ISO 22301 : 2012

What can you expect from the certification process?

Business Continuity 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 22301 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.

Context Of The Organisation

This means: **understanding external and internal issues, as well the things that could go wrong and the level of risk you're prepared to tolerate.**

- We have thought about the 'things that might go wrong' that will drive the Business Continuity Management System (BCMS).
- We have also thought about and set out the external and internal issues that have an impact on how our BCMS works, as well as what we can reasonably expect the outcome of implementing it to be.
- We've set out a document covering all the ways in which we'll assess risk, as well as the levels of risk we consider acceptable in our organisation.

The Needs & Expectations Of Interested Parties

This means: **understanding the people that are likely to be impacted by the BCMS and what they need, and expect from you.**

- We've thought about all of the legal and regulatory obligations that we have, and we have put in place a procedure for identifying, considering, documenting and keeping up-to-date with them.
- Employees and all other interested parties have been communicated with, about these legal, regulatory and 'other' requirements.

Scope Of The BCMS

This means: **understanding the areas that the BCMS will cover, as well as what it needs to achieve.**

- The scope of our BCMS 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 understand what the BCMS needs to achieve and deliver, as well as how it relates directly to our organisation.
- We've also thought about the things we want to (consciously) leave out of the BCMS. We have agreed that these will not impact on our ability to provide a continuity of operations.

Leadership

This means: **the role your top management will play in leading, not just managing, your Business Continuity Management System and 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 Business Continuity Management System.
- We have clearly set out who is responsible for making each part of the BCMS a success, as well as what is expected of them, what they'll do and by when. We also understand the importance of demonstrating our commitment to the BCMS.
- We have set out a structure for management reviews and are committed to implementing it, to regularly monitor and evaluate the implementation of our Business Continuity Management System.

Business Continuity Management Policy

This means: **setting out, in writing, what your approach to Business Continuity Management is, as well as what is expected of everyone and every process at your organisation.**

- We've put in place a formal, written policy that is not only totally relevant to us, but regularly updated and communicated to employees and interested parties.
- This policy is readily available for all to read and comment on.

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

QMS INTERNATIONAL

Business Continuity Response & Recovery Plans

This means: planning out what you're going to do when things are disrupted.

- We've set out plans and procedures for all the steps that we'd need to take after an incident occurs.
- We've made sure these plans reflect all those that will need to use them.
- These plans set out all the roles involved and what each is responsible for.
- They also set out what will signal the need for the response to start.
- These plans take into account how we'll manage the immediate effects of any disruption. In particular, this means the welfare of individuals as well as the options we think we have for responding and preventing further loss.
- Our plans set out how we're going to communicate with all interested parties during the disruption.
- Our plans also set out how certain prioritised activities will be continued or recovered, as well as the time frames for doing this.
- We've set out a media response for any incidents.
- We've also set out a procedure for 'standing down' the response, when needed.
- We've looked back over all of these plans and have agreed that this plan contains all the information necessary to allow us to use it effectively, should we need to.

Exercising & Testing

This means: making sure that you've tried out the various procedures and processes, as well as testing them to ensure they work as you need them to.

- We've tested every step of our business continuity procedures to make sure they achieve the objectives we set at the start.
- These are tested, actively, at all levels of the organisation, including the senior management.
- We have a framework for the ways in which we test procedures. These have all been set out as clearly defined exercises, based on relevant scenarios. We've thought about the ways in which these help us to meet objectives.
- These test exercises have been designed to minimise the risk of disruption within our organisation.
- A formal reporting framework has been set out, for after each exercise, as well as the ways we'll review all the outcomes to make sure we continue to improve.
- We've set out a programme for when we will test exercises, at regular intervals, as well as making sure we're aware of any changes that might require us to change the processes set out in the BCMS.

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 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've reviewed how well our BCMS is meeting the needs and expectations of all interested parties. We've made a formal record of this process, as well as any things we need to do to correct less successful areas.
- We've set out a clear framework for monitoring the BCMS.
- We have regular reviews, as well as when significant changes occur. It makes sure our organisation stays compliant with the requirements of the Standard.
- Post-incident reviews are also done and recorded, following any disruptive incidents.

Internal Audit

This means: taking a methodical look at how well the BCMS is performing.

- We have agreed a formal structure for evaluating our Business Continuity Management System, through an internal audit programme. This makes sure it continues to conform to the Standard, as well as what we need within the organisation.
- When we do this audit we make sure that it's done methodically, drawing from our previous risk assessments as well as previous audits.
- We work hard to make sure that any corrective measures we need to take are taken and checked as soon as possible, after they have been identified.

Management Review

This means: making sure that the people responsible for the BCMS review this on a regular basis to highlight areas for change, improvement or poor performance.

- Those responsible for managing and running the business review the BCMS on a regular basis.
- We use this review process to identify the information that we need to put into the BCMS procedures to ensure the outcomes meet our organisational objectives.
- The management review process highlights the changes and improvements we need to make, to ensure we're always compliant with the Standard.
- The results of any management review we conduct are recorded, acted on and communicated to all interested parties.

Improvement

This means: using the results from your evaluation and analysis to identify ways to enhance the Business Continuity Management System and improve the way your organisation reacts to disruptive incidents.

- We have a process for managing the ways in which we do not conform to the Standard, and the steps we need to take to correct this.
- The review process contributes directly, and in a measurable way, to improving our Business Continuity Management System.