The ABA's Path to Business Continuity Certification

George Huff & Diana Gilbert

A Business Case

American Bar Association

2/9/2013

This Business Case is authored by George Huff, a Member of the Special Committee on Disaster Response and Preparedness, American Bar Association, and Diana Gilbert, Director of Administrative Services, American Bar Association. It offers a chronological narrative, beginning in 2010 with assessment of ABA's Business Interruption and Recovery Plan, continuing with in-house surveys, disaster recovery systems tests, and tabletop exercises, performing gap analyses and aligning the plan using BS 25999-2, the requirements specification, which provided the detailed elements and auditable criteria. Appreciating our gaps enabled us to create a strategy and develop a schedule for implementation which we presented to the Business Continuity Planning Task Force. Then, top management's approval was straightforward.

The ABA's Path to Business Continuity Certification

Our path to certification to a business continuity standard began in mid-June 2010 when the U.S. Department of Homeland Security announced its adoption of three industry standards for the voluntary private sector preparedness and accreditation program, known as "**PS-Prep™**," which the Congress authorized in "**Implementing the Recommendations of the 9/11 Commission Act of 2007**." The Act implemented some of the recommendations of **The 9/11 Commission Report** (2004), including the recommendation for a **standard for private-sector preparedness**. The **ABA's Special Committee on Disaster Response and Preparedness** had closely following that legislation and favored the ABA's early adoption of one of the new standards. Along our path to certification, the Special Committee monitored each phase of the business continuity management system (BCMS) lifecycle – deciding, preparing, auditing and improving - and is able to describe the benefits of a business continuity standard, alignment and certification.

What Did the ABA Learn about Management Systems & How Did Our Governance Change as a Result?

Implementing a management system - not just a BCMS - which conforms to an industry standard involves identifying the scope, documenting operating procedures, training, internal auditing and corrective procedures, and requires that implementing procedures exist to improve existing procedures. It can prove to be a time and resource intensive effort that will result in questions, concerns and skepticism from stakeholders throughout an organization. On the other hand, it can significantly improve management practices and production of products and services which translate into increased sales and employment that are magnified if members, customers or clients interpret adoption of the standard as a signal of higher quality products and services.

Similar to any initiative with an organization-wide impact, certification requires management commitment and support, a strong business case, personnel time, and financial resources in order to achieve success and deliver long-term value. At the ABA, external volunteers and existing ABA staff helped create BCM roles and responsibilities within the ABA. We learned it's important to research up front whether certification makes

business sense for our organization, and would be successful within our organization. We learned that implications of the standard's elements reach beyond the organization. As an example, right-sizing an organization's business interruption insurance coverage or securing premium discounts may offset investment and benefit your bottom-line.

Why Did the ABA Pursue Business Continuity Certification?

The ABA is a national advocate of emergency preparedness and response. **See: How Did the Special Committee's Advocacy Move the ABA to Business Continuity Certification?** More recently, as we began looking at organizational certification, we saw the importance of understanding what we hoped to gain as an association, and how we would accurately assess the cost. The gain in our business case involved four benefits:

1. Certification would provide assurance to our members that the ABA has a verified system which minimizes business risk and enhances resilience that enables us to survive any disruptive event;

2. A BCMS in place and verified would ensure the steady supply of products and services to our members and valued customers;

3. The ABA would become an early adopter of the PS-Prep^{TM} Program which would enhance our brand image worldwide; in fact, the ABA became only the second corporation and the first association in the United States to obtain both BS-25999-2 and PS-Prep^{TM} Program certification; and

4. Certification would provide a competitive advantage, establishing the ABA as a model for law associations, lawyers, law firms and other business organizations by cost-effectively selecting a BCM standard, gaining alignment and achieving certification.

As these benefits became clear, we compared them to the cost of certification. In our case, we had two professionals, a Special Committee Member volunteer certified in BCMS and an ABA Director experienced in administration, that were able to operate an internal BCMS. Our costs were as follows:

• Approximately 520 hours of internal staff time to formalize our continuity program, conducting 2010 and 2011 activities in line with requirements, and preparing for certification in 2012;

• For $2,862, we licensed use of BS 25999-2 self-assessment software for 4 ABA staff who were responsible for the business impact analyses of products and services and, for $2,380, we hired an American National Standards Institute (ANSI) certified instructor to train the ABA's internal auditors on the standard; and

• Approximately $20,000 in fees over three years to engage a certifying body. The ABA received responsible/responsive bids from two certification bodies, Orion Registrar and NQA-USA.

