Taking your business continuity program to the next level via ISO 22301

Introduced in mid-2012, International Standards Organization (ISO) published ISO 22301 focuses on Business Continuity Management Systems Requirements. This whitepaper examines several key components that all business continuity professionals should know:

- The evolution of ISO 22301 and its relationship to BS25999:2
- Why it is important and what to consider in relation to your business
- What are the benefits and how do I move my organization on a path towards ISO 22301

Setting a new standard

In May 2012, the International Standards Organization (ISO) published the long-awaited ISO 22301. This standard, "Societal Security — Business Continuity Management Systems — Requirements," was developed based upon an international review of all ISO standards. It utilizes as a foundation BS 25999:2: a standard which has already garnered broad acceptance outside the UK.

Before turning to the content of ISO 22301, what makes it significant, and who should pay particular attention to the standard, it is beneficial to review the appeal of BS 25999:2. This earlier standard entered the scene when it became evident in the business arena that continuity and resilience were issues that should be addressed at the highest levels of organizational management. People began to understand the true difficulties involved in both identifying risks and in crafting policies and procedures to mitigate those risks and ensure organizational survival. BS 25999:2 made it clear that effective business impact and risk assessments demand knowledge of business processes, technology dependencies, regulatory requirements, organizational cash flows, cross-department operations, and regulatory and legal implications, plus a detailed understanding of the resources — especially the people — who will ultimately act in the face of disruptive events.

ISO 22301 builds on this foundation, along with commentary from the international community and the business continuity practices found in other standards, such as NFPA 1600:2010, ASIS International SPC.1-2009, FINR A Rule 4370, NIST SP 800-34, and various national standards such as those in Australia/New Zealand, Singapore, Japan and Canada. ISO 22301 therefore represents the latest step in the evolution of business continuity best practices.

In its relatively brief format (24 pages), ISO 22301 establishes core criteria for organizations of all sizes, and within varied industries. As such, it offers a robust framework for individual organizations to build their own Business Continuity Management Systems (BCMS).

ISO 22301 "… makes executive governance the focal point of a BCM program, and this may make it more rigorous for some organizations to implement."

ROBERTA WITTY
Gartner Analyst

Source: "New ISO BCM Standard Places Executive Governance Front and Center," Gartner Research: May 18, 2012.

SUNGARD® AVAILABILITY SERVICES™

WHITE PAPER

Thought Leadership

What's in a name?
Most readers of ISO 22301 will quickly fall into using an abbreviated name, likely something such as "the business continuity standard." While that is acceptable, it is worthwhile to consider the implications of the full title. The first part of the formal title, "Societal Security," recognizes that no organization operates in a vacuum. Commercial enterprises, government agencies, non-governmental agencies, and charitable organizations all have one thing in common: they operate within the context of society, touching customers, trading partners, suppliers, local, regional, national and foreign governments, and more. The delivery of their products and services to a defined marketplace has ramifications far beyond their four walls. This change in title is a significant shift from the BS25999:2, "Business Continuity Management Specification." ISO 22301 isn't just about business: it is about society.

The next part of the title also deserves executive focus: ISO 22301 calls for "Business Continuity Management Systems." There is an emphasis here on the role of organizational management and leadership. ISO 22301 provides more than context and guidance for C-level executives to consider: in reality, it is a call for leadership action.

The last part of the title, "Requirements," implies rigor and compliance. It could even be construed as a warning: to remain in operation should a disaster strike, the steps outlined in ISO 22301 must be effectively planned, implemented, and validated. Anything less, and businesses cannot be considered recoverable or resilient.

A call to action
Statistics from recent years are daunting: the rate of both natural and man-made disasters is on the rise, at least as far as measured impacts. "Fourteen billion-dollar disasters occurred in 2011 [in the US], the highest number on record. 2011 had more billion-dollar disasters than the entire decade of the 1980s."[1] These impacts are not limited to the United States: "Disasters in 2011 set a new record of $366 billion for economic losses including $210 billion as a result of the March tsunami/ earthquake in Japan and $40 billion as a result of the floods in Thailand. 206 million people were affected by 302 human-impact disasters…"[2]

Because of numbers such as these, ISO 22301 recognizes that the need for every organization to remain resilient is a not a question of "if." It is a question of "when." As a result, ISO 22301 describes a BCMS as more than a static "organizational policy" people pay lip service to. A company that complies with ISO 22301, develops strategies and plans in the context of the organization's particular risk appetite, trains their staff and associated trading partners with regard to the critical steps in each level of plan, and validates that the plan does, in fact, work. Such an active and organic BCMS is dependent upon the dynamic and continuous leadership of the senior management within every organization. ISO 22301 addresses this in two clauses: Clause 4 ("Context of the organization") and Clause 5 ("Leadership"). As Gartner analyst Roberta Witty cites, ISO 22301"… makes executive governance the focal point of a BCM program, and this may make it more rigorous for some organizations to implement."[3]

1 Elizabeth Ferris, "Natural Disasters in 2011 Strike the Rich," The Brookings Institute, www.brookings.edu, March 26, 2012.

