ISO 22301 & 22313

Business Continuity Management System Standards and Application for Incident Communication Plans

everbridge

ISO 22301 & 22313:

Business Continuity Management System Standards and Application for Incident Communication Plans

In today's world, there is an ever increasing array of risks facing all businesses, including natural (meteorological, geological, or biological), human (accidental or intentional), and technological (power, telecommunications, hardware, software, and cyber security). The impact of these hazards can be catastrophic - whether directly affecting the organization, or indirectly interrupting their supply chain, vendors, or business partners. Even small interruptions cause damage to a company's financials and reputation, which means that organizations need a way to prevent potential downtime before it occurs.

To ensure resiliency, or business continuity, organizations need ongoing practices to manage risk and to be prepared for quick and effective response, recovery, and resumption of normal operations. As such, all organizations must incorporate business continuity disciplines into their core management practices.

In addition to safeguarding business interests, organizations have a responsibility to protect the life and safety of their people. In part, this can be accomplished by managing communications when responding to a threat or crisis. Effective, timely communications can also help protect a company's brand and reputation during an event. As a result, development of an Incident Notification and Crisis Communication plan is an important component of business continuity planning.

While developing a business continuity plan can be challenging, efforts to guide organizations by defining standards and best practices have made great progress. In May 2012, the International Standards Organization (ISO) published the first 'international' standard for Business Continuity Management Systems (BCMS), known as ISO 22301. ISO, the world's largest developer and publisher of standards, builds standards by 'consensus', using subject matter experts and professionals from a network of 164 national standards bodies around the world. These experts have been organized into a 'technical committee' (TC 223) to negotiate all aspects of the Societal Security standards, including scope, key definitions and content.

ISO 22301, like many well-known ISO standards, is a management system standard. A "management system" is the framework of processes and procedures used to ensure that an organization can fulfill all tasks required to achieve its objectives.[1] An effective management system has many benefits, including more efficient resource use, improved risk management, and increased customer satisfaction as services and products consistently deliver what they promise.

ISO 22301: Societal Security – Business Continuity Management Systems - Requirements

ISO 22301 specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to prepare for, respond to and recover from disruptive events when they arise.

Because ISO 22301 is a requirements document, accredited professionals can audit to the standard and issue certifications of compliance for organizations that meet the requirements. Like many ISO standards, compliance with and certification for ISO 22301 is voluntary.

ISO 22313: Societal Security – Business Continuity Management Systems - Guidance

In reality, many companies are unprepared for certification of their BCMS. Even if a company has a continuity plan in place, it may not address continuity risks across the entire organization, follow recognized best practices or standards, or be sufficiently tested and maintained. Responding to this need, ISO published a new companion standard for BCMS in December 2012, known as ISO 22313. ISO 22313 expands upon and aligns with ISO 22301 requirements and offers guidance to organizations that are developing or improving their BCMS capabilities. This resource helps by clarifying the intent of the requirements in ISO 22301, and by providing explanations and examples.

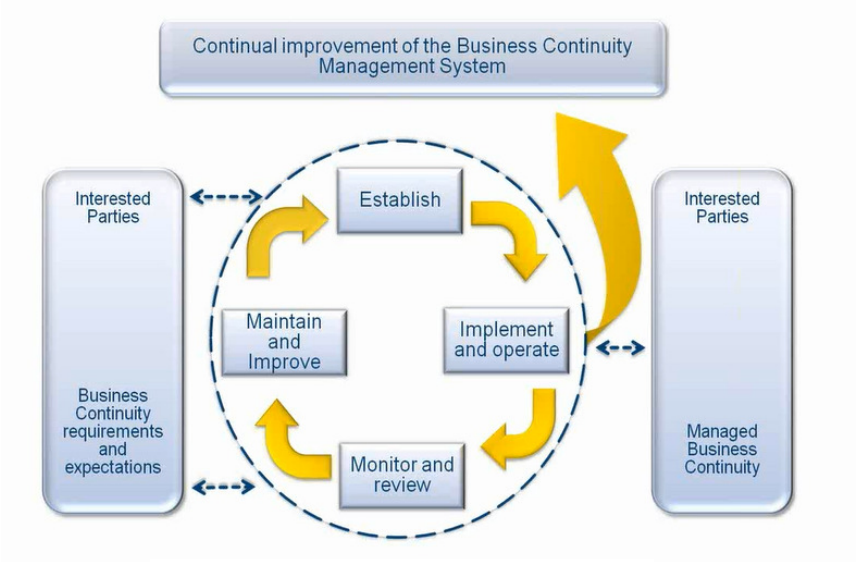
[1] Anderson, Chris. How to Build Effective Management Systems, Bizmanualz, January 26, 2005.

