the Availability Digest

www.availabilitydigest.com

ISO 22301 – The New Business Continuity Management Standard

October 2012

ISO 22301, issued on May 15, 2012, is the first international standard for Business Continuity Management (BCM). It builds on the British Standards Institution's BS 25992-2 standard which has been widely accepted outside of the UK. It is a relatively brief specification, taking only fifteen pages exclusive of definitions and bibliography.

Its title, Societal security – Business continuity management systems – Requirements, was chosen with care. *Societal security* refers to the fact that no organization works in a vacuum. It interacts with its customers, suppliers, government agencies, and others. As such, it is a critical part of a larger society.

Business continuity management systems are part of the overall management systems that establish, implement, operate, review, maintain, and improve business continuity.

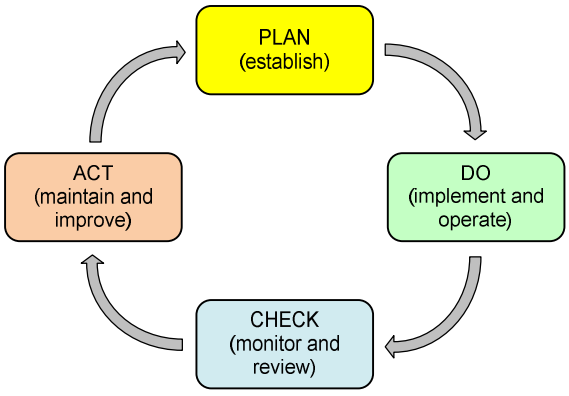
Requirements imply rigor and compliance.

Our modern just-in-time business processes would not be possible without interconnected IT systems and interconnected organizations. A disruption somewhere in this supply chain can have a ripple effect throughout the society in which the disrupted process or system is a part. Natural and man-made disasters will happen. We cannot always avert them. But we can anticipate them and take steps to prevent the cascading of the consequences that often follow.

PLAN-DO-CHECK-ACT Model

ISO 22301 is based on the ISO PLAN-DO-CHECK-ACT model to establish, implement, operate, monitor, review, maintain, and improve the effectiveness of the organization's business continuity management system (BCMS).

PLAN: Planning establishes the organization's business continuity policy. It involves the understanding of the nature of the organization and formalizes the commitment of corporate leadership to business continuity. It plans out the BCMS project objectives, and it establishes a foundation for organizational support.



DO: The BCMS plan is implemented, including a Business Impact Assessment (BIA) and a Risk Assessment. The exercising and testing of the plan is formulated, and the plan becomes operational throughout the organization.

CHECK: The organization verifies that the performance of the results of the BCMS can be consistently achieved. Verification is accomplished through effective monitoring and ongoing evaluation of results. The results are communicated to management for review, and actions are determined for remediation and improvement.

ACT: The changes from the Check phase are incorporated into the plan in a timely manner in order to maintain and continually improve the BCMS.

The ISO 22301 Specification

ISO 22301 comprises eleven sections, or *clauses*. The first four clauses (Clauses 0 through 3) are general, including an introduction that describes the PLAN-DO-CHECK-ACT model, a Scope, References (void), and definitions.

Clauses four through ten comprise the meat of the specification. Clauses 4 through 7 expand the Plan phase. Clause 8 describes the DO phase; and Clauses 9 and 10 address, respectively, the Check and Act phases.

Clause 4 – Context of the Organization

This clause establishes the scope of the BCMS. The internal and external issues that are relevant to business continuity are determined. The organization's services, products, partnerships, and supply chains are identified, and the organization's risk tolerance for disruption of any of these relationships is established.

The organization shall ensure that the applicable legal, regulatory, and other requirements imposed upon it are protected by the BCMS.

The parts of the organization to be included in the BCMS shall be identified. Any exclusions shall not affect the organization's ability to provide continuity of its services and operations.

Clause 5 – Leadership

Top management shall demonstrate leadership and commitment to the BCMS. It shall ensure that the BCMS requirements are integrated into the organization's business processes and that appropriate resources needed for the BCMS are available.

Management shall establish a business continuity policy that provides a framework for setting business continuity objectives, and it shall appoint individuals with the proper authority to be accountable for the implementation and maintenance of the BCMS.

Top management shall be actively engaged in the testing and exercise of the BCMS and shall ensure that internal audits are conducted.

Clause 6 – Planning

The organization shall determine the risks and opportunities that need to be addressed to ensure that the BCMS can achieve its intended outcome with no undesired effects, and it shall provide a plan for continual improvement.

