STRATEGIC BCP®

The BCM Professional's Playbook:

Evaluating and Applying Relevant BCM Standards

When it comes to business continuity (BC), identifying and applying the right standards for your specific needs is definitely not a "one size fits all" solution.

In fact, the answer is typically not a single standard, but a combination of industry regulations, broader BC guidelines, and best practices that collectively satisfy the particular concerns of your industry or application. *(For brevity, we refer to all of those resources under the general term of "standards.")*

The process of evaluating, mapping, and synthesizing standards into a universal framework was initially demonstrated in the form of the original BCP Genome™, prepared by Strategic® BCP in 2006 and updated multiple times since then.

While the original BCP Genome specifically benefits users of Strategic BCP's ResilienceONE® business continuity management (BCM) software, you can follow the same logic described here to create your own framework of references relative to your unique business continuity needs.

Harness the thought process behind the BCP Genome.

Unlike individual standards focused on specific industries, policies, or procedures *(e.g. setting up a planning structure vs. developing specific plans)*, the BCP Genome concept unifies a broad spectrum of relevant BC practices across eight major categories.

The goal of the BCP Genome was to develop a "gold standard" framework based on the collective thought leadership available to BC professionals. It did not set out to interpret standards, but rather to synthesize the best available BC attributes into a common database.

If you follow the same process for your own purposes, you will soon realize the strengths—and gaps—in various standards. Identifying those attributes will help you hone in on the best reference sources for your needs instead of trusting your plans to one less-than-comprehensive standard.

Game-plan checklist:

- ☑ Embrace guidelines that satisfy your unique needs, regardless of industry popularity.
- ☑ Be sure your framework addresses both structure *(organization, management, training, maintenance)* and substance *(Business Impact Analysis [BIA], emergency response/crisis management, business/IT disaster recovery, etc.)*.

Recognize the unique perspective behind each standard.

The primary differences between "regulations" and "standards" are the consequences of non-compliance. While failure to adhere to a voluntary industry standard might raise a red flag to a prospective customer, failure to meet a mandatory compliance requirement can result in costly sanctions.

Industry regulations are but one factor to consider in your evaluation. Incorporate various industry-accepted guidelines and best practices that offer valuable guidance as well—such as the Business Continuity Institute (BCI) Good Practice Guidelines and Disaster Recovery Institute International (DRII) Professional Practices.

You will soon appreciate *(as the chart below demonstrates)* that no single standard covers all business continuity categories equally.

For example, ISO 22301 puts an extensive focus on program organization, management, training, audit, and maintenance, but relatively little on emergency facilities or business and IT recovery. Even the most comprehensive standard (FFIEC) only covers three-quarters of the BCP Genome's 101 unique points. That comparison demonstrates why it is so important not to put all your eggs into one basket by focusing on the industry's current "hot" standard, which can easily change from year to year.

Game-plan checklist:

- ☑ Pinpoint the mandatory regulations for your industry.
- ☑ Research additional voluntary industry guidelines compatible with your needs.
- ☑ Incorporate other best practices that cover issues specific to your application demands.

FFIEC	NFPA 1600	NIST	FERC	GTAG	ISO 22301	HIPAA	TOTAL
1. PROGRAM ORGANIZATION, MANAGEMENT & TRAINING							
8	12	7	3	5	10	0	12
2. BUSINESS IMPACT ANALYSIS (BIA)							
6	4	8	4	8	7	3	9
3. EMERGENCY RESPONSE & CRISIS MANAGEMENT							
18	26	19	19	16	16	1	31
4. EMERGENCY FACILITIES							
12	6	3	1	5	1	0	12
5. BUSINESS & IT RECOVERY							
14	7	8	4	8	5	3	16
6. TESTING							
13	14	13	1	10	8	1	14
7. MAINTENANCE							
3	0	3	1	2	4	1	4
8. AUDIT & GENERAL POLICY							
2	0	2	0	1	3	0	3
TOTAL							
76	**69**	**63**	**33**	**55**	**54**	**9**	**101**

The seven examples shown above demonstrate differences in focus among various standards. In all, the BCP Genome synthesizes a total of 15 standards into 101 unique points of coverage, across eight major categories of business continuity practice.

Don't underestimate the effort.