Every organization's business case for certification is different, and the ABA's reflects the realities of a large professional association. The ABA operates multiple business lines and offers a wide variety of products and services. Your association, law firm or organization's business case should reflect the realities of your business and provide information for your senior leadership team to determine whether

that the benefits are worth the costs. In some small businesses, certification may not be worthwhile and a self-declaration of conformity to a standard makes more business sense.

How Did the Special Committee's Advocacy Move the ABA to Business Continuity Certification?

Before we talk about our approach to BS 25999-2 and PS-Prep^{TM} Program certification, it's important to understand more about the **ABA's Special Committee on Disaster Response and Preparedness**, and why we at the ABA decided to pursue business continuity certification. First and foremost, the Special Committee comprises ABA members selected for expertise in emergency preparedness and response, including disaster law and policy. Their mission is to promote and assist lawyers, law firms, bar associations and the justice system prepare for and respond to disasters; to assist lawyers, as needed, recover from disaster; and to ensure that the rule of law is respected and protected in times of major disasters.

Among other strategic initiatives, the Special Committee spearheaded a **resolution**, adopted by the ABA's House of Delegates in August 2011, urging "all lawyers to regularly access their practice environment to identify and address risks that arise from any natural or manmade disaster that may compromise their ability to diligently and competently protect their clients' interests, and maintain the security of their clients' property." That same month, the Special Committee published, **Surviving A Disaster, A Lawyer's Guide to Disaster Planning, August 2011**. These significant steps paved the way for the ABA's path to business continuity certification, and the broader appreciation of private-sector preparedness. Today, just over a year later, the ABA is a brand-name business which has proven the value of business continuity certification.

The American Bar Association is only the second corporation and the first association in the U.S. to prepare for and successfully achieve BS 25999-2 and PS-Prep^{TM} Program certification. Headquartered in Chicago and Washington, DC (USA), the ABA is a certified not-for-profit corporation. The ABA is closer to realizing vision of **The 9/11 Commission**, along with a growing number of lawyers, law firms and global businesses who are pursuing alignment to an industry standard(s) and, if warranted, certification. The ABA strives to maintain our BCMS certification, realizing that our process enables us to deliver products and services under all-hazards while driving higher performance and continuous improvement.

What Does the ABA's Business Continuity Management System Look Like?

In June 2010, the ABA began to align its Business Interruption and Recovery Plan to the industry standard in preparation for certification to BS 25999-2 and PS-Prep^{TM} Program. We started with the creation of the business continuity management-related roles within our organization:

• **Business Continuity Steering Committee:** The Business Continuity Planning Task Force (BCPTF) is responsible for providing business continuity management system oversight and confirming that the system's scope, goals and objectives align to organizational and stakeholder needs;

• **Program Manager:** This role is responsible for establishing the business continuity management structure and the timelines and activities required to expand, enhance and maintain the business continuity management system; and

• **Program Coordinator:** This role is responsible for the day-to-day execution of business continuity management system activities which includes close coordination with the ABA's business entities.

We established a business continuity policy that defined our program's scope to cover operations at headquarters in Chicago, including delivery of our products and services, as well as the maximum acceptable downtime for each. Our policy also defined objectives for the BCMS, including protecting employee safety, managing the risk of resource loss (e.g., facilities, technology, etc.), and establishing plans to effectively respond to disruptive events. We learned that the goals/objectives of the policy must be aligned with processes that are measurable. Our policy, along with all other management system documentation, is organized, documented and will be maintained within our forthcoming business continuity software tool.

RATIONALE

Having introduced our rationale, our business continuity management system and our reasons for pursuing certification, this section of the business case outlines questions to contemplate at each phase, as well as our personal experiences pursuing BS 25999-2 and PS-Prep^{TM} Program certification, which organizations can consider when evaluating and designing their own path forward toward certification.

1. PLAN (DECIDE)

Quick Assessment – Is There a Business Case?

In almost all cases, aligning to a business continuity standard helps improve program performance and enable continuous improvement. However, even if/once an organization aligns to a standard, there still may not be a business case for seeking certification. So, before applying significant time and resources to this effort, take a step back and think about the potential value to be gained from certification. In other words, is there a business case that warrants the investment of time, attention and resources? For some organizations, certification may act as a **market differentiator** when clients are seeking particular or regulated **legal services** or when bidding on **requests for proposals** (RFPs) to provide mission-critical products and services. For others, it may help reduce the number of business continuity audits or inquiries by customers. Regardless, make sure there's value before moving forward!

