



16000 ASIA  
16000 ASIA

The Concise Guide to  
**BUSINESS CONTINUITY STANDARDS**

25999

## CONTENTS

<b>How standards have evolved since 2012</b>	<b>3</b>
PS-Prep – Where is it today?	3
<b>Overview of the major standards</b>	<b>3</b>
Standards in brief	4
NFPA 1600	4
ASIS SPC.1	5
ISO 22301	6
<b>The business benefits of standards</b>	<b>9</b>
<b>Determining the right standard for your organization</b>	<b>11</b>
Consider your reasons for alignment	11
Internal reasons vs. external reasons	11
Drivers that can influence the selection of a standard	12
Risk management and mitigation	12
Emergency management	12
ISO certification	12
<b>Should you align or certify?</b>	<b>12</b>
Align first, then certify	14
Alignment	14
Certification	15
Notes on implementing a standard	16
Implementation recommendations	17
Engage the C-suite	18
<b>Eight steps to certification</b>	<b>19</b>
<b>The impact of ISO 22301 on your program</b>	<b>21</b>
<b>Summary</b>	<b>22</b>

## How standards have evolved

In 2007, recognizing that much of the nation's critical infrastructure was in the hands of the private sector, the DHS (Department of Homeland Security) began to encourage preparedness in the private sector. From that charge came the Private Sector Preparedness Program, also known as PS-Prep, which identified the characteristics of a sound preparedness program for organizations.

Those early business continuity standards were initially posed as voluntary guidelines and, over time, have been adopted by organizations around the world. Today, regulated industries like finance and government are urged to follow a standard, and in order to protect their own supply chain, may request that any and all of their vendors also align to a standard.

No single standard is considered the best choice for every business, but each of the major standards has characteristics that make it more appropriate for some rather than others.

### PS-Prep – Where is it today?

In the first issue of *The Concise Guide to Business Continuity Standards* we focused on the standards that were, at that time, identified as part of the Department of Homeland Security Private Sector Preparedness (PS Prep) initiative.

Since that time, PS-Prep has been quietly continuing, although it has had little influence in the industry.

So, what's different today? What has happened with the adoption of standards? And, how does that influence what you, as a resilience professional, should know and consider when establishing and managing business continuity programs for your organization?

## Overview of the major standards

No single standard is considered the best choice for every business, but each of the major standards has characteristics that make it more appropriate for some rather than others. Each of the standards includes the core components that will lead to completion of all the essentials needed for a comprehensive business continuity program.

Please note: This paper is not an exhaustive guide to global standards, but uses the history and perspective of the US in the quest for comprehensive business continuity and disaster recovery (BC/DR) standards. While the authors recognize that there are many other highly regarded standards, both nationally and internationally, this discussion is driven by the convergence of the US Department of Homeland Security and the private sector.

Many organizations choose to align to a standard, meaning they use it as a guide to define and implement a comprehensive business continuity program. Others go beyond alignment to attain third-party certification for reasons that are explained further in this document. This paper will help you determine if you should align or certify to a standard, and if so, which standard is best for your business. Keep in mind that aligning to a standard does not guarantee recoverability—standards tell you what to do, not how to do it.

## Standards in brief

### NFPA 1600

The NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity/Continuity of Operations Programs provides a basis for BC/DR planning by providing common 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 as well as 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 and prevention.

These aspects are in line with the analysis, planning and 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,

