

ISO 22301:2019 – Changes, Clarifications but No New Requirements...

Hilary Estall MBCI and IRCA Lead BCMS Auditor explores the recently published 2019 version of ISO 22301 and considers whether ISO's self-proclaimed statement that there are "no new requirements" in the latest re-write actually holds true. Lifting the lid on what appears to be an uncontroversial update identifies areas which, whether aligned or certified to the Standard, will require time and thought to digest and apply.

Hilary is a member of the BSI (UK) Technical Committee responsible for input into ISO 22301 and other, business continuity and resilience related management system standards and guidance documents. She has over twenty years practical experience in her field and applies this in her own, pragmatic way, to uncover the changes and how best to address them.

Introduction

ISO 22301 was revised in late 2019 to reflect ongoing changes in the business continuity world and respond to the continuing development of Management System Standard (MSS) requirements. This article looks at the changes made and the impact to users, offering ideas on how to go about adjusting your BCMS, to reflect ISO 22301:2019 requirements.



Look out for Hilary's Top Tips to help you during your transition to ISO 22301:2019

Basis of Review

ISO Management System Standards (MSS) undergo periodical review to ensure they continue to reflect current thinking and feedback from the international user community. Amendments vary from minor alterations to major re-writes, depending on sector change and general desire for re-modelling and/or improvement. This happens every five years or so. ISO 22301:2012 came up for review in 2017 and the folk at ISO (International Organization for Standardization) began the process by seeking feedback from the respective Committee and its country members as to what level of appetite there was for change. Led by ISO itself, the feeling was that a general review and update to de-dupe the contents and address issues arising since its original publication, both technical and directly related to Management Systems, would be in order. And so the review process began in earnest.

Before I get into the detail it is worth reminding readers that MSS are made up of both technical (ie. Clause 8 business continuity management requirements in the case of ISO 22301) and management system requirements (clauses 4, 5, 6, 7, 9, 10) which together establish a set of requirements for maintaining and improving the framework around which the elements sit. These non-technical requirements of management system standards underwent a review by ISO in 2012 with a view to developing a generic management system framework, making life a lot simpler for organisations with more than one MSS. Annex SL (and associated appendices) was born and ISO 22301:2012 was the first MSS to apply this new approach. This is an important fact to consider when we get into the review of ISO 22301, itself.

The review of ISO 22301 was carried out between 2017 and 2019 with comments gathered from interested parties across the world along with Technical Committees identifying their own proposed amendments, all culminating in the not inconsiderable review and development of a workable solution on which member countries could agree.

ISO 22301:2019 What's changed?

Headline changes, some of which are listed in the Foreword of the Standard, are as follows;

- ISO 22301 now conforms to ISO's requirements for management system standards, which have evolved since 2012 (Annex SL). (Remember ISO 22301:2012 was the first ISO MSS to follow the new Annex SL guidelines. Since then numerous MSS have been revised or developed using this approach and the interpretation applied in ISO 22301:2012 has since evolved). This has been a significant focus for the 2019 update;
- **Requirements have been clarified, with no new requirements added** (but see amendments below);
- Discipline-specific business continuity requirements are now almost entirely within section 8;
- A number of discipline-specific business continuity terms have been modified to improve clarity and reflect current thinking; and
- Content in clause 8 has been reordered, duplication removed and terminology simplified and more consistent.

This all sounds reasonable and it is. Less repetition, requirements located within the most appropriate clause and management system requirements now closely aligned with other Standards, not least, ISO 9001 and ISO 27001. Excellent. However, ISO 22301:2019 does include changes which I believe require further consideration. To an experienced practitioner most of these changes will not even be picked up as "new" and indeed, appear to be simply good BCM practice, but for readers who are less experienced in either business continuity management or management systems, I feel greater explanation is required.

Before I proceed you should bear in mind the following point of note:

Where it is no longer necessary to "document" or conduct other actions you need to decide whether your existing BCMS documentation (to ISO 22301:2012 requirements) continues to be useful to you and your staff. If so, do not feel compelled to remove it just because the latest version of the standard no longer explicitly requires it. Assuming it remains valid an auditor will not penalise you for taking this approach.

Detailed Changes

It is important to read all of the document. That includes the Foreword, Introduction and Clauses 1 to 3 *before* you get into Clauses 4-10; the detailed requirements. It is here you will find the following points to consider:

ISO 22301 Introduction

A new section within the Introduction (0.2) entitled "Benefits of a business continuity management system" has been added. This could be a useful overview and a basis on which to "sell" BCM to senior management, as well as the rest of the organisation.

0.3 Plan Do Check Act (PDCA) Cycle

The PDCA cycle still exists but unfortunately no longer aligns each clause (4-10) to one of the 4 PDCA stages as it did in the 2012 version. However, this is nonetheless a useful section for introducing the approach to management systems to anyone new to them, including ISO 22301, and is a powerful way of showing how significant the “planning” stage is when designing and implementing a new management system. Dig out your 2012 version of ISO 22301 and decide which explanation you prefer.