It's also important to understand the costs associated with certification, since this can be a barrier for some smaller organizations and for business continuity programs with limited resources. Depending on the length of time required for onsite auditors to assess a program between stages 1 and 2, certification (audit) fees alone can exceed US$ 20,000 over a three-year certification period. Determining the business case and associated costs (preparation and audit) is a critical first step, as it helps sell the idea of certification to management without investing significant resources.

In-Depth Assessment and Gap Analysis

Even if there is a business case to pursue certification, it is critical to spend sufficient time understanding and developing the "roadmap" that outlines how to align the current-state program to the selected standard. Many organizations assume that because they have invested heavily in preparedness that they will be sufficiently prepared for certification. However, certification involves successfully responding to audit inquiries based on a specific set of requirements noted in a selected standard. As such, fully understanding the alignment between the program's current state and the standard's requirements enables identification of gap closure strategies and estimates on costs and resources (including required individuals, time, and investment). A required assessment is a formal Business Impact Analysis and Risk Assessment. A Training Needs Assessment is also required. Understanding gaps and resource requirements enables the development of a project schedule with quantifiable measures that can then be presented to program management for review, feedback and approval.

Scheduling the Audit

Following management's approval of the project schedule and required resources, personnel should reach out to the certification body of the chosen standard to scope the certification effort, and then schedule the Stage 1 and Stage 2 audits. It is important to note that scheduling many months in advance is typically necessary in order to involve the most appropriate certified auditors. As such, perform this task early and select dates by which program alignment should be completed since future adjustments to the schedule may not be possible.

Our Decision – "Lessons Learned"

● We sought and promptly received the strong support of top management, ABA Executive Director Jack Rives, for our path to business continuity certification.

● We referenced BS-25999-1, the Code of Practice, in addition to BS 25999-2, the Specification, to better understand the BCM standard's intent.

● We sought honest input in surveying and assessing the BCM program to ensure we were requesting sufficient resources, and the right amount of time necessary to align.

● We sought candid discussions with potential certification bodies about their expertise, experience, and emphasis on customer service.

5

2. DO (PREPARE)

As important as the initial analysis is to understanding the overall effort necessary to align to BS 25999-2, ISO 22301 or other certifiable standard, actually performing the alignment and preparing for the audit is the most critical step of the certification process, as this step enables success in seeking certification. Three key activities that will help enable success are establishing the program's scope and objectives, involving the right personnel and performing an internal audit. (1.) BS 25999-2 and ISO 22301 strongly emphasize the establishment of a clear program scope and objectives within a program policy in order to clearly define and understand the breadth and depth of the BCMS. While this may be done in a variety of ways, most organizations choose to identify critical products and services that will be included in the business continuity program. Related to this, certifying bodies also require a certification scope, to define exactly what portions of the program are considered within the certification purview. Scope the certification effort to include those elements of the organization that will benefit from the certification, whether it is one or more products/services, locations, or the organization as a whole.

(2.) Involving and educating key personnel (including management) engaged in the certification process or business continuity program is an important activity to ensure that everyone involved in the effort is aware and supportive of the process and willing to do their part to improve the program, including documenting results. We learned/emphasize that **everyone in the organization** must be involved in BC; for certification, BCM must be **embedded** in the organization. It may be helpful to emphasize the importance of approaching the certification process from the perspective of an auditor, as doing so will better prepare the program for the audit process and potentially reduce the time and effort required for the certification audit and the subsequent remediation effort.

(3.) Internal audit is a key activity following the completion of the program alignment and remediation process (and a requirement before the Stage 2 audit). Here, a fresh set of "independent" eyes (not necessarily a formal "internal audit" department) reviews the newly aligned program against the standard in order to identify any gaps or areas of opportunity. We hired an expert to train ABA auditors on the BCMS process.

Pre-audit coaching including using self-assessment software is an option which organizations may consider choosing that is designed to help prepare key personnel by reviewing the documentation for the audit process leading to third-party certification.