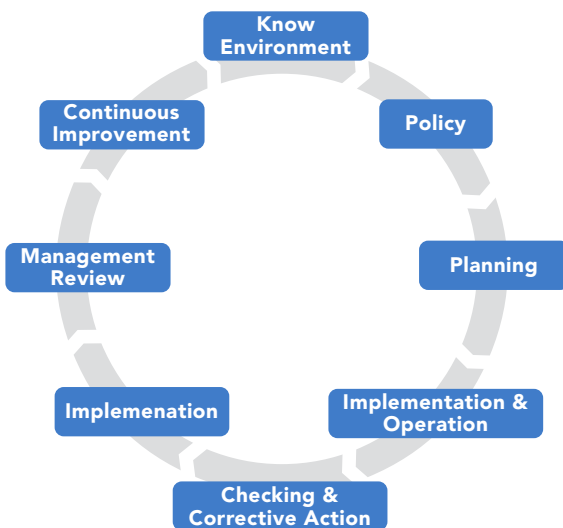


incident management systems and operational procedures in order to prevent, prepare for and respond to a disaster or emergency situation. The NFPA 1600 standard emphasizes a regular planning process in order to improve current strategies and confront newly identified problems.

NFPA 1600 is updated every three years and in 2016 included a new small business preparedness guide along with material on addressing the needs of persons with access and functional needs, as well as adding some information on the role of social media in crisis communications plans.

### ASIS SPC.1

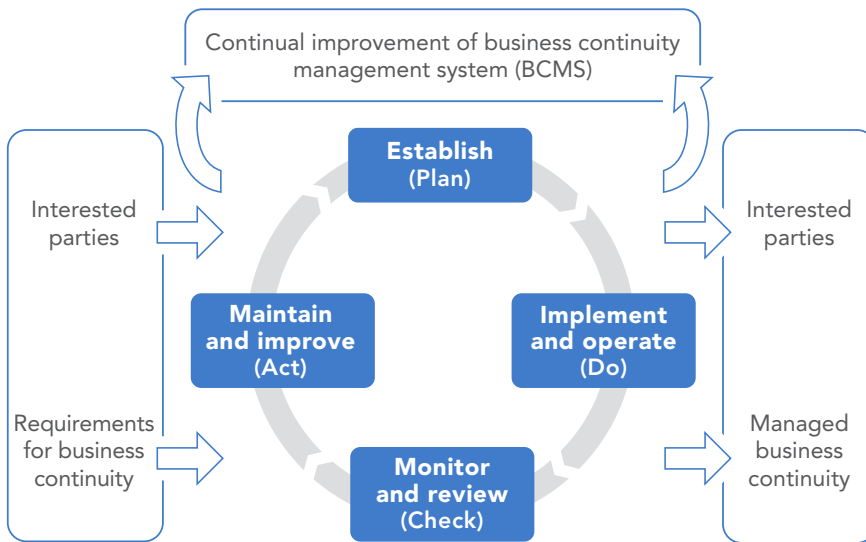
*ASIS International SPC.1-2009 Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements* is a management framework for action planning and decision making to anticipate, prevent, prepare for and respond to a disruptive incident. The ASIS SPC.1 standard seeks 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 implement 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 compliance to the standard.

### ISO 22301

One of the latest developments in the industry is the replacement of the standard BS25999 with the newer standard, ISO 22301 – Societal security – Business continuity management system – Requirements. ISO 22301 is intended to have a unifying impact on the business continuity industry at large and indeed, the momentum is growing towards acceptance of ISO 22301 as the standard of choice for many organizations. For that reason, we have taken the time to review the new standard and include the latest information about ISO 22301.



ISO 22301 was built on the foundation provided by British Standard BS 25999-2 and uses that best-practice approach at its basis. BS 25999-1 designated an incident response structure, provided incident management plan content and outlined requirements for all types plans. These requirements are still intact and have been expanded

upon in ISO 22301.

According to the BSI (British Standards Institute), the ISO 22301 standard was built around the “Plan, Do, Check, Act” concept, a stepped approach that repeats as an ongoing cycle. ISO 22301 then took a much broader approach, covering any type of disaster, including international considerations.

At its most fundamental, ISO 22301 draws a direct connection between the outputs of the BIA (business impact analysis) and RA (risk assessment) and the development of risk treatments, including strategies for continuity and recovery.

