

What is Organizational Certification?

By Brian Zawada (MBCP – Avalution Consulting)

As Published in the 2008 Summer Issue of the Disaster Recovery Journal

There has been a great deal of difficulty in determining the effectiveness and quality of an organization's business continuity process and where to turn for the best guidance regarding how to build an effective program. This has particularly been an issue in multiple industries where there has been no single form of consensus. Whether your background is focused on business continuity, security, information technology, communications, risk management or any other competency, you most likely feel besieged by an overabundance of recommendations, guidelines and general thoughts regarding how to plan for continuity of operations. Add to that the different needs of manufacturing, banking, service, retail and hospitality organizations (to name a few), and the path forward becomes quite complicated.

But what could be a promising new development took place beginning in 2007 – the introduction of organizational business continuity certification. External validation of a business continuity process could offer credibility to executive management, shareholders and customers – as well as much needed focus and visibility.

Although business continuity certification is new, some businesses are already familiar with certifications for a wide variety of disciplines, including quality, security and safety processes. These efforts all evolved over time and have been accepted by industry because they provide business value.

This article explores two emerging business continuity certifications – British Standard (BS) 25999 and the Title IX voluntary preparedness certification process. Perhaps even more important, it is the author's intent to make the case for using certification processes and standards (any standard that makes business sense, such as National Fire Protection Association Standard 1600 and Disaster Recovery Institute International's Ten Professional Practices) to "do something" and advance business continuity readiness – even if certification isn't right for your organization today.

What is BS 25999?

Authored by the British Standard Institution, BS 25999 replaces PAS 56 as an "umbrella" standard providing a basis for understanding, developing and implementing business continuity within an organization, to integrate risk management disciplines and processes with business continuity, and to provide confidence in business-to-business and business-to-customer dealings. BS 25999 is written in two parts. Part 1, the Code of Practice (published November 2006), outlines the standard's overall objectives, guidance and recommendations. Part 2, the Specification (published November 2007), details the activities that should be completed in order to meet business continuity objectives within the context of an organization's view of business risk. Part 2 is also designed to be "auditable", meaning only objective, measurable concepts are included in the Specification.

A first of its kind in the business continuity industry due to the all-encompassing nature of the standard and the accompanying certification effort, BS 25999 compliance certification is demonstrated by independent assessment against BS 25999-2 (the Specification). Like all other certifiable international standards, BS 25999 certification requires a thorough

assessment process to ensure the organization has properly documented and addressed all the elements of the standard and that the Business Continuity Management System (BCMS) is operating effectively and consistently.

What is Title IX?

The 9/11 Commission recommendations evolved into Public Law 110-53, which provides for a voluntary preparedness standard and certification process for private sector organizations. This legislation was passed in the House (371-40), in the Senate (85-8), and signed into law by President Bush on August 3, 2007. Title IX, a section of Public Law 110-53, refers to the "voluntary" private sector preparedness certification and accreditation program. Title IX's goals included the following:

- Consultation with the private sector
- Develop guidance or recommendations
- Identify best practices
- Use voluntary consensus standards
- Develop and promote a program to certify the preparedness of private sector entities that voluntarily choose to seek certification
- Manage and implement accreditation and certification programs
- Demonstrate ability to certify private sector entities
- Provide business justification for preparedness and adoption of voluntary preparedness standards

A great deal of caution is being exercised by authorities to develop/select a standard(s) and an associated certification process capturing the right recommendations that truly benefits U.S. business and in turn, their customers, employees, investors and all Americans. It is the author's contention that the Title IX process should be developed with maturity model concepts so that organizations can not only benchmark themselves internally and externally, but also develop a plan ensuring continuous improvement is being made.

In order to provide private sector recommendations to the Department of Homeland Security, the Sloan Foundation convened a cross functional group of fifteen subject matter experts on October 23, 2007. Participant backgrounds included business continuity, security, crisis management, emergency management and risk management. The National Fire Protection Association (NFPA), the Disaster Recovery Institute International (DRII), the American Society for Industrial Security (ASIS) and the Risk and Insurance Management Society (RIMS) also reviewed and provided input.

