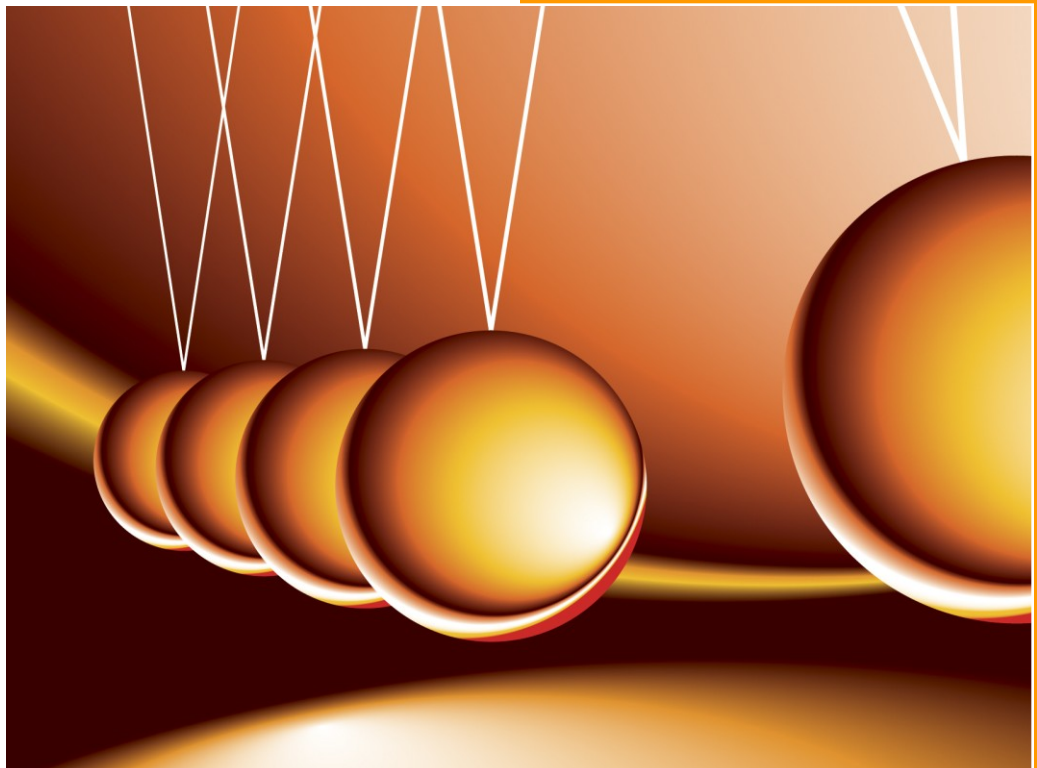


# How to Deploy BS 25999



## **Avalution Consulting**

Susan Yardis, Robert Giffin

## **BSI Management Systems America**

John DiMaria

TABLE OF CONTENTS

**TABLE OF CONTENTS ..... 2**

1. INTRODUCTION..... 3

2. ACHIEVING PROGRAM CREDIBILITY BY CHOOSING THE RIGHT STANDARD FOR YOUR ORGANIZATION ..... 4

    2.1. *How to Choose the Best Standard for Your Organization* ..... 4

    2.2. *How BS 25999 Answers These Questions* ..... 4

3. USING THE STANDARD TO BUILD YOUR PROGRAM ..... 5

    3.1. *An overview of BS 25999* ..... 5

    3.2. *Development of the BCMS*..... 6

    3.3. *Implementing and Operating the BCMS* ..... 7

        3.3.1. Scoping the BCMS ..... 7

        3.3.2. Analysis ..... 7

        3.3.3. Risk Reduction Activities ..... 9

        3.3.4. Planning Activities ..... 11

        3.3.5. Exercising Activities..... 13

        3.3.6. Strategy and Plan Review Activities ..... 14

        3.3.7. BCMS Review and Maintenance Activities..... 14

4. MATURING YOUR BUSINESS CONTINUITY PROGRAM..... 15

    4.1. *How To Evaluate Your Organization* ..... 15

    4.2. *Common Areas of Improvement* ..... 16

        4.2.1. Training and Awareness ..... 16

        4.2.2. Review of Documentation..... 19

        4.2.3. Program Evaluation..... 20

5. TAKING THE NEXT STEP: THE CERTIFICATION PROCESS..... 21

6. CONCLUSIONS ..... 24

## 1. INTRODUCTION

Business continuity programs, similar to other enterprise processes, are most effective when grounded in generally accepted standards and built according to the business' objectives. Business objectives and "proven" standards together form a foundation that adds credibility and viability to a continuity program. This whitepaper explores a new code of practice (and its associated specifications document), the British Standard Institution's BS 25999, viewed by a growing body of practitioners as a complete description of a mature, repeatable and actionable business continuity program. In addition to providing implementation details for the standard, this document covers how to use BS 25999 to obtain executive support, create a business continuity program or increase the maturity of an existing program.