Plan-Do-Check-Act

Like all ISO management system standards, ISO 22301 and 22313 are based on the principle of continual improvement. An organization or company assesses its current situation, establishes objectives and develops policy, implements actions to meet these objectives and then measures the results. With this information the effectiveness of the policy, and the actions taken to achieve it, can be continually reviewed and improved.

ISO 22301 and 22313 apply the widely adopted Plan-Do-Check-Act (PDCA) model to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of an organization's BCMS[2].

The PDCA model provides concepts and language that help organizations define the maturity of their management system capabilities, identify gaps, and develop actions that improve key practices to achieve the desired or justifiable level of maturity. A wide variety of capability maturity models (CMM) has been developed with this intent, although no CMM has been developed or widely adopted for ISO 22301 at this point.



The Plan-Do-Check-Act Model

[2] ISO. (2013). Management system standards. Retrieved from http://www.iso.org/iso/home/standards/management-standards.htm

ISO 22301 Adoption Progress

ISO 22301 has already been adopted as the standard in many nations that have led the way in Business Continuity Management. As of November 2012, the previous standard in the UK, and the first standard that led to accredited certification, BS 25999-2 from the British Standards Institute (BSI), has been withdrawn and replaced by ISO 22301. A two year transition plan for organizations that have already certified to BS 25000-2 is in progress. In the US, the voluntary Private Sector Preparedness program (PS-Prep) sponsored by the Department of Homeland Security and FEMA, has initiated a process to approve and adopt ISO 22301. PS-Prep was an outcome of recommendations from the 9/11 Commission and already recognizes other BCMS standards, including BS 25999-2, NFPA 1600, and ASIS SPC.1.

Structure and Content of ISO 22301 and 22313

ISO 22301 and 22313 are intended to be applicable to all sizes and types of organizations, including large, medium and small organizations operating in industrial, commercial, public and not-for-profit sectors[3]. Both documents are broken into 10 clauses, which will be reviewed briefly on the following pages.

Clauses 1 Through 3

Clauses 1 through 3 provide background information for the document: Scope, Normative References, and Terms and Definitions.

Clauses 4 Through 10

Clauses 4 through 10 provide the core content to describe the Management System in question, and can be directly related to the PDCA model provided above:

- Clause 4: Context of the organization (Establish / PLAN)
- Clause 5: Leadership (Establish / PLAN)
- Clause 6: Planning (Establish / PLAN)
- Clause 7: Support (Establish / PLAN)
- Clause 8: Operation (Implement and Operate / DO)
- Clause 9: Performance evaluation (Monitor and Review / CHECK)
- Clause 10: Improvement (Maintain and Improve / ACT)

[3] ISO. (2013). ISO 22313:2012. Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=50050

Clause 4: Context of the organization (Establish / PLAN)

Evaluate and understand the internal and external factors relevant to the purpose and operations of the organization. This establishes foundational information for developing, implementing and improving a BCMS. The ISO standard provides examples of both internal and external factors to consider. Special focus is given to understanding the needs and expectations of interested parties, and determining the scope of the BC management system.

Clause 5: Leadership (Establish / PLAN)

Demonstrate management commitment and leadership in establishing objectives for and implementing a business continuity management system. The standards provide excellent examples and guidance for how this can be demonstrated and accomplished, such as; ensuring BCMS policy and objectives align with strategic objectives of the organization, ensuring BCM roles and responsibilities are clear, communicating the importance of fulfilling the BCMS policy and objectives, actively engaging in exercising and testing, and others.

