MIR3℠
INTELLIGENT NOTIFICATION

Alphabet Soup: Making Sense of BC/DR Standards

Part 1:

Business Continuity Standards – A Primer

Why all the attention now?

One of the hottest topics in BC/DR these days is standards. BC standards have been around for a while, but the rollout of the Department of Homeland Security's (DHS) Private Sector Preparedness initiative (PS Prep) focused new attention on the subject and put the quest for comprehensive and effective standards on a fast track. In the process, three standards have emerged as leaders for certification and recognition under the PS Prep Program: NFPA 1600, BS25999 and ASIS SPC.1.

This brief will give you an overview of each of the major standards, touching on international standards and established guidelines and regulations that drive the definition and implementation of BC programs.

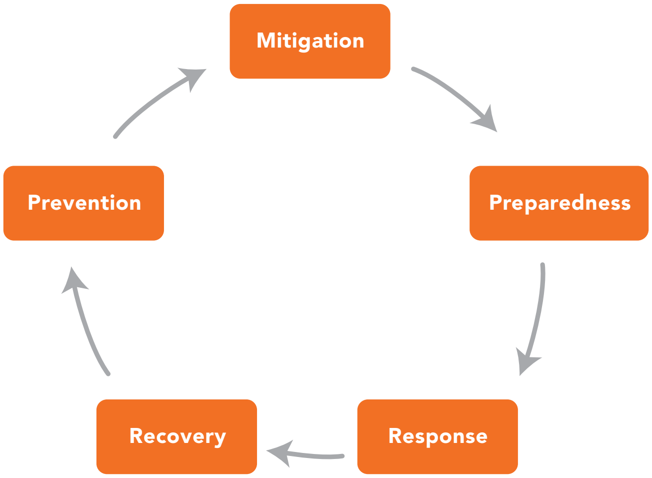
Which standard is best?

NFPA 1600

The NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs* provides a basis for BC/DR programs by providing common program elements, techniques, and processes. This standard follows a "total program approach" to enhancing disaster/emergency management and BC programs to manage the impact of disasters. The NFPA standard emphasizes program policies and management components, providing guidelines that address the analysis, planning and implementation of the core elements of crisis management, business resumption planning and IT disaster recovery.

To certify to the NFPA 1600 standard, your organization must develop a fully documented program to be run by a program coordinator and an advisory committee whose primary function is to administer, maintain, and review the organization's program. The standard identifies five primary aspects in its response program:

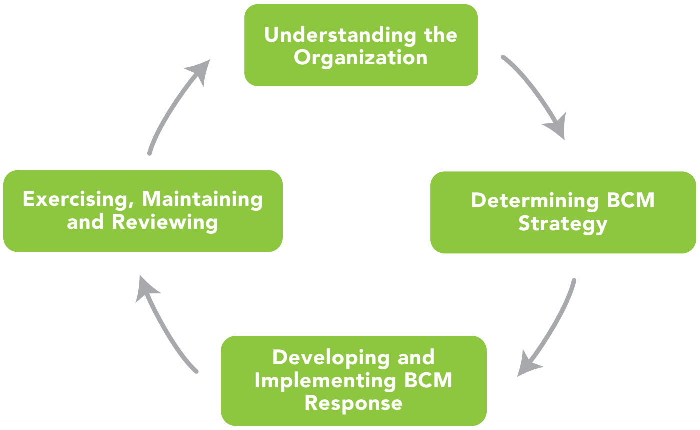
- Mitigation
- Preparedness
- Response
- Recovery
- Prevention



These aspects are in line with the analysis and planning/implementation of the core elements of PS Prep. NFPA 1600 addresses these core elements by requiring risk assessments, impact analyses, incident prevention strategies, mitigation strategies, resource management and logistics, incident management systems, and operational procedures in order to prevent, prepare for, and respond to a disaster or emergency situation. The NFPA 1600 standard emphasizes a regular planning process in order to improve current strategies and confront newly identified problems.

BS 25999-2

The British Standard 25999-2:2007* specification for business continuity management (BCM) defines requirements for a management systems approach. The emphasis of this standard is on creating, implementing, and managing an effective BCM system and then embedding it within the organization's culture. The standard primarily focuses on the planning and implementation of the core elements through its attention to continuity and recovery plans.

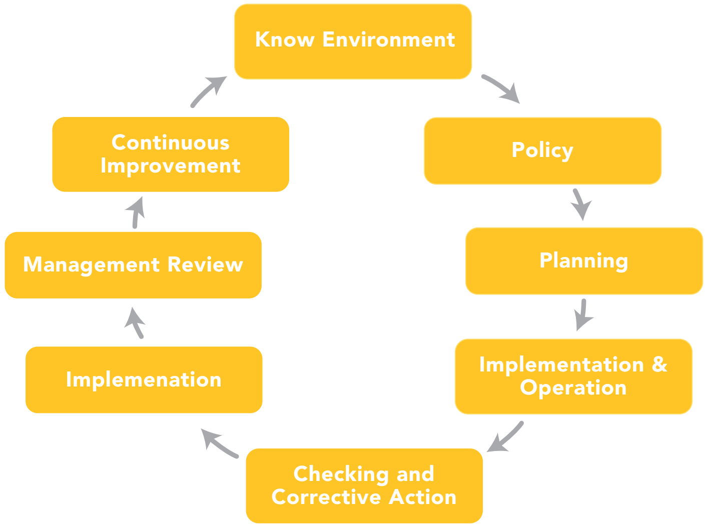

Understanding the Organization
Determining BCM Strategy
Developing and Implementing BCM Response
Exercising, Maintaining and Reviewing

The British Standard describes detail-oriented continuity and recovery plans that organizations must enact for accreditation. It requires specifics on how your organization will reestablish operations, communications and policies during disasters and specifics on how to implement a media response strategy. The British Standard requires action and task details that need to be performed once the response plan is initiated, as well as the resources required for business continuity and business recovery efforts at different points in time.