2 United Nations, "2011: Record Year for Economic Losses" in Evidence, Issue 4, January 2012 (www.unisdr.org).

3 Roberta Witty, "New ISO BCM Standard Places Executive Governance Front and Center," Gartner Research: May 18, 2012.

"…by removing inventory from the supply chain, every participant becomes more dependent on others. Furthermore, the system as a whole becomes less resilient."

DR. YOSSI SHEFFI

Source: The Resilient Enterprise, Cambridge: MIT Press, page 90.

Beyond the organizational walls

As already noted, ISO 22301 makes multiple references to business continuity considerations which are outside the organization. Beginning with Clause 4.2, "Understanding the needs and expectations of interested parties," the standard challenges organizations to think broadly about just who those "interested parties" may be. At a very basic level, consider outsiders such as customers, supply chain partners, and third-party service providers — those external entities with systemic roles in a business' success.

Customers are the principle stakeholder for any organization: without them, any organizational effort is, at best, an academic exercise. In the face of a crisis or disruption of services, the impact felt by customers may range from minor dissatisfaction to grave danger. Therefore, crisis communication that is both timely and sufficient is critical to secure customers' positive opinion and to encourage them to maintain their relationship with the organization once the disruptive event has been concluded.

Supply chains are vital to organizational success, and ISO 22301 calls out these dependencies within the context of the BIA (8.2.2.d) and in the discussion of defining a BC strategy (8.2.1). In fact, the importance of resilient supply chains for the effective operation of organizations on a global basis is the subject of government attention: the U.S. "National Strategy for Global Supply Chain Security" includes the goal of fostering a resilient supply chain, which is defined as encompassing preparation and planning, mitigation of risks where possible, and recovery when disruptions do occur.[4]

From a resilience and continuity perspective, supply chain partners and all 3rd party vendors demand special attention. The complexity of a recovery program within a single organization is challenging enough; the cumulative effect of multiple organizations each preparing their continuity strategy within the framework of their policies and business processes adds a new level of complexity which grows almost exponentially as the number of 3rd party interactions are considered.

4 National Strategy for Global Supply Chain Security, The White House, January 23, 2012, page 3.

ISO Reference	P-D-C-A	Consulting	LDRPS	BIA Professional	Risk Assessment	Assurance[NM]/Notifind	Incident Manager	Test Management	Work Force Assessment	Vendor Assessment
4 – Context of the Organization	P	✖	✖	✖	✖					
5 – Leadership	P	✖		✖	✖					
6 – Planning	P	✖	✖	✖	✖	✖		✖	✖	✖
7 – Support	P	✖	✖	✖	✖	✖	✖	✖	✖	✖
8 – Operation	D	✖	✖	✖	✖	✖	✖	✖	✖	✖
9 – Performance Evaluation	C	✖	✖	✖	✖	✖	✖	✖	✖	✖
10 – Improvement	A	✖	✖	✖	✖			✖		

Table 1: Sungard AS CMS and ISO 22301 mapping

This is not a new problem, but lean supply chain management disciplines accentuate the impact. Dr. Yossi Sheffi explains this phenomenon: "… by removing inventory from the supply chain, every participant becomes more dependent on others. Furthermore, the system as a whole becomes less resilient."[5]

Supply chains — whether viewed in a manufacturing setting or in other vertical markets, such as the flow of capital in our global banking systems — are fragile systems highly dependent upon information technology. The claim can easily be made that "just-in-time" business processes would not be possible without modern automation systems. Within the context of these interconnected systems and organizations, the reality check that leaders must accept is this: disasters continue to happen, both of the natural and man-made variety. Many companies or organizations would correctly assess themselves as "targets" when completing a risk assessment, but all organizations are subject to natural events and their sometimes catastrophic results. Interconnected organizations drive our digital economy.