ISO 22301 provides clear documentation regarding what must be communicated in the case of an incident, when it should be communicated, and to whom. An organization that follows ISO 22301 must also establish procedures for receiving communications from interested parties. In addition

to BS25999-1, ISO 22301 also includes some of the requirements of ASIS. SPC.1:2009 and NFPA 1600:2010.

ISO 22301 places much greater emphasis on understanding quantifiable requirements, setting objectives, and measuring performance. These metrics tend to make the standard more easily accepted by top management and thus more widely adopted.

The standard also provides a sorely needed foundation of common vocabulary for business continuity best practices and processes.

The primary components of the standard are found in its clauses numbered four through ten, where BCP (business continuity planning) is formulated into a business continuity management system (BCMS).

ISO 22301 is part of a series of standards developed by ISO technical committee ISO/TC 223, Societal Security. Other standards in the series include:

- ISO 22300:2012 Terminology
- ISO 22301:2012 Business continuity management systems – Requirements
- ISO 22311:2012 Video-surveillance – Export interoperability
- ISO 22313:2012 Business continuity management systems – Guidance
- ISO 22315:2014 Mass evacuation – Guidelines for planning
- ISO 22317:2015 Business Impact Analysis
- ISO 22320:2011 Emergency management – Requirements for incident response
- ISO 22322:2015 Emergency management – Guidelines for public warning
- ISO 22324:2015 Emergency management – Guidelines for color-coded alert
- ISO 22397:2014 Guidelines for establishing partnering arrangements
- ISO 22398:2013 Guidelines for exercises
- ISO/TR 22312:2011 Technological capabilities
- ISO/TR 22351:2015 Emergency management – Message structure for interoperability
- ISO/PAS 22399:2007 Guideline for incident preparedness and operational continuity management

Regarding risk management, ISO 22301 specifically points to ISO 31000: Risk Management – Principles and Guidelines, as a reference to how to manage risk. Just as in BS 25999, the scope of the risk assessment may be limited to the scope of the business continuity management system.

ISO 22301 is intended to ensure consistency with all future and revised management system standards and integrate with, in a straightforward, way, ISO 9001 (quality), ISO 14001 (environment), and ISO/IEC 27001 (information security).

### Notes on ISO 22301 adoption

According to the BCI 2015 Benchmarking Survey, six out of ten organizations have adopted ISO 22301 in various forms such as certification (10%), compliance (11%) and alignment (39%). Segmenting the data according to top management commitment, however, reveals interesting results: Organizations with strong top management commitment to business continuity are four times more likely to adopt ISO 22301 in some form than the ones who exhibit little or no commitment at all.\*

For those organizations that are certified against the standard, the main benefits were cited as: assurance of continued services (61%); protecting reputation and brand (48%); reduced risk of business interruption (48%); greater resilience against disruption (45%); and quicker recovery from interruption (44%).\*

Large enterprises are more than twice as likely to align with ISO 22301 compared to small and medium sized enterprises or SMEs (46% to 21%, respectively). Organizations in manufacturing (13%) report higher rates of ISO 22301 certification than the overall average (10%). Companies in Oceania (49%), the Middle East/North Africa (44%) and the United States (48%) report higher alignment rates than the survey average of 39%.\*

For organizations that have not certified their BC management system against ISO 22301, 21% report that certification may not be appropriate for their businesses. Others cite lack of top management commitment (13%), costs (12%) and perceived lack of benefits (12%).\*

It is surprising to note that the Benchmarking Survey indicates 82% of organizations do not request ISO 22301 certification from their suppliers. The study offers a reason behind this, stating that ISO 22301 is a fairly new

\*Business Continuity Institute, ISO 22301 Benchmarking Survey 2015, <http://www.bcifiles.com/ISO22301BenchmarkingReport2015.pdf>



standard and many organizations have not yet transitioned to the standard as a requirement for assurance, much less adopted it.\*