Clause 3 - Terms and Definitions

There are some new (examples include “disruption” and “impact”) and revised terms and definitions, others have been removed and some amendments to the respective Notes, made. Readers should also refer to ISO 22300 where many other terms and definitions are found. (Note ISO 22300:2018 is itself currently under review)

Clause 4 - Understanding the Organisation and its Context

Much reduced in length, this is now only a high level requirement. There is no need to document what your “context” might look like just determine what the external and internal issues are. The 2019 reduced wording may not be as explicit to newcomers to the Standard but reflects other MSS now applying similar wording.

Clause 5.2 - Business Continuity Policy

The requirement to review the Policy for continuing suitability has been removed from the Policy clause (5.2.2) but remains within the Management Review Inputs (clause 9.3.2.e) thus removing duplication. Take care not to overlook this requirement.

Clause 6 – Planning

Clause 6 has been re-structured to reflect other current MSS. ISO 22301 now includes **6.3 Planning changes to the BCMS**. Users of other MSS should have arrangements in place to address this requirement but existing ISO 22301 (only) users are now clearly directed to give thought to and decide how they will articulate their plans to make changes to the BCMS.



Top Tip

As an auditor, I have picked up on how this might look when “re-allocating” (clause 6.3 d) BCMS responsibilities and authorities. In other words, how an organisation might plan for (and evidence) and develop new, competent and suitably authorised, staff. Whilst this makes complete sense and most organisations will take this process in its stride, it is, nevertheless, something else to be considered. It is also, in my experience, an area which does not always receive adequate and appropriate focus.

Clause 7.4 - Communication (relating to the BCMS itself)

Clause 7.4 now reflects other MSS in so much that it only refers to the need to communicate elements of the BCMS. Previously, the wording overlapped between management system communication expectations as well as those specifically for managing business continuity communications, such as ensuring the availability of the means of communication during a disruptive incident. Business continuity specific communication requirements are now all to be found under clause 8.4.3.1).

Clause 8 – Operation

One of the criticisms of users of ISO 22301:2012 was the lack of a detailed requirement around the need for an organisation to manage its supply chain's own business continuity capabilities. Loose reference to this was made at the end of clause 8.3.1 stating the organisation should conduct evaluations of the BC capabilities of its suppliers. This requirement led, in my experience, to a wide interpretation of what this might look like in practice but with no clear "requirement" to attach itself to. ISO 22301:2019 is no more specific (see clause 8.6 c) but the good news is that we now have a dedicated document **PD ISO/TS 22318 Societal Security — Business continuity management systems — Guidelines for supply chain continuity** which provides additional, detailed guidance in this area.

Clause 8.2.2 - Business Impact Analysis

Attention now focuses on the requirement to define "impact types and criteria" relevant to the organisation's context and to use these for assessing impact over time. Using the upcoming version of ISO 22313 (due to be re-published early 2020) examples of "impact types" are offered and include; Financial, Reputational, Operational and Legal and Regulatory. (This should not be viewed as a complete list of impact types). These are not new concepts and many organisations already include such consideration in their BIA and/or Risk Management methodologies so this should be seen as clarification rather than a new requirement. That said, some ISO 22301 users may now need to ensure their BIA methodology reflects this. Have a look at **PD/ISO/TS 22317 Societal security - Business continuity management systems - Guidelines for business impact analysis (BIA)** for more information on this subject.

The BIA analysis is used to identify prioritised activities. The need to determine resources and dependencies (clause 8.2.2 g and h) only extends to "prioritised activities".

References to "risk appetite" have been removed from the Risk Assessment clause 8.2.3 (but still alludes to it in Context clause 4.1 Note and Strategies clause 8.3.3). The decision for this was because ISO 31000 Risk Management – Guidelines; no longer refers to risk appetite.

Clause 8.3 - Business continuity strategy

Now expressed as "Business continuity strategy and solutions". Each strategy may be formed of one or more "solution". This is nothing new and readers should not be thrown by the new terminology. An example might be to implement a strategy around premises with a solution being to identify alternative company locations to use or contract with a third party recovery centre. Also, Resource Requirements; Transportation (clause 8.3.4 f) has been extended to include "logistics".

There is now a requirement to "implement and maintain selected business continuity solutions (clause 8.3.5) so they can be activated when needed". Again, this may now be more explicit but one would hope organisations are already reviewing strategies and their ongoing applicability, as the business matures or changes and amending them as required.

Clause 8.4 - Business continuity plans, including response structure

This is an interesting section both from the point of view of the system implementer as well as from the auditor as there are some specific nuances which will need to be addressed, possibly for the first time. The wording of the standard now stipulates business continuity plans and procedures shall;

- Be structured such that one or more teams are responsible for responding to disruptions.

- The relationships between the teams must be stated as well as their roles and responsibilities.
- Each team must identify personnel including “alternates” and state responsibility, authority and competence to perform designated role (This goes further than before in terms of Alternates).
- Details on how to manage the immediate consequences of a disruption including the impact on the environment
- Each plan must include a process for standing down (was on the collective list in Clause 8.4.4 g)
- Each plan shall be useable and available at the time and place at which it is required.