Stephen Flynn, international expert on homeland security and trade, described the issue in these simple, but insightful words: "Disasters cannot always be averted, but we can anticipate and take pragmatic steps to prevent the cascading consequences that are likely to flow from them."[6]

Plan-Do-Check-Act model

At the center of ISO 22301 is the ISO model "Plan-Do-Check-Act," frequently abbreviated "PDCA." The PDCA lifecycle model offered in ISO 22301 is in many respects identical to that which has been part of BS 25999:2; the only difference is that the ISO diagram includes the specific words "Plan," "Do," "Check" and "Act."

Clauses 4 through 7 of ISO 22301 expand upon the concept of "planning," and emphasize the importance of understanding the context of an organization, discussing leadership and commitment to BC, planning out the BCMS project and objectives, and establishing a foundation for organizational support.

"Do" is then addressed in Clause 8, titled "Operation," where some expected activities such as conducting a BIA and risk assessment are included, along with a discussion of exercising and testing the plans (8.5).

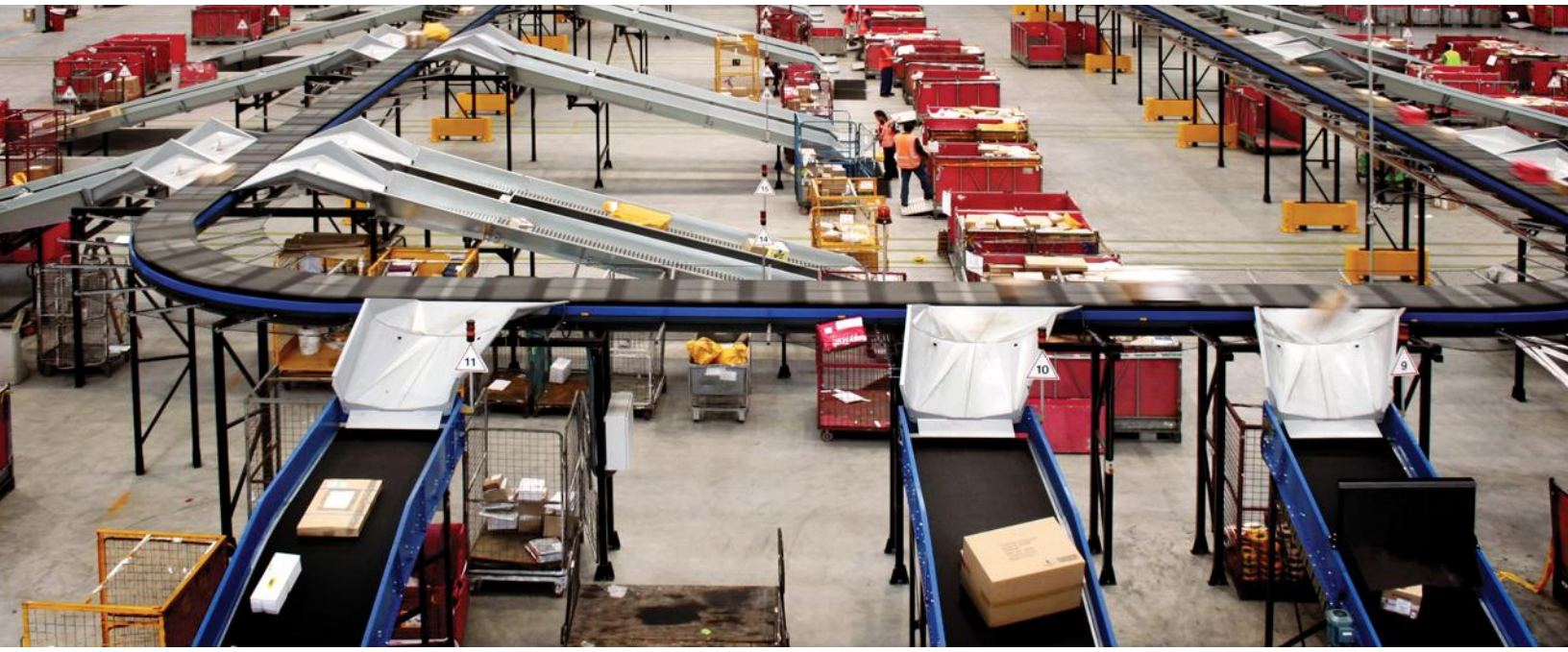
Clause 9, "Performance Evaluation," takes into consideration the important task of "checking" that what has been accomplished in the validation testing can be consistently achieved, through effective monitoring and ongoing evaluation of results.