Clause 6: Planning (Establish / PLAN)

Develop strategies and specific plans for addressing the issues and requirements identified in clause 4. The ISO standards present the importance of addressing risks and opportunities, and establishing objectives with plans for achieving them. Examples and guidance include: identifying responsibilities and setting appropriate targets for completion, ensuring that stakeholders are kept informed, and making certain that progress is monitored and documented.

Clause 7: Support (Establish / PLAN)

Ensure that the organization provides the resources needed for success. This section provides requirements and guidance for identifying key elements that are needed to support BCMS and the organization's ability to respond to incidents, such as; resources, competence, awareness, communication and documented information. Experience has shown that the level of support within the organization is a critical success factor.

Clause 8: Operation (Implement and Operate / DO)

Provide the elements of BCMS operations needed to achieve business continuity. This section defines; operational planning and methods of control; business impact analysis (BIA) to understand how the business is affected by disruption and how this changes over time; ongoing risk assessment to identify, analyze, and evaluate the risks of business disruptions in a structured way. Additional requirements and guidance is provided for establishing the incident response structure, provide warning and communication (more detail provided below), documenting and using continuity plans and procedures for recovery, the crucial need to test and exercise the plans.

Clause 9: Performance evaluation (Monitor and Review / CHECK)

Determine what needs to be monitored and measured, and how and when it will be done and evaluated. This section provides requirements and guidance for evaluating the organization's performance against the plan. For example, the use of internal audits is described, as well as methods for management review of the overall BCMS.

Clause 10: Improvement (Maintain and Improve / ACT)

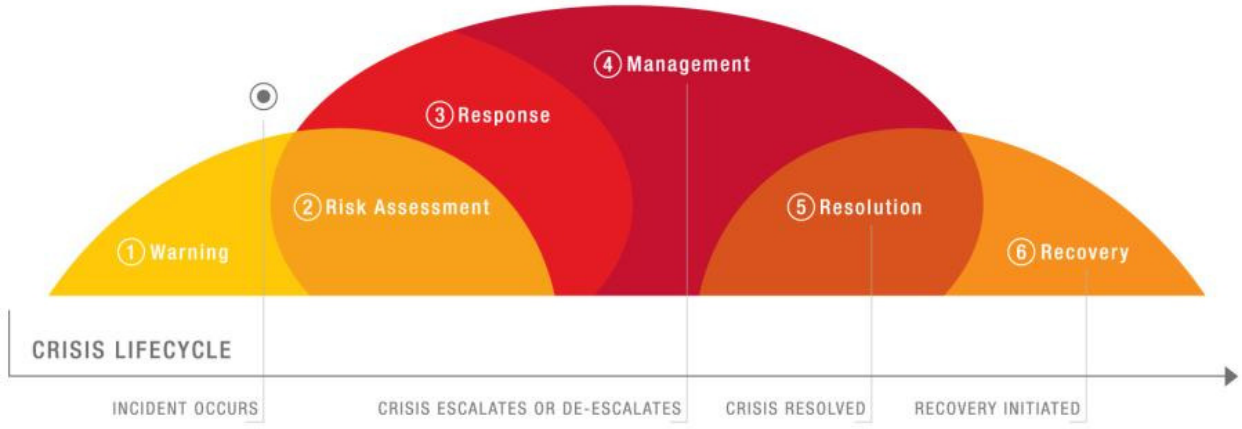
Act upon findings from performance evaluation. Define defines the need to take corrective actions from non-conformities, provides examples of actions organizations can take to improve the BCMS over time and ensure corrective actions from audits, reviews and exercises are addressed. Mature organizations recognize the need for ongoing, continuous improvement.

Application of BCMS standards to Incident Notification and Crisis Communications

Although ISO 22301 and 22313 provide requirements and guidance for the overall Business Continuity Management System, they can also be applied to any of the individual components of an overall plan. An example of one of these components, and an important aspect of business continuity preparation, is an Incident Notification and Crisis Communications plan.

Establishing an effective Incident Notification and Crisis Communications plan

The ISO standards provide requirements and guidance to establish an effective Business Continuity Management System, including Incident Notification and Crisis Communications. The ability to communicate throughout the life cycle of an incident or crisis is crucial; beginning with the initial warning of an impending incident, if anticipated, or immediately after an incident occurs, if unexpected. During this early stage of a response, communication is crucial to protect life and safety, and the business reputation and brand. As the response continues, effective communication is necessary to assess damage and mitigate the risk of further damage, manage the ongoing response, develop resolutions to the incident, and quickly initiate recovery and resumption of normal business operations.



