

Standards and Regulatory

International Enterprise Risk Management Standards

ISO 22301

ISO 22301 is the latest (2012) international standard for Business Continuity Management (BCM) developed to help organizations plan to minimize the risk and impacts of disruptions to their business and operations. It is also known as the standard for Business Continuity Management Systems. ISO 22301 specifies requirements to plan, operate, monitor, review, and maintain a documented management system to prepare for, respond to and recover from disruptive events when they arise. Organizations can become certified and will therefore be able to prove its compliance to its customers, partners, owners, and other stakeholders.

BS25999

The British Standards Institute (BSI) launched the BS25999 Standard in 2006/2007 as a two-part business continuity management standard to replace its predecessor "PAS56" (Publicly Available Standard) published in 2003. Part 1 provides guidance and recommendations by outlining an understanding of the development and implementation of business continuity management within an organization. Part 2 complements Part 1 by providing more specific details of the requirements for "establishing, implementing, operating, monitoring, reviewing, exercising, maintaining and improving" the existing BCM system (BSIamerica.com). Although only officially recognized in the United Kingdom, the BS25999 standard has been adopted and implemented worldwide.

ISO/IEC 31010

The International Organization for Standardization, commonly known as "ISO" and the International Electro Technical Commission expanded upon the previously published ISO 31000:2009 by publishing the ISO/IEC 31010 as a standard for risk assessment practices. The standard addresses risk assessment ideas and procedures to help a business identify potential risks as well as their probabilities, consequences and potential solutions. ISO/IEC 31010 is a generic standard and therefore is not specific to any one industry.

Business Continuity Standards for Financial Institutions

FFIEC

The Federal Financial Institutions Examination Council is responsible for creating the set of standards to which financial institutions are held accountable, and for developing the reporting systems to be used in practice. It's periodically updated "Business Continuity Planning IT Examination Handbook" promotes the importance of business continuity planning in the financial services industry. As the financial system is central to the overall economy, its resiliency is necessary in order to maintain public confidence.

FINRA

FINRA is a private, self-regulatory organization that performs financial regulation of the United States securities industry. By overseeing all brokerage activities, FINRA aims to protect investors and maintain market integrity. In this way, it is the successor of the National Association of Securities Dealers (NASD). FINRA also prides itself on the FINRA Investor Education Foundation which promotes investor education to underserved groups.

Business Continuity Standards for Energy

FERC COOP

The Federal Energy Regulatory Commission is an independent agency that oversees the use of oil, electricity, and natural gas in the United States. It established its Continuity of Operations Plan (COOP) to be set in place in the event of a crisis such that FERC's mission essential functions may still be carried out without interruption. These regulatory requirements are applicable to all companies in the energy industry.

Business Continuity Standards for Government

FCD (Federal Continuity Directive)

The Department of Homeland Security proposed the idea of the Federal Continuity Directive (FCD) in order to maintain governmental continuity. FCD 1 has its primary objective in improving the resiliency of National Essential Functions in the time of a crisis. It provides the Federal Executive Branch with the framework necessary for developing continuity plans. FCD 2 offers the guidance and direction for governmental departments and agencies to identify and analyze their Mission Essential Functions and any relationships that exist among them such that the continuity plans can be put in place.

Business Continuity Standards for Health

HIPAA

The 1996 Health Insurance Portability and Accountability Act protects American workers and their families by granting the right to preserve and transfer health insurance coverage in the event of a job change or loss. It also orders a set of national standards for the healthcare industry which includes confidentiality regulations, billing principles and guidelines for electronic health care transactions.

US Private Sector Business Continuity Standards

NFPA 1600

NFPA 1600 is a national standard published in 1995 and observed on the local as well as global scale by both public and private nongovernmental entities. NFPA published its 2004 edition after the National

Commission on Terrorist Attacks upon the United States (the 9/11 Commission) endorsed the adoption of its NFPA 1600 as the nation's standard for private-sector preparedness in a post 9/11 world. The most updated edition was published in 2010.