B.3 Format and Structure

ISO 22301 is the second published standard to adopt ISO's new high-level structure for management systems standards (MSS). This structure contains ten sections plus a bibliography:

- Scope.
- Normative References.
- Terms and Definitions.
- Context of the Organization.
- Leadership.
- Planning.
- Support.
- Operation.
- Performance Evaluation.
- Improvement.

B.4 What does the standard contain?

The Table of Contents includes the sections shown in Table B-1.

Table B-1. ISO 22301 Table of Contents

B.6 Who should consider it – by country/region, size/type of organization? When might it not be relevant or appropriate, or another standard more helpful?

The ISO 22301 standard is structured to be scalable to any size or type of organization – whether a big multinational or a small enterprise; private or public; charities; for profit or not-for-profit. The key criteria are that the organization wishes to:

- Create, implement, maintain and improve a BCMS.
- Use a common language of BC throughout the enterprise.
- Align with the organization's stated business continuity policy.
- Prove conformity to stakeholders and the public.
- Gain independent certification and registration of its BCMS.
- Conform to this international standard.

It can also be used as a powerful audit tool.

This standard is applicable to virtually any organization in any part of the world for the continuance of its mission-critical activities following disruption. However, public emergency services and aid relief organizations should consider some of the other standards in the ISO 22300 family and NFPA 1600, which are perhaps more applicable to organizations with a focus on public responsibilities as opposed to self-continuation.

B.7 What about ISO 22301 certification?

Figure B-1 below summarizes the key activities that have to be undertaken.

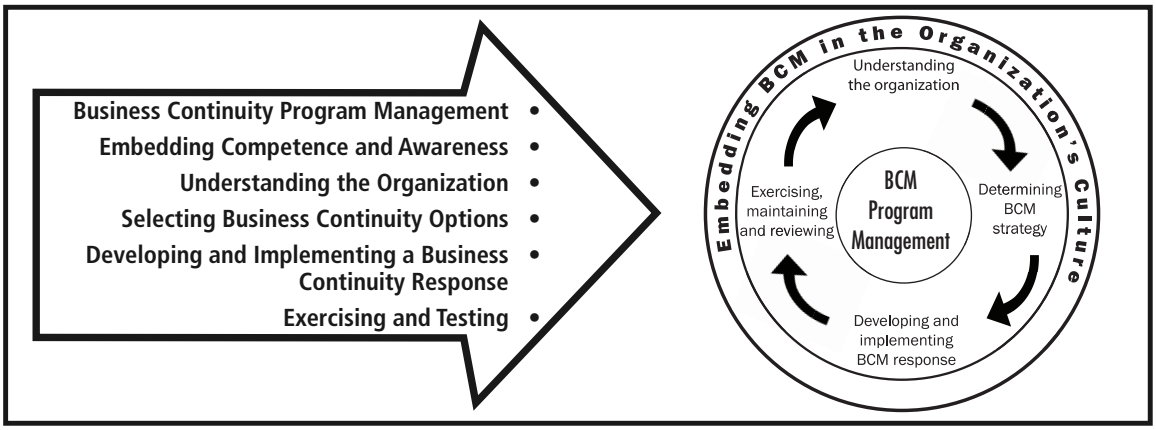

Figure B-1. ISO 22301 Lifecycle (Source: ISO[3])

There are two basic stages, and several steps, on the road to certification.

Stage 1, the Assessment Stage, sets the scope and timeframe for the project.

Step One: Obtain, understand, and agree on the standard

It sounds obvious, but you will need to buy a copy of the standard and preferably the supporting guideline before you can start preparing for your application. Read and understand them. Each word

Table B-5. BS 25999-2 versus ISO 22301 – Similarities and Differences

Key:	• No or negligible changes
	• • Moderate changes
	• • • Major changes

Most Important Areas	Section in BS 25999-2	Sections in ISO 22301	Change
Understanding the organization	–	4.1	•••
Understanding the needs and expectations of interested parties	–	4.2	•••
Determining the scope	3.2.1	4.3	••
Management commitment	–	5.2	•••
Business continuity policy	3.2.2	5.3	••
Business continuity objectives	3.2.1.1	6.2	••
Competences	3.2.4	7.2	•
Awareness	3.3	7.3	•
Communication & warning system	4.3.3.3	7.4, 8.4.2, 8.4.3	•••
Documented information	3.4	7.5	••
Business impact analysis	4.1.1	8.2.1, 8.2.2	•
Risk assessment	4.1.2	8.2.1, 8.2.3	••
Business continuity strategy	4.2	8.3.1	•
Resource requirements	4.3.2.2, 4.3.3.3	8.3.2	••
Risk treatment (protection & mitigation)	4.1.3	8.3.3	•
Incident response structure	4.3.2	8.4.2	•
Business continuity plans/recovery plans	4.3.3	8.4.4, 8.4.5	•
Exercising & testing	4.4.2	8.5	•
Monitoring, measurement, analysis & evaluation	4.4.3	9.1	•••
Internal audit	5.1	9.2	•
Management review	5.2	9.3	•
Nonconformity & corrective action	6.1.3	10.1	••
Preventative action	6.1.2	6.1, 9.1.1	••

The organization therefore decided in 2011 to become certified to the BCM standard as soon as possible following its release that year, and with little change between the final draft and the published ISO standard, there were few changes to be made to its implemented management system.