	Europe	North America	Asia	Oceania	Middle East & North Africa
Top management commitment towards ISO 22301	Strongly - 24% Fairly - 29% Slightly - 21% Not at all - 15%	Strongly - 21% Fairly - 27% Slightly - 27% Not at all - 19%	Strongly - 41% Fairly - 29% Slightly - 18% Not at all - 8%	Strongly - 18% Fairly - 39% Slightly - 18% Not at all - 18%	Strongly - 34% Fairly - 28% Slightly - 22% Not at all - 9%
Approach to ISO 22301	Compliance - 7% Certification - 10% Alignment - 36% None - 37%	Compliance - 14% Certification - 5% Alignment - 45% None - 34%	Compliance - 16% Certification - 20% Alignment - 31% None - 24%	Compliance - 15% Certification - 0% Alignment - 49% None - 36%	Compliance - 19% Certification - 3% Alignment - 44% None - 34%
Validation of ISO 22301 within organisation	67%	62%	71%	56%	82%
Seeking ISO 22301 certification from suppliers	Yes - 7% No - 85% Don't know - 7%	Yes - 7% No - 82% Don't know - 10%	Yes - 31% No - 62% Don't know - 7%	Yes - 0% No - 84% Don't know - 16%	Yes - 11% No - 81% Don't know - 7%

ISO 22301 adoption levels by region

## The business benefits of standards

A BCMS is broadly accepted as the most comprehensive approach to organizational resilience. It enables organizations to update, control and deploy effective plans, taking into account organizational contingencies and capabilities as well as business needs. Unlike the BCP, a BCMS can and should be embedded in the culture of the organization.

A standards-compliant BCMS:

- Creates effective operational business continuity plans
- Ensures all business continuity plans are fit for purpose
- Aligns plans with strategic organizational objectives
- Continually improves business continuity plans as the organization grows
- Reduces the cost of business interruption insurance policies

BC management is, at the highest level, a risk mitigation tool primarily for operational risks. In general, it's an offset to the risks created to a large extent by the lean manufacturing/JIT/single-source crowd as well as uninsurable risks like customer loyalty and reputation. None of these fit neatly on a spreadsheet so, often, not all benefits are recognized.

\* Business Continuity Institute, ISO 22301 Benchmarking Survey 2015, <http://www.bcifiles.com/ISO22301BenchmarkingReport2015.pdf>

The largest value of resilience, to any company, is protection. Specifically, protection of:

- Employees
- Clients
- Cash flow

As Bill Douglas, co-author of this paper puts it, “Resilience is strength. It can be your company’s biggest competitive advantage.” It’s important to think about and speak about resilience from a position of strength, rather than solely from a position of risk management.

C-level executives need to see value to the organization in terms of growth and revenue. The best way to show this is through the value the programs add to the organization as a whole.

Value points may include:

1. An offensive state of readiness instead of the usual reactionary posture
2. Business processes improve across the entire organization
3. Processes and procedures are well-documented, driving process improvements
4. Incident response framework is pre-emptive to avoid disaster or crisis
5. Strategies for sustaining and/or recovering critical services is implemented

When a truly resilient company is negatively impacted—whether from natural, market, competitive, financial, regulatory, or other forces—that company can capture market share, engage competitor’s clients, attract new talent, capture positive press and much more.

All of these resilience strength moves, *done in the offensive* as opposed to the defensive, increase the enterprise value of the company. Employees and shareholders alike benefit from increased enterprise valuations, regardless of the size or location of the company.

The plain truth: Resilience wins in business. Believe it, talk it, live it, and instill this mentality throughout your company.

## Determining the right standard for your organization

Now that you know more about standards, and particularly the new ISO 22301 standard, you are probably wondering whether your organization should align to a standard. If the answer is yes, you'll then want to know which is best. Other questions may include, "How do I know which standard to select?" or, "How do the various standards compare?" and, "How do I get executive support for the effort associated with implementing standards?"

These are important questions—but the answers may not be as relevant to individual business continuity programs as you would expect. The reasons why you are seeking to align to a standard can help point you in the direction of the right standard for your organization. Remember, while each of the standards include great information about what to do to develop a comprehensive BC program, they only tell you what to do—not how to do it.