> **Our Preparation - "Lessons Learned"**
> ● Document and organize everything. Alignment and certification are different processes. A good program does not equal an auditable program. A good program does not equal an auditable "management system." It's not just a program anymore when seeking certification.
> ● The steering committee "shall" meet periodically to present progress, address issues, and ensure the project stays on track. Meeting is not optional. Also key is tracking the review of all management system components, using the meeting minutes and management review matrix.

3. CHECK (AUDIT)

The audit process can be stressful and confusing, so it's important to fully understand the focus and purpose of each phase. Organizational certification efforts (including the new ISO 22301) include two phases: a Stage 1 audit, focused on comparing the design of the program to the standard; and a Stage 2 audit, focused on the organization's program performance based on the design of the management system. While Stage 1 focuses primarily on the existence of documentation that describes alignment to the standard, auditors often use the review to communicate Stage 2 expectations and the evidence they are expecting to see from a performance perspective.

During each audit visit, it is important to adequately prepare for the auditor, including having audit evidence organized and easily viewable or retrievable. "Evidence mapping" (mapping evidence to the requirements noted in the standard, in other words anything that has the word "shall" accompanying it) is an efficient and effective tool that can be used here. In addition to documentation, it is important that at least one employee who is very familiar with the business continuity program be present to discuss the program's scope, objectives, processes, outcomes and evidence.

During the audit, it is easy to take a defensive stance with the auditor as he or she probes for documentation, information and evidence. However, it is important to remember that the auditor is an expert on the standard, has seen several different approaches to aligning to requirements, and knows what to expect and accept. It is possible (and valuable) to present a case on why your approach meets the intent of the standard, but if the auditor still disagrees, it is important to respect their opinion in a professional manner and discuss solutions they've seen that successfully satisfy audit requirements.

Auditors are almost always willing to consider an alternate approach that results in an acceptable outcome, but keep in mind that due to independence requirements, they cannot help you develop a definitive solution. Make sure to fully understand shortcomings before the auditor leaves from each visit; there is no benefit from having the auditor return just to find the exact same non-conformity during the Stage 2 audit.

Utilize the time between the Stage 1 and Stage 2 audits to remediate any issues identified by the auditor. Before moving forward with remediation work, present outcomes and requested resources to management to keep them involved in the process and comfortable with the level of effort necessary. If the schedule agreed upon by management to complete the remediation work is not possible by the Stage 2 audit, contact your certifying body immediately to assess if dates can be adjusted (however, keep in mind that there is a maximum amount of time allowed between Stage 1 and Stage 2).

> ### *Our Audits: Lessons Learned*
> ● Organize and become immediately familiar with your program and documented evidence to make the process significantly more pleasant and efficient.
> ● Present your case, but don't be defensive.
> ● Make sure you understand all shortfalls before your auditors leaves, to avoid being written up for the same non-conformity upon their return. As an example, we did not understand how our correction method would be perceived from the auditors' view, using the benchmark standard, ISO 19011:2011, Guidelines for auditing management systems.

4. ACT (CONTINUOUS IMPROVEMENT)

It is easy to assume that once the Stage 2 audit is complete, the certification effort is over. The truth is, however, that the effort is just beginning, as it is highly likely that remediation work of some kind will be necessary. It's important to keep in mind though that non-conformities do not necessarily equal failure. Instead, try to view them as further opportunities for program improvement, as remediating these issues will both strengthen the program and enable certification.

Instead, try to view them as further opportunities for program improvement, as remediating these issues will both strengthen the program and enable certification. Following the audit, submit an action plan to your certifying body on how you plan to address any issues identified. Once the auditor reviews and approves the submitted action plan, certification may be granted.

Certification is valid for three years, although annual surveillance "checkups" are required to confirm your program is operating as designed and still meets the requirements of the standard, and ensure corrective actions were implemented in accordance with the action plan. Every three years, a "full" audit will again be necessary in order to perform an "in-depth" assessment of current program operations, although the process is still typically less complex than the initial certification process.

Continuous Improvement Tips and Pointers
● Certification to a standard doesn't signal the end of business continuity planning efforts. Rather, it's the opportunity to use the groundwork of a certified management systems approach to business continuity to drive continuous improvement and preparedness throughout the organization.
● Keep current with the remediation. The auditors will ask to see it in future check-ups, so make sure you have something to show them.