As with anything of value, the process of creating your own "gold standard" framework for BC practices takes time and effort. For example, the original BCP Genome focusing on nine key industry standards took more than a thousand hours to identify common aspects of business continuity across a variety of industry standards.

One encouraging aspect of the process, though, is that the more you do, the better you will be able to spot the repetition that occurs across multiple standards. For example, the first four standards mapped in the initial version of the BCP Genome accounted for 95% of the key points derived from the next five standards combined. The six additional standards mapped to the BCP Genome since then have resulted in small language adjustments, but have not added any new points to the initial 101 key points of the framework.

Don't be overwhelmed by the initial scope of the process. Keep your primary focus on the most relevant standards, with an eye toward the known needs and vulnerabilities of your organizational environment, and then expand it as necessary.

Game-plan checklist:

- ☑ Identify known areas of compliance concern within your current BC planning process or organization, and incorporate appropriate points in your framework from the most relevant industry standards.
- ☑ Incorporate additional standards or guidelines, as needed, to complement and refine your initial framework.
- ☑ Don't become discouraged. You will be able to reap the benefits of your efforts for years to come.

Don't overlook the value, either.

While some BC professionals battle a perception of low value for their function within the organization, nothing gets top management's attention like documenting real threats to profitability and plans to mitigate that exposure. Having a clear, documented explanation of what non-compliance can cost is one way to focus executive attention.

Build your framework with an eye toward justifying specific BC processes, and the cost implications of failing to implement them. Keep track of potential negative impacts—as well as potential cost-savings—as that framework evolves, to make it harder for executives unfamiliar with BC processes to overlook their value.

In certain industries, such as the financial sector, potential gaps in compliance highlighted by a thorough BC-framework evaluation can save more than just money. Having appropriate business continuity and disaster recovery plans could help avoid NFA-imposed fines that could run into tens of thousands of dollars. On the other hand, passing an FFIEC audit to avert a Memorandum of Understanding can prevent far more embarrassing consequences.

Game-plan checklist:

- ☑ Use your framework to document any potential exposure to penalties for non-compliance.
- ☑ Look for before-and-after cost justifications for any efficiency improvements in BC processes or outcomes.
- ☑ Document examples of how improving BC practices can enhance value in terms of better Business Impact Analysis, risk assessment, and risk management.

Learn from the experience of others.

There are multiple ways for you to take advantage of the thought, effort, and documented framework resulting from the original BCP Genome effort.

One way is to use the process outlined in this document as a guideline for developing your own framework, particularly if you need to satisfy the requirements of multiple industry standards.

A second, easier way is to evaluate the credibility and compliance of your existing BC planning and management processes through a paid BCP Genome Assessment. In that case, a Strategic BCP professional will review your plans against the latest BCP Genome and identify those standards with which you comply, as well as those aspects of important or mandatory compliance standards that your plans fail to address.

The third, easiest, and most comprehensive way to ensure the advantages of the BCP Genome is to use ResilienceONE BCM software—the only BCM software that incorporates it as a means of documenting your ability to satisfy ALL major compliance requirements.

Game-plan checklist:

- ☑ Whichever route you choose, you can learn more by participating in periodic seminars and Webinars presented by the developers of the original BCP Genome.
- ☑ If you do not have the time, manpower, or expertise to develop your own framework, contact Strategic BCP to evaluate your best options for ensuring compliance with ALL major BC regulations and standards.

See the BCP Genome in action.

To arrange for a BCP Genome Assessment of your existing BC plans, in order to evaluate full compliance with standards applicable to your organization, write to: contact@strategicbcp.com.

To see how the BCP Genome documents BCM software compliance with ALL mandatory regulations and voluntary standards within your industry, visit www.strategicbcp.com to schedule a Live Demo of the BCP Genome concept within ResilienceONE BCM software.

Since 2004, Strategic BCP®—innovator of ResilienceONE® BCM software—has been leading the way in elevating the productivity and relevance of business continuity professionals. For a closer look at better ways to assess and manage risk, continuity, disaster recovery, and compliance, all in one comprehensive program, contact us:

Toll-free: 866.594.SBCP (7227)
E-mail: solutions@strategicbcp.com
Website: www.strategicbcp.com