The Sloan Foundation supports a decision being made on this effort which will move the U.S. toward voluntary certification – fully realizing the importance of providing assistance to small and medium size organizations, which may or may not have the same resources to implement all of the necessary components of full compliance.

Most recently, a Committee of Experts was also convened by the American National Standards Institute's (ANSI) American Society for Quality (ASQ) National Accreditation Board (ANAB) to assist in offering accreditation activity recommendations. Their recommendations include defining requirement criteria for the certification bodies, the audit teams, oversight assessors and an application process to be accredited by ANAB.

NFPA 1600 and DRII

Beyond the two certification offerings outlined thus far in this article, many other standards exist that are available for consultation and may be used to self-assess compliance. Some are industry-specific, others industry independent. Even industry-specific standards and requirements are often useful since many of the tenets contained can apply to others. The following table lists a number of standards and regulatory requirements for consideration – some specific to business continuity or its related sub-disciplines, others that are more broadly associated with risk management. Following this table, two key efforts are described further, NFPA 1600 and DRII's Professional Practices.

Industry-Specific Standards	Industry-Independent Standards
<ul style="list-style-type: none">• FFIEC Business Continuity Handbook (recently updated)• HIPAA Security Requirements• U.S. Federal Continuity Directive• BASEL II (Operational Risk Management)• NYSE Rule 446• AUS/NZ Standard 221• Singapore TR 19• COBIT• ITIL Service Continuity Management	<ul style="list-style-type: none">• NFPA 1600• DRII 10 Professional Practices• ISO PAS 22399• ISO 24762• ISO 27001• AUS/NZ Standard 4360• COSO ERM Framework

NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs is a consensus standard, which had its origin in 1991 and as such, has matured and evolved over the past seventeen years. Many improvements have come about and it is already recognized as a leading standard by DHS, FEMA and the 9/11 Commission. Since it was originally published in the United States, a number of international versions were issued.

NFPA 1600 advocates that organizations take an "all hazards approach" to prepare for any incident, including human, natural or technological events. NFPA 1600 also advocates a team-based approach to response, restoration and recovery preparation with strong senior management support and involvement.

The DRII Ten Professional Practices (applicable to international entities and business continuity professionals) were designed to establish necessary skills and competencies for individuals focused on business continuity. However, a number of organizations translated these people-focused requirements into organizational business continuity program characteristics. DRII's Ten Professional Practices focus on life-cycle oriented processes designed to establish requirements, define strategies, document plans, exercise strategies and advance awareness amongst all stakeholders. Additionally, DRII content also provides guidance on process development, governance, compliance and continuous improvement.

Comparing BS 25999 and Title IX

Although premature to compare BS 25999 to Title IX (given the latter continues to take shape) the following table seeks to clarify key points as executive management, risk managers and business continuity professionals evaluate both initiatives.

	BS 25999	Title IX
Intent	Create value by assessing compliance with a generally-accepted standard that defines methods to increase business continuity readiness – inclusive of risk mitigation / treatment	Create value by assessing compliance with a generally-accepted standard that defines methods to increase business continuity readiness – inclusive of risk mitigation / treatment
Scope	International entities – public and private sectors	U.S. private sector
Approach	BSI Management Systems, consistent with ISO 17021 guidelines	To be defined
The Underlying Standard(s)	BS 25999-2, with the caveat that BS 25999 notes that other standards and regulations may be a fit and/or may be required by the business	To be determined, NFPA 1600 mentioned in legislation (and other standards may also be included in this initiative)
Availability	Organizational certification available as of November 2007	To be determined

This table demonstrates that both add value to business continuity visibility and readiness, even though a number of unknowns remain specific to Title IX. But are they in competition? A section dedicated to comparing BS 25999 and Title IX must conclude with the point that these two initiatives – although appearing similar – are not competing with one another. Both offer (or will offer) similar value propositions and emphasize continuous improvement toward higher levels of readiness.