COMMUNICATION DURING A CRISIS

Source: Robert C. Chandler, PhD - Director, Nicholson School of Communication

Development and deployment of an effective Incident Notification and Crisis Communications Plan require the same management system practices detailed in the ISO standards. The plan needs to be based on the Plan-Do-Check-Act model, requiring a clear understanding of the overall organization, strong leadership, good planning, full support for success, well controlled operations, careful evaluation of performance, and methods for continuous improvement.

ISO 22301 and 22313 both specifically highlight the importance of incident communication; including the examples of requirements and guidance presented below:

Support Checklist (derived from Clause 7 of ISO 22301 and 22313)

- ✓ Make adequate provision for communication technology and communication with interested parties
- ✓ Establish incident response teams, such as communications, and provide team members with the necessary competence, authority and responsibility to successfully manage an incident
- ✓ Provide communication procedures to provide effective exchange of information with interested parties
- ✓ Determine what, when and with whom the organization will communicate, both internally and externally
- ✓ Implement and maintain procedures for internal and external communications (such as; employees, customers, suppliers, local community, media, and other interested parties)
- ✓ Implement and maintain procedures to receive, document and respond to communications from all interested parties
- ✓ Integrate with national or regional threat advisory systems, if appropriate
- ✓ Ensure that the means of communication remains available during an incident
- ✓ Provide for the operation and testing of communications capabilities

everbridge

Operational Checklist (derived from Clause 8 of ISO 22301 and 22313)

- ✓ Establish appropriate communication procedures and protocols for activation, operation and coordination
- ✓ Using life safety as first priority, consult with interested parties to decide whether to communicate externally about an organization's significant risks
- ✓ Implement and maintain procedures for Warning and Communication
  - detecting and monitoring an impending incident
  - receiving, documenting, and responding to communication from interested parties
  - receiving, documenting, and responding to any national or regional risk advisory systems or equivalent
  - alerting interested parties that might be impacted
  - operating a communications facility
  - assuring that the means of communication remains available during an incident
  - supporting structured communications with emergency responders
  - record vital information about the incident, including actions taken and decisions made
  - ensure interoperability of multiple responding organizations and personnel
  - regular exercising of warning and communication procedures

Alignment to Related ISO Standards

In addition to ISO 22301 and 22313, a number of related ISO standards have been developed that may be beneficial to, or already adopted by your organization. Because the ISO BCMS standards are so recent, ISO 22301 was the first standard to be fully compliant with new ISO guidelines for management system structure and terminology, called ISO Guide 83. ISO 22313 follows the same guidelines, as will all ISO management systems standards. This benefits all organizations by making it easier to align and integrate with other ISO standards that might apply, providing consistent structure and language.

For example, some standards have been developed as part of the overall Societal Security standard by technical committee TC 223. Others address requirements or guidance for management systems that are closely related to BCMS. Organizations implementing the ISO 22301 standards may want to consider the following list of related ISO standards as well (not intended to be an all-inclusive list):

- **ISO 22300 Societal Security – Terminology**: Contains terms and definitions applicable to societal security to establish a common understanding so that consistent terms are used.
- **ISO 22320 Societal Security – Emergency Management – Requirements for Incident Response**: Specifies minimum requirements for effective incident response and provides basics for command and control, operational information, coordination and cooperation within an incident response organization.
- **ISO 31000 Risk Management – Principles and Guidelines**: Provides principles and generic guidelines on risk management that can be applied throughout the life of an organization, and to a wide range of activities and any type of risk.
- **ISO 27000 Information Security Management**: A series of standards specifically reserved for information security matters. The series includes a range of individual standards and documents, addressing topics such as; information security management systems (ISMS), measurement and metrics, information security risk management, and guidelines for accreditation of organizations offering ISMS certification.
- **ISO 28000 Specification for Security Management Systems for the Supply Chain**: Specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain.
- **ISO 9004 Managing for the Sustained Success of an Organization**: Provides guidance to organizations to support the achievement of sustained success using a quality management approach.

