SearchCompliance.com

Understanding BC, resilience standards and how to comply

By Paul Kirvan

COVID-19 is casting a new light on standards and regulations governing business continuity, or BC, and resilience.

The past decade has seen a marked increase in the number of BC guidelines. Companies have responded to these new rules by establishing additional compliance benchmarks and by selecting employees to become professionally accredited as BC auditors.

In the wake of COVID-19, complying with BC and resilience standards has become even more important.

Achieving compliance is essentially a two-step process: First, companies must identify which BC and resilience standards or regulations are most relevant. Second, they must launch a program that demonstrates how compliance is achieved.

Relevant standards and regulations

Table 1 lists some of the most relevant ISO standards. Applicable regulations will depend on individual companies and the industries they serve. Banking and financial sectors, for example, have both federal and state regulations that address BC and resilience issues. These organizations can decide to achieve compliance with those particular benchmarks in lieu of the global standards. The key objective is to achieve and demonstrate compliance with one or more relevant standards and regulations.

Table 2 is a partial listing of U.S. standards, regulations and good practices developed by a number of organizations, among them ASIS International, National Fire Protection Association, Federal Financial Institutions Examination Council, ISACA, Financial Industry Regulatory Authority, Federal Emergency Management Agency and NIST. *Disaster Recovery Journal* continually updates its generally accepted practices for BC, and the NIST Special Publication 800 series of standards is a good source for guidance about IT.

Steps for achieving compliance with BC and resilience standards

The following steps illustrate how companies can achieve and demonstrate compliance. The key word here is *demonstrate*. Confirming compliance can be accomplished through documents that indicate how the organization satisfies the requirements set forth by a specific standard. Most standards are organized into chapters, sections, subsections and other outline formats. Companies can simplify the process by selecting a specific section and then describing how compliance has been achieved.

1. **Obtain management's approval** to begin the process of standards compliance, and explain how compliance will benefit the organization.
2. **Establish a team** that includes representatives of several relevant departments, such as BC/resilience, risk management, IT, administration, finance, internal audit and HR.
3. **Research relevant standards, regulations and good practice documents**, and decide which documents are most relevant to the organization. Obtain current versions of those documents.
4. **Brief team members** on the selected standard(s) so they have a basic understanding of the requirements. If possible, invest additional time with internal audit, as it may, in fact, be the unit that eventually assesses and certifies that compliance has been achieved.
5. **Consider contracting outside professionals** if internal audit is not able to participate in compliance activities. Look for providers who have been certified as auditors for specific BC/resilience standards,

such as ISO 22301:2019. Two organizations that provide such accreditations are Disaster Recovery Institute International and International Consortium for Organizational Resilience. Alternatively, check BC consulting firms to see if they have employees who are certified as standards auditors.

6. **Map the selected standard(s)** to existing BC/resilience programs, and identify where programs are noncompliant.
7. **Develop a plan** to update the BC/resilience program to resolve noncompliance issues, and execute the plan.
8. **Arrange for an internal audit** or an experienced third party to assess the revised BC/resilience program, and validate that issues of noncompliance have been resolved. Brief senior management on the results of that assessment, and ask if they want to have a formal compliance audit.
9. **Arrange for a formal audit** if senior management requires one. Results of that audit will formally document compliance with the relevant standard(s) and regulation(s).

Once the organization is believed to have met its goals, perform periodic assessments and/or audits to ensure compliance is maintained.

02 Oct 2020