### Consider your reasons for alignment

When determining which standard to align with, consider your reasons for adopting a standard. Is it your intention to simply align to a standard, or is it important that you achieve third-party certification to that standard—and why? Let's start with the easiest part of this question. If you are simply selecting a standard to help you drive your program, you will find any of the main standards to be an excellent roadmap to define and implement a business continuity program. Each of the standards, when compared at a high level, include the core components needed in a comprehensive program.

#### Internal reasons vs. external reasons

Your company may be driven to align or certify to a standard because of choices made internally or because of external requirements. Internal reasons include the knowledge that you are following established best practices, the desire to increase the confidence of stakeholders and investors, or as a way to maintain an edge over your competition.

External reasons come into play if your company is in a regulated industry that requires alignment or certification, or if a client requires it to become part of their supply chain.

## Drivers that can influence the selection of a standard

Each of the standards has its own differentiating factors that lead to the selection of one over the other. A key consideration when determining your path to standards adoption is the culture of your organization or the environment in which you must operate. What is your internal culture, and what is most important for your organization?

### Risk management and mitigation

If your organization has a strong risk management culture and focuses on mitigating risks, or strives to align to industry standards for risk management, you might find the ASIS SPC.1 standard more of a fit than either ISO 22301 or NFPA 1600. This may help to secure the support of the corporate risk management team for your BC program.

### Emergency management

The NFPA 1600 standard was initially adopted primarily by emergency managers. If emergency management is of the highest importance to your organization, this standard could be your best choice. Although the standard's development has expanded to include professionals in business continuity, the NFPA 1600 standard is a bit more comprehensive in the area of emergency management than the other standards.

If your organization currently follows the National Incident Management System (NIMS) and the incorporated Incident Command System (ICS), the terminology in the NFPA 1600 standard will be familiar and comfortable.

### ISO certification

Many organizations have already achieved various ISO certifications. The alignment and certification to ISO 22301 extends that commitment to ISO standards. Organizations with other ISO certifications will more easily adapt to the management system concepts in the ISO 22031 standard.

## Should you align or certify?

Let's review the reasons why you should follow a standard and whether or not you should align to a standard and when you should take the extra step to certify.

Why should you follow a standard? Standards:

- Observe acknowledged and recognized best practices
- Have been developed by a consensus process involving industry professionals
- Provide a common platform for program components
- Establish measurable and auditable criteria
- Outline a comprehensive program management view
- Assist with risk management
- Are an important element in supply chain risk mitigation

Aligning your business continuity program and all key processes with 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 by way of certification:

- **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.
- **Infrastructure criticality** – There are 19 sectors identified by the DHS as components of critical infrastructure for the United States. 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 organizations to require critical providers,

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.

such as your business, to demonstrate preparedness through adoption and certification to a standard.

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

## Align first, then certify

Throughout this paper, we've talked about two major initiatives as regards the use of industry standards for your internal business continuity program: alignment and certification.

### Alignment

Aligning to a standard should be considered a best practice and one that will benefit any organization, small or large. Alignment to a standard doesn't need to be segregated from your normal business continuity program activities.

Aligning to a standard, whether you ever pursue certification to that standard has great benefit and might be all that you need to do for your organization.

If you are just starting a program, the standard provides guidelines that will direct you through the initial setup of your overall program as well as each component. While the standard will provide the *what* for your activities, you may want to supplement that with other industry training and resources for the *how*. If time and resources are constrained, there are many qualified third-party consulting organizations that can help.

If you have an existing program, it is never too late to retrofit your program with the components that are needed for alignment to the standard. The first step in this process is a self-analysis of your program against the detailed components of the selected standard.

Remember, if your ultimate goal is certification, you will need to meet each and every one of the specific items in the standard.