The purpose of British Standard 25999 is to provide a basis for understanding, developing and implementing business continuity within an organization and to provide confidence in business-to-business and business-to-customer dealings. British Standard 25999 is written in two parts. Part 1, the Code of Practice, outlines the standard's overall objectives, guidance and recommendations. Part 2, the Specifications, details the activities that should be completed in order to meet business continuity objectives within the context of an organization's overall business risks.

### **Background: From Business Continuity Planning to Business Continuity Management System**

Business continuity is a rapidly maturing discipline that has moved from the realm of IT systems recovery to holistic business recovery and resiliency. With these changes, business continuity-related terminology has also matured. A few years ago, business continuity planning (BCP) was the latest term to articulate the growing role continuity was playing in protecting critical business processes from failure. As this practice has grown and established itself as a key risk management discipline for businesses, a movement toward standardization has occurred, similar to the quality initiative standardization experienced in the 1990's. As a result, "systems thinking" (such as quality systems) has been applied to business continuity planning, resulting in a new term:

*"... 'systems thinking' (such as quality systems) has been applied to business continuity planning, resulting in a new term: Business Continuity Management System (BCMS)."*

Business Continuity Management System (BCMS). While BCMS sounds like some new class of pricy business continuity (BC) software, it's not. BCMS refers to a program that encompasses the development and management of policies and procedures to protect an organization's people, processes and supporting technology. BS 25999 proposes and evaluates business continuity based on this collection of processes and resources – referred to as whole systems thinking.

### **Support Grows for BS 25999**

Prior to publication, most draft British Standards draw an average of 250 downloads. BS 25999-1, however, logged some 5,000 downloads, 20 times more than normal. This extraordinary number of downloads demonstrates how important this issue is to a large number of organizations. Another important consideration is that two of the largest American insurance companies, Aon Corporation and Marsh Inc, have also participated on the drafting committee. This interest and participation is very unique and is an early indication that the standard and certification will have strong support by the US insurance industry. It is an benefit to insurance providers if they could persuade their customers to develop and maintain a strong, viable business continuity management system, business interruption-related risk would decrease, thereby decreasing claim payments.

As you read this whitepaper, it will be helpful to refer to both parts of BS 25999. You can purchase your own copy of BS 25999 parts 1 and 2 from the BSI Global website ([www.bsi-global.com](http://www.bsi-global.com)).

### 2. ACHIEVING PROGRAM CREDIBILITY BY CHOOSING THE RIGHT STANDARD FOR YOUR ORGANIZATION

#### 2.1. HOW TO CHOOSE THE BEST STANDARD FOR YOUR ORGANIZATION

Directors of business continuity often cite standards as evidence that they are performing (or need to perform) key activities. However, the most important aspect of effectively using a standard as a benchmark is choosing the right standard. The following questions can help an organization evaluate the various standards to find the best fit for their organization:

1. Is the standard international in nature, providing a framework agreeable to organizations and bodies regardless of geography?
2. Does the standard provide a concise and complete framework, outlining not only business continuity but also analysis and risk mitigation activities?
3. Does the standard reflect management's approach regarding risk management?
4. Is the standard grounded in business terminology, not business continuity terms?
5. Does the standard instill management confidence by describing the "what and how" of key risk management activities?
6. Does the standard not only focus on program development but also long-term program management and maturity activities?

#### 2.2. HOW BS 25999 ANSWERS THESE QUESTIONS

British Standard 25999 provides an organization with guidance and details necessary to build or mature a complete business continuity management system. Read the answers below to determine if BS 25999 is the right choice for your organization.

1. BS 25999 is an internationally-accepted standard, developed by the world's leading international standards, testing, registration and certification organization.
2. A standard is often needed to help focus the program on key activities designed to increase responsiveness and recoverability. BS 25999 provides a framework and specifications to follow and focus attention on the most critical areas, while still providing a "holistic" approach to manage business interruption risk.  
When developing a business continuity plan, it is essential to know the differences between a business continuity management system and a business continuity plan. Business continuity plans, by definition, focus solely on the recovery from an interruption, leaving the residual risks of an interruption occurring unmitigated. BS 25999 outlines a system to address the risk of an interruption occurring as well as the risks that occur following an interruption, and how to mitigate both sides of the equation.
3. An organization should select a standard that reflects the organizations' current approach to risk management. The standard is geared to achieve risk management by utilizing critical activities and objectives, so if these objectives do not align with the organization's approach, attempts to modify the standard will weaken the system structure. Similarly, if efforts are made to modify the organization's approach to risk management to match the standard, the organization may resist changing their culture.
4. Although the use of terminology is inevitable, extensive use of acronyms and "dated" terminology should be avoided; instead, any terms used should be descriptive and require very little explanation. (Reference section 3 of the specifications to further understand the basic terminology used by BS 25999).

5. Standards can be confusing due to their generalized and high-level explanation. BS 25999 was developed in two parts, the Code of Practice and the Specifications, to make the standard easier to understand and implement. Part 2, the Specifications, sets out minimum requirements for an effective management system for Business Continuity and provides a framework for its implementation, management and continuous improvement within an organization. Part 1 of the standard is “good practice” and may go beyond the requirements of part 2. Part 1 is also written in such a way that organizations can receive independent verification that the management system is operating effectively.
6. BS 25999 outlines the continuous lifecycle of a business continuity management system, defining the system as a living and continuously evolving program. Figure 1 depicts this lifecycle.