The business continuity objectives shall take into account the minimum level of products and services that is acceptable. These objectives shall be monitored and updated as applicable.

The organization shall determine who will be responsible for meeting the objectives, what resources will be required, and how the results will be evaluated.

Clause 7 – Support

The organization shall provide the resources necessary for the establishment, implementation, maintenance, and continual improvement of the BCMS. People assigned to BCMS tasks shall be demonstrably competent. They shall be aware of the business continuity policy, the implications of not conforming to the BCMS requirements, and their own role during disruptive incidents.

The organization shall determine the need for internal and external communications, including the content, the timing, and the audience for different messages. This shall include communication with employees, customers, partners, the community, appropriate authorities, and the media. Communication facilities intended for use during disruptive events shall be tested.

The BCMS shall be documented to the extent determined by the organization as being necessary for the effective implementation of the BCMS procedures. The documented information shall be controlled to assure its preservation, availability, change control, and the prevention of unintended use of obsolete information. Protection shall be provided to prevent the compromise or the unauthorized modification or deletion of the documentation.

Clause 8 – Operations

The organization shall plan, implement, and control the processes needed to meet the BCMS requirements. It shall establish criteria for the processes and implement control of the processes in accordance with the criteria.

A formal process for business impact analysis and risk assessment shall be established. This analysis shall take into account legal and other requirements that may be imposed on the corporation and shall be kept up-to-date and confidential.

The business impact analysis shall identify the activities that support the organization's products and services, the impacts of not performing these activities, the minimum acceptable timeframes for resuming these activities, and the dependencies for these activities including suppliers, partners, and other relevant parties.

The risk assessment evaluates the risk of disruptive events to the organization. It identifies which disruptive risks require treatment and describes the treatments commensurate with the organization's business continuity objectives.

Based on the results of the business impact analysis and the risk assessment, the organization shall determine a strategy to protect prioritized activities. This strategy shall include stabilizing, recovering, and resuming prioritized activities within the specified time frames and mitigating the impact of their disruption. Proactive measures for reducing the likelihood of disruption of prioritized activities, shortening the disruption period, and limiting the impact of a disruption on the organization's products and services shall be considered.

The resources needed to implement the strategies shall be determined. Resources include people, information and data, equipment, facilities and consumables, IT and communication systems, transportation, finance, and partners.

The procedures to be followed in the event of a disruption shall be well documented. They shall be specific regarding the immediate steps to be taken during a disruption and be flexible to respond to unanticipated threats and changing conditions. Impact thresholds that justify the initiation of a formal

response shall be identified, and communication with interested parties, emergency responders, authorities, and the media shall be specified. Life safety shall be the first priority.

There shall be documented procedures for restoring normal business activities from the temporary measures adopted to support the disruption.

The organization's business continuity procedures shall be exercised and tested periodically to ensure that they are consistent with the organization's business continuity objectives.

Clause 9 – Performance Evaluation

The organization shall determine what needs to be monitored and measured and the methods and intervals for these activities. These procedures shall define the performance metrics appropriate to the needs of the organization. Results shall be recorded to facilitate subsequent corrective actions.

When a disruptive incident occurs, a post-incident review shall be undertaken to determine the effectiveness of the BCMS and to suggest potential improvements to it.

The organization shall conduct internal audits periodically to determine whether the BCMS conforms to the organization's requirements and is effectively implemented and maintained. Those responsible for an area being audited shall ensure that any necessary corrections are undertaken without undue delay.

Top management shall review the BCMS at prescribed intervals to ensure its continued suitability, adequacy, and effectiveness. The review shall conclude with proposed revisions to the BCMS to improve its effectiveness.

Clause 10 – Improvement

Nonconformity with the organization's business continuity objectives may be discovered via the exercising and testing of the BCMS, via the internal audits, or from top management reviews. Nonconformites shall be corrected via changes to the BCMS.

An evaluation shall be undertaken to determine if a nonconformity occurs elsewhere. If so, additional corrections to the BCMS shall be made.

The organization shall continually improve the suitability, adequacy, and effectiveness of its BCMS.

Summary

ISO 22301 is just the first business continuity specification to be issued by ISO. Coming soon are ISO 22313 – Guidance to Creating a Business Continuity Management System and ISO 22390 – Guidelines for Exercising and Testing

Acknowledgement

We thank our subscriber, Dr. Bruce Holenstein, for bringing this topic to our attention.