Recommendations

Improve your existing BCMS – adopt the ISO 22301 and 22313 standards

Depending on the maturity of their overall BCMS, organizations should consider acquiring either ISO 22301 (requirements) or ISO 22311 (guidance) or both. ISO 22301 is the standard that will be used to audit organizations for certification, or can be used to self-assess compliance. The guidance document (ISO 22313) is an excellent resource for organizations that are looking to improve their overall BCMS program capabilities.

The standards can be purchased for a small publishing fee. In the US, purchase from the American National Standards Institute (ANSI) at http://webstore.ansi.org. Internationally and in the UK, purchase from British Standards Institute (BSI) at http://www.bsigroup.com/en-GB/iso-22301-business-continuity. ISO standards can also be purchased directly from ISO at http://www.iso.org/iso/home/store/catalogue_ics.htm.

Protect your business and people – establish an Incident Notification and Crisis Communications plan

Following the requirements and guidance outlined in the ISO standards, create an Incident Notification and Crisis Communications plan as part of your overall Business Continuity Management System. This plan should account for communications throughout the life cycle of an incident or crisis; beginning with either the initial warning of an anticipated incident or immediately after an unanticipated incident occurs, and continuing through recovery and resumption of normal business operations.

Certification – certify your BCMS

A number of auditing organizations have been accredited to provide certification for ISO 22301 internationally. ISO 22301 has not yet been fully adopted in the US, but this is considered to be imminent. Currently, in the US, certification is provided for PS-Prep (described in Section I) using the standards BS25999-2, NFPS 1600, ASIS SPC.1. In the UK and internationally ISO 22301 certification bodies are fully active.

Benefits of certification include:

- Increased and improved awareness, understanding and management of continuity risks
- Reduced impact and improved management of disruptive incidents, including reduced recovery times
- Increased capabilities for protecting human life and safety, reputation and brand, all assets and business commitments
- Demonstrates to employees, customers, clients, partners, suppliers, and other stakeholders that the organization is committed to resilience, which can provide a competitive edge.

Conclusion

Regardless of your current capabilities, these ISO standards offer a path for continuous improvement of your Business Continuity Management System. They represent many years of lessons learned and proven best practices. All organizations have responsibility to their stakeholders to deliver on commitments regardless of disruptions that can and will occur. Whether these are used as a reference, a framework for improvement, or requirements for certification, they provide value to all organizations.

About Everbridge

Everbridge provides industry-leading interactive communication and mass notification solutions to organizations in all major industries and government sectors.

Communication failures have historically plagued organizations in their ability to respond to and minimize the human, operational and financial impact of critical events and emergency incidents. Everbridge began with a shared vision: empowering a single person to communicate with any number of people as easily as communicating with one person to save lives, protect assets, minimize loss, and ensure continuity of operations. Everbridge brings technology and expertise together at every level for a complete solution. Everbridge solutions match your unique needs, from safety and survival during a crisis to cutting costs and achieving efficiencies in your everyday operations. Our understanding of mass notification and interactive communication challenges is leveraged in everything we do, from how we build our technology from the ground up to the expertise of the people we hire and best practices we share with the community.

We design the Everbridge system according to several key tenets:

- **Target the individual** – not the device. Everbridge has the most comprehensive notification system available, offering more than 30 contact paths that can be designated by incident type or by escalation steps.
- **Ease-of-use during any situation** – emergency or daily use – so even a non-technical person can communicate effortlessly and without anxiety.
- **Speed and reliability of communications.** Every second counts in an emergency. With global datacenters and an infrastructure unparalleled in security and reliability, the Everbridge mass notification system is designed for rapid and efficient communications worldwide so your message will always go through.
- **Universal accessibility** – with a fully managed system requiring no hardware, no software, no maintenance, and a flexible pay-as-you-grow model, organizations large and small have access to the same powerful communication capabilities.
- **Scalability** – the Everbridge mass notification system provides the ultimate flexibility in communication capabilities to meet changing needs in today's dynamic environment. The Everbridge system is inherently scalable to grow with and adjust to the requirements of any organization quickly and without disruption to internal processes, infrastructure, or resources.

Visit www.everbridge.com to learn more.