Lastly, since this article not only touches on certification but also the use of other standards and regulatory requirements, it's important to note that BS 25999 references the need to leverage the entire body of standards and requirements to define a program that fits the organization's unique needs. It is expected that Title IX will do the same, recognizing standards such as NFPA 1600 as a baseline to follow for effective business continuity strategies.

Certification Offers Business Value!

Beyond a comparison between BS 25999 and Title IX, both efforts intrinsically offer business value to organizations electing to pursue organizational certification. As pointed out earlier, business continuity remains a fragmented discipline, with programs implemented based on numerous standards containing varying degrees of depth and rigor. Certification to an accepted standard provides an objective measure of an organization's program. Certification may add value to your organization in the following five ways:

1. Business continuity capability and performance provides competitive differentiation. With that said, it is traditionally difficult to make a solid comparison between organizations. However, certification can provide a straightforward means of comparison for potential customers. For existing customers, certification can provide a degree of assurance, which is critically important if your organization is operating as a single or sole source provider of a critical product or service and your customers have expressed concern and are evaluating secondary sources.
2. Related to competitive differentiation, certification will provide a convenient and time-saving answer to frequent business continuity program surveys and inquiries from customers, as well as regulators, investors and insurance carriers. With the existence of a third-party registered certification, there is no longer a need to share proprietary planning information to satisfy continuity inquires and concerns. As well, certification may begin to offer direct cost-savings opportunities on a recurring basis. Industry associations are in the process of debating the direct benefits of "viable" business continuity programs on credit ratings and business interruption insurance premiums.
3. The organizational certification process also introduces discipline, holding the organization accountable to consistent focus and participation in a life-cycle oriented business continuity management system. With employee turnover always a concern, organizational certification (and the inherent requirements that mandate system documentation, accountability, repeatability, continual improvement and evidence) will enable an effective knowledge transfer process.
4. Also from an internal perspective, developing a business continuity program in accordance with a standard provides the program owner with the ability to easily and confidently answer management questions regarding the state of the program. Questions such as "What's everyone else doing?" or "Are we doing everything we should be?" can be clearly quantified and answered through reference to the standard. Program weaknesses and non-conformities will be highlighted during initial and continuing certification audits, which can then be built upon to show progress. As well, for organizations with decentralized business continuity efforts, audits will encourage compliance, ensure conformity across the organization and act as a catalyst for continuous improvement.
5. Some standards, in particular BS 25999 and NFPA 1600, provide guidance specific to planning strategies, operational risk management methodologies and risk treatment concepts that offer program optimization opportunities. These structures can assist organizations working to integrate business continuity into a larger enterprise risk management framework or those struggling to align many disjointed

elements of a business continuity management system. This value alone – whether the organization is interested in certification or not – demands that organization's utilize a structure that shares terminology and processes across a multitude of risk management disciplines.

Conclusions

Each organization must consider whether choosing organizational certification – through BS 25999 or via the Title IX initiative – is of benefit to them. Incentives to comply, although not formalized as of yet, are promising.

However, even if organizational certification isn't for your organization now (or ever), develop an understanding of the many standards available – including NFPA 1600 and DRII's Professional Practices. Find one or more that works for your organization – build and/or mature your program based on one or more of the standards that aligns best with your business.

Overall, organizational certification is new, with its potential benefits continuing to come into focus. The recommendations are rather simple:

- Stay informed and evaluate the business benefit of organizational certification
- Select one or more standards that contribute to the maturation of your organization's business continuity program and continuously measure your compliance with standards as a catalyst for continuous improvement
- Above all else, do something – don't get frustrated with the growing body of standards and the growing number of professional associations getting involved

Harness the unique perspectives offered by each business continuity standard (and the authoring entities) to enable your organization to increase response and recovery readiness. Focus on the business value of your business continuity program and meeting the needs of your customers.

Brian Zawada, MBCP, co-founder and director of consulting services for Avalution, focuses exclusively on business continuity management solution design and development. In addition to having served as both a consultant and an internal business continuity professional, Zawada is a frequent author and speaker.