Take care that you don't just focus on the highest level to meet the requirements; you must drill into each individual component. However, this doesn't have to happen at one time. This alignment could become a

transitional project that is accomplished over multiple years (given no driving business issue that requires an immediate alignment). You can perform a gap analysis to identify the most important areas for focus and establish a project timeline for the initiatives that you can undertake to close those gaps.

Aligning to a standard, whether you ever pursue certification to that standard has great benefit and might be all that you need to do for your organization.

### Certification

Certification to a standard is the next step after alignment. The decision to certify can be a long-term goal as you approach alignment activities, or it can be a decision that is deferred until alignment has been attained. Certification brings a more formal acknowledgement that your program meets all the criteria established in the selected standard. Certification to a standard, in itself, does not make your program any more comprehensive; however, it represents a statement to external organizations that you have aligned your program to comply with all the specifications in a standard.



Certification brings a more formal acknowledgement that your program meets all the criteria established in the selected standard.

Remember, certification will require a continued commitment to audits by third-party firms to retain your certification. Before you decide to pursue certification, make sure you have a sound business justification for the value of the certification. Certification comes with benefits as well as costs. The effort to certify to a standard is something that will likely require executive approval for the expense of a third-party audit and the necessary allocation of internal resources.

## Notes on implementing a standard

### Remember

- educate yourself
- define the scope
- manage the project
- document the process
- audit your program

Be aware that standards can represent a cultural change for your organization. You need to educate yourself and your advocates inside the organization of the value of aligning to a standard and prepare all for the work that lies ahead.

Before you begin, it's important to understand what needs to be done, the resources that will be required, the timeline for completion and the ultimate costs associated with the process.

Recognize the importance of defining your scope. The scope of your alignment must match that which is required by your customer or client, whether internal or external to your organization. Taking the time to define the scope is important so that resources are used to best advantage. Rather than align your entire enterprise, pick a key process or service and go through the alignment or certification process specifically for that process or service.

Focus on project management. Begin by developing a detailed project plan that addresses the actions steps for everything that must be done to take you through completion of an audit. Some of the tasks might seem complex, but breaking complex tasks into smaller activities will allow you to plan and execute without getting lost in the complexity.

Document your process as you go through it. To achieve alignment or certification to a standard, you must not only follow the standard with the activities you include in your business continuity program, but you must also document the processes so that auditors will be able to validate your conformance to key activities.

Remember that preparedness is a process. Like all business continuity planning and preparedness, attaining certification is merely a measurement of a program at one specific point in time. Continued certification will require constant attention to the details of your program, as well as ongoing documentation and follow-on audits to retain certification. Preparedness is a journey, not a destination.



### Implementation recommendations

If you have not begun the implementation process, here are some tips to get you started:

1. Learn about the standards. Invest in a copy of them. Read them. Study them. Take classes on how to implement them.
2. Benchmark your current program against the requirements of the standards. What's missing? In what areas can you improve your program?
3. Use the guidance documents to guide you through the process
4. Demonstrate to management how the implementation of the standard will increase the company's resilience and, therefore, the enterprise value of your organization.

In order to demonstrate to management the value of this endeavor, aim to quantify the key points and find a way to report them clearly and regularly. Ask for feedback. Compare your company against others. Transparent reporting of the metrics should validate goals of the program, and if done well, either imply or directly indicate the company's return on investment (ROI).

When reporting, divide metrics into three categories:

1. Quantification of the risks, threats and corresponding impacts
2. Validate and address these risks and impacts
3. Sustainability

The BC management system approach is more efficient than the previous, often compartmentalized approach and ties to other management systems in place within the organization. It can eliminate waste and duplication of services. It embeds BC management into the culture of the organization versus maintaining ownership with a few individuals.

A management system is a proven framework for managing and continually improving your organization's policies, procedures and processes. Business units can work with a shared vision, with information sharing, benchmarking, and teamwork.

You, the BC/DR professional, have the opportunity to guide and direct this teamwork. This can be a tremendous opportunity for personal and professional growth and visibility.

