objectives.
- We have integrated the steps that need to be taken into our day-to-day practices and systems and not just treated them as 'one-off' tasks.
- We've thought about the ways in which we might need to change the PIMS, over time, to ensure it stays effective.

Support

This means: making sure you have the resources and tools you need to run and continually improve your PIMS.

- We understand what resources (people, infrastructure, working environment etc.) we need in order to establish, implement and maintain our PIMS.
- We have set out a plan for reviewing resources on a regular basis, to make sure we continue to provide adequately trained staff, along with the right equipment and materials, to meet our customers' expectations.
- We recognise that accurately measuring and monitoring the ways in which our products and services meet our personal information obligations is important. So we have identified the resources required to provide valid, reliable results.
- We have made sure that we have a good infrastructure in place to ensure conformance to the Management System Standard and legal compliance, both now and in the future.
- We recognise the levels of understanding we must have, to ensure that our processes can work effectively, and our products/services conform to the expected criteria set out in our PIMS.
- We have taken steps to ensure that the people impacting on our PIMS are appropriately trained or that their training needs have been identified to help them achieve the required skill set.
- We've made sure that each person in our organisation understands how they can contribute towards the PIMS' success.
- We've planned internal and external communications to make sure everyone knows about the PIMS.
- We understand what documented information needs to be provided – both to satisfy the requirements of the Standard and to ensure the requirements continue to be met effectively.

Operation

This means: the steps you need to take to get going on your PIMS.

- We adhere to the idea that data processing should be fair, lawful and transparent.
- We have i*dentified whether we need to/assigned* a Data Protection Officer (DPO) who is responsible for ensuring our PIMS meets our legal obligations and any applicable laws.
- We have clearly set out processes to ensure we meet the requirements specified by the Standard.
- We get the permission of those on whom we hold personal data to use this information, and adhere to their rights under applicable data protection laws. For children, we gain consent of their legal guardians.
- Any changes that need to take place will be considered carefully, within the structure of our PIMS, and carried out in a way that will ensure continuing relevance and success.
- We work with external providers to ensure that our Personal Information goals are met through their systems and operations, using a clearly defined process. Especially if we share data with those providers.
- We have documented procedures in place that enable us to detect and react to emergency situations that contravene the safety or privacy of personal information. We have communicated these procedures to our staff.

Performance Evaluation

This means: using your experience and knowledge to monitor, measure and analyse processes and changes, to consistently seek out ways to improve.

- We understand what we need to monitor and measure and have set out the ways in which we will do this, to get useful, valid results.
- We have agreed when we need to analyse and evaluate these results.
- We have agreed a formal structure for evaluating our PIMS, through an internal audit programme.
- We will agree any areas for potential improvement and development, within the PIMS, and how we will include these in management reviews.
- We have set out a structure for management reviews and are committed to implementing it, to regularly monitor & evaluate the implementation of our PIMS.

Improvement

This means: using the results from your evaluation and analysis to identify ways to enhance the PIMS that serve to increase levels of data protection across the organisation.

- We have identified areas for improvement that focus on meeting our PIMS objectives. We have also taken the steps necessary to put these changes into action.
- We have a process for managing the ways in which we do not conform to the Standard, and how we will correct this.
- We know how we will prioritise the continual improvement of the suitability, adequacy and effectiveness of our PIMS.
- We consult with and encourage the participation of staff within the development and continual improvement of our PIMS.

Implementation and Certification in 30 days

Through QMS' award-winning certification process, you could achieve an BS 10012 certification in as little as 45 days. The process is straight-forward and cost-effective and includes access to LAUNCHPAD, our on-line Management System Portal hosting a library of useful templates and tutorial videos.

0333 344 3646 | enquiries@qmsuk.com | qmsuk.com

QMS INTERNATIONAL