To help understand the process start to finish, the following diagram depicts each phase of our certification effort and the overall effort:

PLAN (Decide)	DO (Prepare)	CHECK (Pre-Audit & Audit)	ACT (Improvement)
7 MONTHS	13 MONTHS	3.5 MONTHS	1 MONTH
6.11.2010 – 2.3.2011	2.4.2011 – 4.1.2012	4.3-2012 – 7.10.2012	7.10.2012 – 8.1.2012

Questions and Concerns Regarding Standards, Alignment and Certification

The business continuity community is growing rapidly with changes to existing standards and the **development of new standards**. More organizations are considering business continuity certification and it's natural to have questions and concerns about aligning to one or more of the many available industry standards (e.g., **BS-25999-2, NFPA 1600:2013,** or **ASIS SPC 1.2009**, and the recently approved **ISO 22301:2013**), particularly if your law firm seeks to comply with the Model Rules of Professional Conduct and/or sector-specific regulations affecting your clients. Further, you may also be concerned that certification is expensive, only applies to large organizations and/or requires significant changes to your program's current objectives and scope. Along our path to certification, we discussed concerns with business continuity professionals of global organizations and consultants, such **Avalution Consulting**. After a careful assessment of emergency preparedness and response, and completing a two-year process of embedding **BS 25999-2** within the ABA's corporate governance, we found that we agreed with **Avalution Consulting's** three conclusions:

• **The Cost Certification Varies, but is Calculable:** While the cost of certification varies due to differing needs (based on current-state preparedness efforts and alignment to a specific standard), there are ways to estimate costs up front before investing significant resources. A majority of costs relate to preparing for certification by aligning to a standard (time and resource costs) rather than completing the certification process (third-party certifying body audit costs). *You might roughly compare alignment and certification to studying the law (years) and passing the bar exam (months) – two processes which together provide you the capability of delivering products and services to your clients*. By estimating costs up front, your organization can determine if the investment makes business sense.

• **Certification Applies to Both Small and Large Organizations:** As America's largest law association, the ABA's experience demonstrates that a large organization may achieve certification in a cost-effective manner and benefit from the certification process by adopting an approach that avoids overcomplicating the process but still meets the requirements of a standard. The ABA comprises nearly 1,000 employees and offers **services to nearly 450,000 members** across more than 80 business lines. Small organizations which offer fewer products and services will find that adopting **management systems** and achieving certification is simpler than they expected. As is true of the learning curve for any size of an organization, the learning curve for BCM is steeper in the first year than in subsequent years.

Maintaining the ABA's BCMS certification in year two will be less challenging for the ABA than year one path of achieving it. As we explain in this business case, maintaining certification is not only less time-

intensive and less costly, but is also an integral part of the BCMS standard's lifecycle (continuous improvement) process. *You might roughly compare maintaining certification (annual audit check-ups) to continuing legal education (annual CLE credits) – an on-going process of professional development that many states require of lawyers to maintain their licenses to practice law.*

• **A Management System is a Management System:** An organization which adopts a management system standard should proceed with a focus on results and practicality. The system will become part of the day-to-day operations. It enables the organization to be flexible and innovative by balancing the need for discipline and structure against the need to remain flexible. Recently, there has been discussion on the Internet regarding the development of ISO business continuity management standards. Many posts raise concerns that certifying to a **PS-Prep^{TM}** standard (BS 25999-2, NFPA 1600: 2013 or ASIS SPC.1.2009) will be useless once ISO standards become popular. (It is noteworthy that George Huff, one of the authors of the ABA's business case, is a member of the U.S. Technical Advisory Group to ISO Technical Committee 223, which was responsible for writing ISO 22301: 2012 and ISO 22313: 2012, that ISO published in 2012.). While this is a legitimate concern, it is important to note that almost all recent and forthcoming standards are based on **management systems**, offering a common foundation. Once in place, changing elements or requirements, or even adding another standard within the structure of a management system becomes part of the lifecycle (continuous improvement) process, not a new, separate or time-intensive project. This enables value delivery and implementation cost reduction in both the short- and long-term. In addition, ISO certifying bodies typically grandfather in those certified against the superseded standards, at least until the certification expires and renewal is necessary anyway.

CONCLUSION

Certification to BS 25999-2, ISO 22301 or other certifiable standards provides an organization with the opportunity to develop and implement their business continuity program aligned to an international standard that is recognized around the world. Perhaps more importantly, it enables an organization to leverage a management systems approach in order to drive accountability and repeatability of business continuity efforts, all the while demonstrating a commitment to resiliency and preparedness. How do we know? We did it ourselves.