### Engage the C-suite

As the BC/DR professional, you must engage the C-level executives of your organization. This is imperative not just to the success of the resilience program you're commanding, but to your own professional career. Make a commitment to get in front of management and be taken seriously.

A significant differentiator of ISO 22301 is that it demands executive involvement. This is a good thing for all parties, and could provide a significant upward path for you. We suggest the following guidelines as you engage the C-suite:

- If your steering committee is not SVP-level or higher, lobby to get higher execs involved. You must have decision-makers and high-level sponsors in the room.
- Take a presentations class or a public speaking class. Organizations such as Dale Carnegie put on concise, valuable seminars to improve these skills. You must feel confident in expressing your views, engaging in conversation that may at times be in disagreement, and do so with confidence and authority. Executives respect concise clarity; they do not want to be buried with detailed, data-ridden slide decks.
- Be strategic with how you engage with your steering committee. Have a standing deck of no more than a dozen slides with the key topics and metrics. Focus on clarity and repetition. Brevity is better.
- Take the opportunity to tie any of the BC management data or the progress of your resilience program to the company's goals. If you can make a case for improving revenues, lowering costs, or measuring return on investment (ROI), do so with confidence.
- Start and end your meetings promptly. Publish and circulate an agenda at least a day prior to the meeting.
- If someone in the room is heading for the weeds (getting off topic or agenda) or shifting attention to irrelevant topics, calmly suggest a separate time to meet with them one-on-one to review the topic and discuss their question fully.
- Don't be offended by questions. Simply answer and move on. If you don't know the answer, say so, then promise and deliver the answer by a specific day or time. Questions are a learning opportunity for everyone in the room.

You will earn the respect of the C-suite over time. Execution is required for the program’s success, and elocution of that success equates to your personal success.

## Eight steps to certification

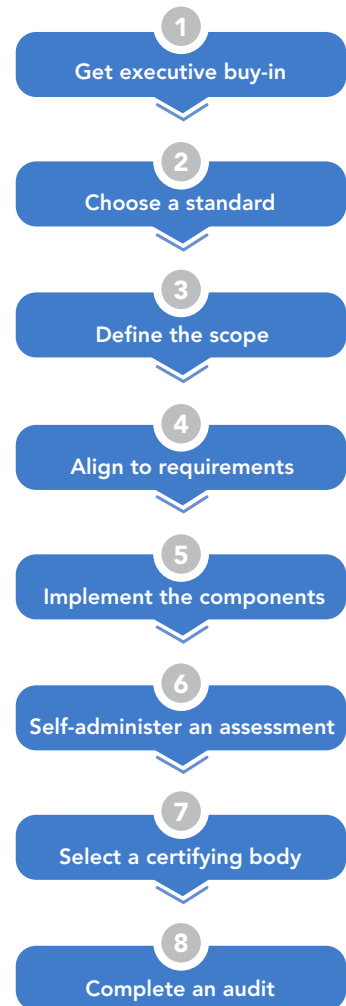
If your company wants to certify to a standard, it must have a third-party review by an authorized certification board to validate the company’s preparedness to a standard. However, in some cases a self-declaration of conformity can meet your company’s goal. Regardless of the decision to move for formal 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. Once you are equipped with a full understanding of the process, you must clearly articulate a value proposition for the executive team that will authorize the initiative. Trying to define a fiscal return on investment is always challenging, but certification might be something that can be used to position your organization with a competitive advantage in securing new business or retaining a key customer. In some instances, using preparedness as a brand attribute can help position your company for expansion in key business sales.

### Step 2: Choose a standard

Once you have buy-in, your next step is selecting a standard that will be used in developing an internal business continuity program. Use the information in this paper to help you determine which standard is the best fit for your organization before you begin.



### Step 3: Define the scope

As stated earlier, it's not necessary to certify your enterprise-wide program, or all of a single location at one time. 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 regulatory requirements

Many of the current processes that are in place to meet regulatory requirements can 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 the components within your 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. Note that the certification process is a pass/fail system, requiring 100% conformity to the standard within your scope.