The final clause in ISO 22301, "Improvement," provides the framework for "acting" to ensure that changes required from the evaluation stage are incorporated in a timely manner into the plans an organization relies upon.

As illustrated in Table 1, the Sungard AS Continuity Management System (CMS) has program elements which correlate to the ISO 22301 across each Clause. This mapping and integrated capability helps organizations actively engage with the full Continuity Life Cycle, both within their organization and with outside partners.

5 Yossi Sheffi, The Resilient Enterprise, Cambridge: MIT Press, page 90.

6 Stephen Flynn, The Edge of Disaster, New York: Random House, page 168.



Planning is only the beginning

A significant emphasis in ISO 22301 is that of maintaining the BCMS and testing its effectiveness. Maintaining a BCMS is mentioned no less than twenty-seven times, while testing is considered fifteen times throughout the document. This emphasis is consistent with every major continuity standard. For example,

- NFPA 1600 speaks to testing (chapter 7) and program improvement (chapter 8)[7]
- FFIEC Business Continuity Planning Handbook speaks of the "Principles of the Business Continuity Testing Program" (page 17) and "Updating Business Continuity Plan and Test Program" (page 27)[8]
- The American National Standard on Organizational Resilience addresses exercises and testing (4.5.2.2) and corrective action (4.5.3)[9]

7 NFPA 1600: Standard on Disaster/ Emergency Management and Business Continuity Programs, 2010 Edition.
8 Federal Financial Institutions Examination Council Business Continuity Planning IT Examination Handbook, March 2008.
9 ASIS International, Organizational Resilience: Security, Preparedness and Continuity Management Systems – Requirements with Guidance for Use, ASIS SPC.1-2009.

A closer examination of the detailed language in ISO 22301 serves as a reminder that a BCMS demands continuous improvement, because all organizations are constantly changing and adapting within their market. This could include regulatory changes, changes to suppliers, shifts in business revenue drivers, adjustments to staff or other physical resources, and more. Organizations must therefore not only perform ongoing maintenance and testing (5.3); they must make adjustments as necessary and validate those modifications to ensure an up-to-date and robust BCMS.

A strategic investment

In any discussion on business policy and process, it is reasonable to ask, "Why should my organization invest in this effort?" While the reasons are many, some that serve as a foundation for standards-based business continuity development include:

- **Increased operational resilience:** Operational resilience requires comprehensive knowledge of the organization; as such, it cannot be achieved by a single department or managed by a single individual. ISO 22301 calls for effective and timely Business Impact Analyses (BIA) and risk assessments to provide an integrated, cross-department view of the organization. The result is a greater opportunity to actualize operational resilience enterprise-wide.
- **Enhanced protection of shareholder value:** Studies have shown that organizations who experience an outage without any plan in place have a more difficult time recovering; for many, lost revenue may lead to closed businesses.
- **Improved operational effectiveness and efficiency:** Experience has shown that the collaborative style required to conduct effective BIAs and risk assessments will invariably identify business processes which are counterproductive to resilient operation, and which are usually also counter to operational effectiveness. The result of mitigating the findings from the ISO 22301 process will usually lead to a more effective and efficient organization.

Taking your business continuity program to the next level via ISO 22301

What's Next

ISO 22301 is an important next step in the evolution of international standards for business continuity, but it is not a final step. ISO 22313, "Guidance to Creating a Business Continuity Management System" is under ISO development, and is anticipated before the end of 2012. ISO 22390, "Guidelines for Exercising and Testing" is also anticipated by late 2012 or early 2013, and will serve as a natural extension of ISO 22301 Clause 8.5. Organizations of every size need to understand how ISO 22301 provides a framework to help them achieve a level of maturity within their continuity planning process. Reviewing this standard and putting into place the action plans and business processes it recommends will ensure the operational resilience businesses need to promote their growth in the years ahead.

"Disasters cannot always be averted, but we can anticipate and take pragmatic steps to prevent the cascading consequences that are likely to flow from them."

STEPHEN FLYNN
International expert on homeland security and trade

Source: The Edge of Disaster, New York: Random House, page 168..

For more information
Visit the **Operational Resilience section of the Sungard AS website** as well as the **Sungard AS Blog**.

About Sungard Availability Services
Sungard Availability Services provides managed IT services, information availability consulting services, business continuity management software, and disaster recovery services.

To learn more, visit **www.sungardas.com** or call 1-888-270-3657

Connect with Us