Top Tip

Consider the underlined words (above). Do you need to review and amend your BCMS arrangements so these requirements are adequately (and clearly) addressed? The word “relationship” is interesting and requires thought. How can you demonstrate this to an auditor?

Clause 8.5 - Exercise programme

Again, some new words have been inserted and require consideration. An organisation must now develop teamwork, competence, confidence and knowledge for those who have to perform in relation to disruptions

Clause 8.5.d now makes a direct reference to validating continuity strategies and solutions (rather than simply BC arrangements)



Top Tip

Consider the underlined words (above). We’re beginning to see a pattern here. The Standard is expecting you to dig a bit deeper and consider the human aspects of business continuity. Think how you might demonstrate these requirements. You can expect a (competent) auditor to pick up on these individual words and seek assurance of your compliance with each one!

Clause 9 - Performance evaluation

Monitoring, measurement, analysis and evaluation now includes requirements to identify not only when monitoring and measuring shall be performed but also when the results shall be analysed and evaluated but also by whom. This accountability may help focus minds and whilst I always encourage organisations to take this extra step, this is now a requirement.

Reference to performance metrics has been removed but that isn’t to say you should automatically stop producing them, if they are helpful to you.

With the tidying up of clause requirements. Performance Evaluation now only focuses on the business continuity management system and not business continuity documentation and capabilities.

Strangely, there is no longer a specific requirement for internal audit programmes to be based (amongst other things) on the results of risk assessments. Whilst unexplained and simply following the way other MSS have been revised, this is surely a consideration for all departments responsible for planning and conducting internal audits.

Management Review Inputs and Outputs have been re-organised and the lists are shorter. However, beware some requirements, such as considering the results of exercises and testing, may have been removed from the latest “input” requirements only to have been inserted into clause 8.6 (b).

Finally, Continual Improvement has been expanded upon (a bit) and now requires the organisation to make good use of the BCMS analysis it has undertaken in its ongoing goal of improvement. For die hard management system users, this is unlikely to present a challenge but I frequently come across organisations which appear to have overlooked the underlying purpose/s of having a management system and therefore the need to take a step back and consider how it’s maximising the data generated from all their hard work!

Summary

ISO 22301:2019 requires a keen eye to spot the changes but more importantly, in my opinion, a broader view of business continuity management and the system it forms part of. A BCMS still requires the majority of its components to focus on the Planning element of the PLAN, DO, CHECK, ACT model so bear this in mind both when you are developing your BCMS as well as reviewing and updating it.



Top Tip

My final tip is when faced with a “list” of requirements in a standard, many an auditor will use this as a crutch on which to base their questions. They are easy pickings to work through, like any checklist, so be prepared to be able to demonstrate your compliance to each “sub” requirement. The downside to having a competent auditor is they are likely to encapsulate their questions in a more general conversation with you, mentally ticking off which points you have addressed and which remain unanswered, so be prepared!

Transitioning to ISO 22301:2019

If your organisation is currently certified to ISO 22301:2012 you are likely to have up to three years to transition to ISO 22301:2019. After 30 October 2022 certification to ISO 22301:2012 will no longer be valid.

For information, at the time of publication of this article, BSI has stated it will continue to deliver audits against ISO 22301:2012 until 30 April 2021 to allow you time to get your system updated and aligned to ISO 22301:2019.

NOTE. The above information relating to transitioning to the 2019 version of ISO 22301 has yet to be formally ratified by UKAS. Certification Bodies accredited by UKAS will also be required to transition

to ISO 22301:2019 before being able to offer accredited certification to its clients to the latest version of the standard.

Next Steps

1. Purchase your copy of ISO 22301:2019.
2. If you are already certified to ISO 22301:2012 speak to your Certification Body and ask them to explain their ISO 22301 transition programme (it may or may not include additional auditing time). Note, not all bodies may yet be in a position to answer this question!
3. If you are considering becoming certified to ISO 22301 you should be working towards the 2019 version. Depending on when you believe you will be ready for certification, your chosen Certification Body may or may not be able to offer accredited certification to the 2019 version for a few months. Check what you are signing up to first!
4. Use this article as a starting point for your transition work
5. Consider a Gap Analysis or pre-certification assessment from Perpetual Solutions to make sure you are best placed to achieve your certification goal.

About the Author

Hilary Estall MBCI is Director of [Perpetual Solutions](#), a business continuity and management system consultancy practice. Prior to starting her company in 2009 she worked for BSI, her final role being Global Scheme Manager for Business Continuity Management and the establishment of the BS 25999 BCMS certification scheme. Author of *Business Continuity Management Systems; Implementation and certification to ISO 22301*, Hilary remains an active member of the BSI Technical Committee responsible for the UK's input and development of continuity and resilience related British and ISO Management System Standards.



[Perpetual Solutions is an authorized affiliate of BSI Standards providing an authorized link to the BSI Shop.](#)

