ISO/IEC 20000-1 : 2011

What can you expect from the certification process?

IT Service 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 20000-1 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.

Your IT Service Management System

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. It also covers your obligations as well as how you support this process and monitor areas for improvement.**

- The people responsible for the organisation have understood the certification process and have taken responsibility for the effectiveness of our IT Service Management System.
- Our IT Service Management System is structured to reflect the strategic vision and priorities of our organisation. This has been communicated throughout the organisation so that everyone understands how it is relevant to overall success.
- The people responsible for the organisation have agreed the key areas for activity and are committed to providing the necessary, competent resources to make this process a success.
- The people responsible for the organisation are committed to making sure that all risks are identified and are being managed effectively.
- We have set out a clear protocol for the ways we handle documentation and records, relating to this IT Service Management System.
- We understand what resources (people, infrastructure, working environment etc.) we need in order to establish, implement and maintain our IT Service Management System.
- We understand the service requirements, as well as having a clear framework for delivering the service, the management of risks, as well as how we will monitor and measure the things we're doing, to ensure best practice and compliance with the Standard.
- We have agreed when we need to analyse and evaluate these results. We have agreed a formal structure for evaluating our IT Service Management System, through an internal audit programme and reviews of the people responsible for its implementation.
- We will agree any areas for potential improvement and development, within the IT Service Management System, 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 and evaluate the implementation of our IT Service Management System.

Design & Development of New or Changed Services

This means: **the ways in which the IT Service Management System adapts to support and respond to the design and development of new or changed services.**

- We've made sure that there is a suitable process in place to support each stage of the process – be that the planning, design, development or testing – and to make sure that these changes and developments can be integrated into our existing practices without disruption.
- We have a framework for ensuring that we have considered, properly, any changes planned and the effect this will have on our IT Service Management System.
- All the service requirements are identified, designed, reviewed and documented, at each stage of the planning and design phases.
- All new and changed services are tested to make sure they meet the objectives we have set out for IT Service Management, prior to release.
- After services have been changed we always step back to evaluate and report whether they have achieved what was needed and expected.

Service Delivery Processes

This means: **the ways in which you deliver your services, as well as the infrastructure that supports this, and how this is tested to comply with the Standard.**

- All services that we deliver have been clearly set out, agreed and documented in a catalogue of services. They are also supported by service level agreements, which are regularly reviewed and agreed with customers.

- The risks to continuity of service provision and availability have been assessed and documented.
- We have developed plans for recovery from any risks identified. These are regularly monitored and tested to make sure they deliver on the objectives set out at the beginning.
- We have allocated a budget to support the cost of service provision and we have put in place a framework to ensure this fits within the organisation-wide financial management system.
- We've considered the human, technical, information and financial resources that we need to be successful with this IT Service Management System. We have made sure that our needs and requirements are met across these four areas.
- We have set out an Information Security Policy and a clear approach for managing information security risks.
- We have also implemented any changes that can be made to reduce or remove these risks, using physical, administrative and technical controls.
- Any changes that need to take place will be considered carefully, within the structure of our IT Service Management System, and reviewed to identify potential security risks, as well as ensuring we have thought about their impact.

Relationship processes

This means: **making sure you have a framework in place to manage your customer relationships and better understand their needs and expectations.**

- We have identified individuals who are responsible for managing the customer relationship and ensuring customer satisfaction.
- We understand the importance of measuring and monitoring our performance. This is reviewed at planned intervals, with the customer.
- We have set out what we understand by the term 'service complaint' and the procedure we follow for managing complaints and their escalation.
- We have identified individuals who are responsible for managing the contractor and supplier relationship and ensuring agreed performance levels.
- Our Suppliers understand what is expected from them in terms of communication, requirements, scope and level of service. This is documented and supported by service level agreements, which we have all agreed.

Resolution processes

This means: **ensuring you have a framework to support the ways you resolve problems, errors and minimise the impact of incidents.**

- We have a framework that sets out the way we manage and resolve incidents and problems.
- There is an agreed definition of a 'major incident' and both customers and the people responsible within our organisation understand this.
- We have set out a procedure that covers the way we identify problems and minimise their impact.
- Data and trends on incidents and problems are recorded and (regularly) analysed so that we can better understand and anticipate causes.
- This information is kept up-to-date and is available so that problems and incidents can be prevented and better managed.

Control processes

This means: **the ways in which you plan, manage and monitor control processes to ensure that they comply with the Standard.**

- We have set out a definition for each type of configuration item, as well as a description and status. This also includes the relationship that it has with other configuration items and service components.
- All configuration items are clearly identifiable. They're recorded in a configuration management database and we restrict update access so as to maintain accuracy and clarity.
- When we change any configuration items we make sure that this change is traceable, auditable and can be seen within the context of its starting point.
- We have set out a change policy to support this. This not only defines our understanding of controlled configuration items, but also sets out the ways we establish whether this change will have a major impact or not.
- We have a formal procedure for recording, classifying, assessing the impact of, approving and scheduling any changes.
- We also have a formal procedure for managing emergency changes and their release.
- Any changes we make are reviewed at planned intervals – we are testing them for effectiveness, analysing them for trends looking for opportunities to improve things yet further.
- We have agreed a release policy with the customer. This agrees the frequency of any releases.
- Releases are planned and communicated in advance. This allows us to identify the ways in which they might impact on our change, incident and problem management processes.
- All releases are built and tested within a controlled environment. We do this before deployment and using criteria that sets out what we're looking for and the ways we're planning to test it.
- If a release fails we have a framework in place to rectify this.
- We also have a process set out to ensure we can monitor successes/failures, as well as reporting them so as to identify opportunities for improvement in the future.