### Step 6: Self-administer an assessment of conformity

Once all the components of the standard have been implemented (or as the process is being implemented), 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 way 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. Self-auditing will allow you to demonstrate progress and keep the management team committed to the process.

### 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 should be one that has experience within the business sector in which your company operates, particularly if in regulated environments. An auditor with experience in your specific industry will be able to apply that knowledge towards the understanding of how your program has been created.

Once you have selected the auditing firm, your responsibility is to actively manage the entire audit process, scheduling resources and providing access to documentation that the audit team requires. By establishing a strong relationship with the auditors, you can explain your program as questions arise and help the auditors understand how you have conformed to the specifications of the standard.

### Step 8: Complete an audit by the certifying body

The hard work is done; now it's up to the certifying body to complete the audit and validate that the specifications of the standard have been addressed completely. As you near completion of your program readiness, including the preparation of all the documentation needed for compliance to the standard, it's a good idea to get a second-party pre-audit before you request a formal third-party auditor compliance review. The second party is typically a consultant who understands the standard you have selected as well as the audit process you will be going through for the third-party audit. This external review, prior to the official audit, will allow you to identify any gaps that the auditors might identify, remediate those gaps and thus give you a level of confidence that you are fully prepared for the certification audit process.

## The impact of ISO 22301 on your program

The biggest organizational impact of ISO 22301 is the increased visibility and interaction with senior management. One of the major benefits of an ISO-based system is better governance, and with that comes regular steering committee updates.

Many internal business continuity professionals will need to rethink the metrics they report and, more importantly, get comfortable discussing them with senior business leaders on a regular basis; we've discussed ways to do that in this paper.

ISO22301 can help BC professionals communicate better with the entire organization, particularly with management, and provide a better sense of uniformity across the company.

Conforming to ISO 22301 allows BC pros and upper management to better compare their programs to others and measure effectiveness.

## Summary

When you first explore the complicated world of business continuity standards, it can appear to be an alphabet soup of letters and numbers, with little to differentiate each one. All of the standards are respected, but one may be better for your particular organization than another; by now you should know which standard makes the most sense for your business.

We've talked a lot about selecting and certifying to a standard. The overarching theme is commitment to preparedness for your organization, aligned to defined industry best practices for business continuity—demonstrated to your stakeholders, board of directors, executives, employees, customers, clients, external regulators and supply chain.

---

### LEARN MORE ABOUT THE STANDARDS

- ISO 22301 – (purchase)  
[http://www.iso.org/iso/catalogue\\_detail?csnumber=50038](http://www.iso.org/iso/catalogue_detail?csnumber=50038)
- ASIS – (free)  
<https://www.asisonline.org/Standards-Guidelines/Pages/default.aspx>
- NFPA – (free)  
[www.nfpa.org/aboutthecodes](http://www.nfpa.org/aboutthecodes)

### OTHER REFERENCES

- The Sloan Report – Framework for Voluntary Preparedness (includes crosswalk of standards)  
<http://www.sloan.org/fileadmin/media/files/olsiewski/frameworkforvoluntarypreparednessfinalreport.pdf>
- ANSI ANAB  
<http://anab.org/>
- For organizations that have been identified as third-party certifying bodies for alignment to the DHS PS-Prep Program:  
<http://anabdirectory.remoteauditor.com/>

### Contributors to this paper include:

**Ann Pickren**, OnSolve president, MBCI, and business continuity expert

**Bill Douglas**, *ResilienceGuy.com*, strategic growth and strength advisor

### About MIR3

OnSolve is the market leader in real-time, mass notification and collaboration solutions used by the world's largest organizations. The OnSolve suite of critical communication tools is a key component of effective business continuity, emergency response, IT alerting, and security programs around the globe. Visit us on the Web at [www.onsolve.com](http://www.onsolve.com).

ASIS  
PC.1

N

NIFPA

OnSolve  
866 939 0911  
onsolve.com

16000

BS