The decision to become an early adopter was an interesting one as this was a new certification and not a transition from BS 25999, the British standard on which the ISO is largely based. Andrew Macleod, BCM Consultant at Needhams, explains the thinking behind becoming an early adopter of the new standard:

> As you would expect from the nature of our business, we have always had a business continuity management system in place. However, it was felt that certification to BS 25999 wouldn't give us the competitive advantage, particularly within the overseas markets.
>
> BS 25999 was published in 2007 and the business continuity environment has changed since. The revision of the standard has made it more meaningful, precise, and relevant to today's organizations, and there are now better ways to conduct your BCMS than previously thought.
>
> From our experience, we found that while many companies chose to align their BCM systems to BS 25999, many also saw it as something of an administrative burden. With the introduction of ISO 22301, however, I think many will reconsider this position.
>
> Certainly, when the ISO standard was approaching publication, we felt that we needed to become an early adopter of external certification. And now we are certified, we can approach our clients from a position of first-hand knowledge of the process – it's a strong position to be in.

B.18 Looking forward – what else should organizations be considering, aside from ISO 22301?

ISO 22301 is just one of several standards which ISO 22312: Technical Specifications says are intended to "... work towards international standardization that provides protection from and response to risks of unintentionally, intentionally, and naturally-caused crises and disasters that disrupt and have consequences on societal functions." This series of standards covers "public planning and response" and also "private sector planning and response."

TC 223 has the additional standards in hand:[19]

- ISO 22300 Societal Security – Vocabulary provides a reference for the BC-related terms that will become standard international usage.
- ISO/DIS 22311 Societal Security – Video Surveillance – Export Interoperability.
- ISO/TR 22312:2011 Societal Security – Technological Capabilities documents the knowledge gathered in the six-month study period conducted by ISO/TC 223/Ad hoc group 1 (AHG1), in which AHG1 examined the different existing available technologies which would be relevant to standardize within the field of societal security.
- ISO 22313 Societal Security – Business Continuity Management Systems – Guidance tells you how to interpret the requirements of ISO 22301. This is also used by certifying bodies as a checklist for your understanding of the requirements.
- ISO 22315 Societal Security – Mass Evacuation aims to specify a good practice framework to assess the plans for the mass evacuation of a large area. The framework covers the six planning activities of preparing the public to evacuate, understanding the evacuation zone, making evacuation decisions, disseminating the warning message, evacuating pedestrians and traffic, and shelter management.

- ISO 22320:2011 Societal Security – Emergency Management – Requirements for Incident Response establishes a basis for the coordination and cooperation between all parties involved in handling an incident. It reduces the risk of misunderstandings and provides a more effective use of combined resources. It is also intended to improve interoperability by specifying processes, systems of work, data capture, and management to provide timely, relevant, and accurate operational information.
- ISO 22322 Societal Security – Emergency Management – Public Warning outlines international good practice for setting up an incident response system. It defines requirements for the individual and collaborative preparation and implementation of effective incident responses.
- ISO 22323 Societal Security – Organizational Resilience Management Systems – Requirements with Guidance for Use, based on ASIS International SPC.1.2009, relates to operating a management system that "integrates risk assessment, anticipation, prevention, protection, deterrence, readiness, prevention, mitigation, response, and recovery when managing the uncertainty of achieving objectives (risk) related to disruption (intentional, unintentional and natural)." It clearly has potential to overlap with BC and possibly divide the market.
- ISO 22325 Societal Security – Guidelines for Emergency Capability Assessment for Organizations.
- ISO 22351 Societal Security – Emergency Management – Shared Situational Awareness links emergency management aspects of ISO 14001 – Environmental Management System with an organization's overall Emergency Management System for Improving Readiness Assurance.
- ISO 22397 Societal Security – Guideline to Set Up a Public Private Partnership provides broad guidelines to create partnership agreements between organizations to improve coordination, collaboration and cooperation before, during, and after disruptions.
- ISO 22398 Societal Security – Guideline for Exercises and Testing provides advice on managing your testing and exercise program. This document includes "discussion-based" and "operationally-based" aspects and includes useful appendices or "annexes" with examples of many elements, ranging from scenario development to evaluation of the actual exercise.
- ISO 22399 Societal Security – Guideline for Incident Preparedness and Operational Continuity Management provides a generic guideline to develop a management system to ensure incident preparedness and operational continuity. It also gives guidance on developing performance criteria for incident preparedness and operational continuity.
- ISO 22324 Societal Security – Emergency Management – Color-coded Alert.

B.19 So is ISO 22301 the ultimate, the final, the last, BC standard?

No, the publication of ISO 22301 cannot be interpreted to mean that there is no longer a need for new standards. There is such a need, particularly to deal with newer technologies: some of the issues with cloud computing are mentioned at 6.3.5.2. However, in a recent survey:[20]

- 52% of respondents with no plans to use cloud services identify security as the main inhibitor.