The British Standard also emphasizes the maintenance, review, and improvement of the core elements. It requires that your organization develop and conduct exercises that are consistent within the scope of the BCM system, hold post-exercise reviews of each exercise, and review its BCM arrangements to ensure continuing suitability, adequacy, and effectiveness. This standard establishes an internal auditing system, management review of the BCMS, and reviewing inputs and outputs from the BCMS in order to ensure that management monitors and reviews its effectiveness and efficiency.

ASIS SPC.1

ASIS International SPC.1-2009 *Organizational Resilience: Security, Preparedness, and Continuity Management Systems** is a management framework for action planning and decision making to anticipate, prevent and prepare for and respond to a disruptive incident. The standard seeks to increase organizational and customer confidence by creating a safe and secure environment for both



the organization and its stakeholders. It emphasizes the planning and implementation of the core elements, as well as the maintenance, review and improvement element.

The ASIS standard plans and implements its Organizational Resilience (OR) management policy by requiring management to provide evidence of its commitment to implementing disaster/emergency response strategies. ASIS focuses on the maintenance, review and improvement element by providing auditable criteria to establish, check, maintain, and improve its management system. The standard requires your organization to implement evaluation activities that include: internal audits, exercise and testing, management reviews, input and output reviews, program maintenance, and policies aimed at continuously improving the standard.

Should you certify? Why would you?

Aligning your business continuity program and all key processes to a standard is clearly a smart decision for any organization, but needs to be considered carefully as the process takes time and resources. Here are some things to reflect on when making the decision whether or not to formally conform to a standard:

- **Regulatory environments** – Many businesses are required to operate within regulatory environments and must implement specific components in their business continuity program. Compliance and certification to a standard will complement the requirements for the regulations.
- **Organizations providing products and services that are critical to the infrastructure of the United States (as defined by the DHS)** – There are 19 sectors identified by the DHS as components of the US's critical infrastructure. While not required by the DHS to implement programs and certify to a standard, these critical sectors are encouraged to adopt the PS Prep program (and thus the approach to a standard).
- **Supply chain criticality** – Businesses are becoming more and more dependent on critical supplies, products or services to deliver products or services to customers. Interruptions in the supply chain for critical products or services is becoming more and more intolerable, resulting

in increased pressure from an organization to require critical providers, such as your business, to demonstrate preparedness through adoption and certification to a standard.

- **Competitive positioning** – Securing new business requires demonstrating a competitive advantage over the competition. Your organization can position an internal business continuity program as a competitive advantage in business development.

How do you certify to a standard?

If your company wants to certify to a standard, it must have a third-party review by an authorized certification board to validate the company's preparedness to a standard. However, in some cases a self-declaration of conformity can meet your company's goal. Regardless of the decision to move for formal certification or simply self-declaration, here's how to get started:

Step 1: Get executive buy-in
Without the commitment of executives, it'll be tough to secure the resources needed to implement all the components of a standard and complete certification.

Step 2: Choose a standard
Your organization must begin by selecting a standard that will be used in developing its internal business continuity program.

Step 3: Define the scope
It is not necessary to certify your enterprise-wide program, or all of a single location at one time. Your company may select the scope of the business continuity program to meet the business requirements that are driving the company's pursuit to certification.

Step 4: Align to any regulations required for your industry
Many of the current processes that are in place to meet certain regulatory requirements can also be applied toward implementation of key specifications within your chosen standard. This alignment exercise will help identify the gaps that must be addressed for adherence to the standard.

Step 5: Implement all the components within the selected scope
Using each of the components of the standard, within the given scope of the BC program, design and implement key processes to meet each of the specifications as defined in the standard. Remember, the certification process is a pass-fail system, requiring 100% conformity to the standard within your scope.

Step 6: Execute a self-administered assessment of conformity
Once all the components of the standard have been implemented (or as the process is being implemented), it helps if you perform a self-assessment of conformity to all the components of the standard. An audit by a third party is costly and you want to be sure your organization is

ready before attempting it. Self-assessment is a good tool to measure progress and readiness for certification. And in fact, some organizations may elect to stop at this point and use the results of the self-administered assessment of conformity as sufficient for their internal requirements as well as any external requirements.

Step 7: Select a certifying body

Once the internal program (within the scope selected) has met all of the requirements as defined by the standard, a third-party certifying body must be selected to complete an audit of the defined program scope. Selecting a third-party certifying body is an important step. The certifying body selected should be one that has identified experience within the business sector in which your company operates, particularly in regulated environments.

Step 8: Satisfactorily complete audit by the certifying body

All the hard work is done, now it is up to the certifying body to complete the audit and validate that the specifications of the standard have all been addressed completely.

Learn more about BC/DR standards and why they matter by joining the full webinar series:
Alphabet Soup: Making Sense of BC/DR Standards

MIR3: Proven technology, global reach

Founded in 1999, MIR3 is a leading developer of notification and response technology. The company has a history of meeting exacting customer requirements with innovative technologies that continue to set standards for the industry. MIR3 is the provider of choice for many of the Global FORTUNE 100 companies and thousands of other organizations around the world. When you choose MIR3, you are choosing a strong company with extensively proven technology and a solid global communication infrastructure.

* The Sloan Report, *A Framework for Voluntary Preparedness*, January 18, 2008