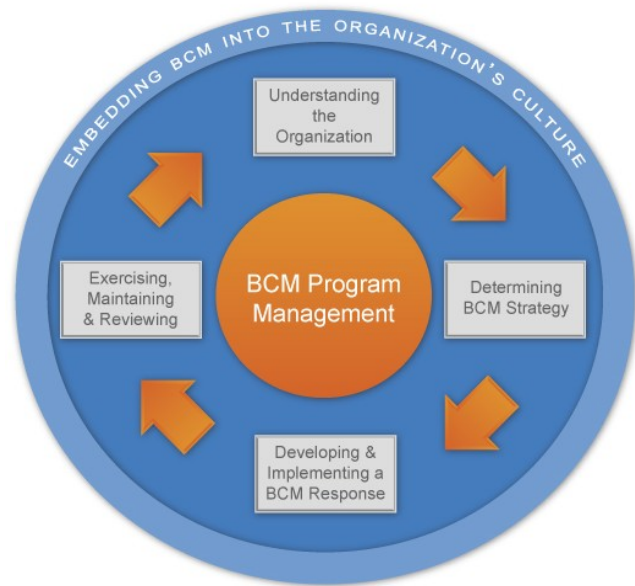


Figure 1

### 3. USING THE STANDARD TO BUILD YOUR PROGRAM

BS 25999 describes “big picture” process expectations (the Code of Practice), as well as details on how to meet the expectations (the Specifications). By following this framework and the activities within each area, a business continuity professional can build a BCMS that aligns with BS 25999. The following sections provide additional detail on various approaches to achieve BS 25999 compliance. This overview can provide a business continuity professional with the basic understanding of the contents of BS 25999; however, the standard should be read to fully understand the specific requirements.

#### 3.1. AN OVERVIEW OF BS 25999

Both the Code of Practice and Specification are organized into two main phases: Development of the BCMS and Implementing and Operating the BCMS. Within each phase, key activities are noted to carry out the implementation of the standard. Each of these key activities is listed below.

##### DEVELOPMENT OF THE BCMS

- a. **Program Requirements** – development of the requirements, objectives, and desired outcomes of the BCMS
- b. **Suppliers and Outsourced Partners** – analyzing the business continuity capabilities of the organization’s suppliers and outsourced partners
- c. **BCM Policy** – developing the policy outlining the roles and responsibilities of all employees in regards to the BCMS, the key activities and timelines associated with the BCMS, and the retention of records within the BCMS
- d. **Provision of Resources** – determining what resources are required to effectively operate the BCMS, including budget, personnel and tools
- e. **Training, Awareness and Competency** – determining the competency of personnel operating key roles within the BCMS, and providing training as required
- f. **Documentation and Records** – developing the processes to manage the documentation and records created as a part of the BCMS

### IMPLEMENTING AND OPERATING THE BCMS

- a. **Business Impact Analysis** – determining the impact of a disruption of critical organizational activities
- b. **Risk Assessment** – understanding the threats and vulnerabilities to the organization’s critical activities
- c. **Risk Treatment Options** – determining the strategy options to mitigate risk by reducing the likelihood of an interruption or limiting its timeframe
- d. **Business Continuity Options** – defining how the organization will recover critical activities, and accounting for those activities not deemed critical
- e. **Response Activities** – determining the processes to respond to an interruption and manage the business recovery activities
- f. **Planning** – documenting the processes determined in the previous three sections
- g. **Exercising** – validating the plans and arrangements are effective and up-to-date with current information
- h. **Strategy and Plan Review** – updating the plans and arrangements following exercising or review
- i. **BCMS Review and Maintenance** – reviewing and revising the BCMS to ensure the program is meeting objectives in an efficient manner

After reading and fully understanding BS 25999’s requirements, the business continuity professional should determine the process necessary to implement the specifications or activities required to meet the standard. With that said, every organization is different, in its size of operations, physical distribution of facilities and culture. The next section discusses the implementation processes successfully used worldwide. Notice that the section is divided into the same two sections as section 3.1.

### 3.2. DEVELOPMENT OF THE BCMS

The first step in developing a BCMS is to evaluate management’s requirements and level of risk tolerance, as well as any requirements from external organizations. To best understand these factors, one large manufacturing organization formed a committee, including the COO, CIO, CFO, and key product area subject matter experts, to meet and discuss these factors and make key decisions regarding the BCMS. This kind of steering committee is a practice that not only provides business-wide consensus, but also demonstrates upper management commitment to the BCMS.

*“This kind of steering committee is a practice that not only provides business-wide consensus, but also demonstrates upper management commitment to the BCMS”.*



Once the program’s driving factors have been determined and understood, a policy should be drafted to document the decisions made and goals of the BCMS. A business continuity policy should outline the key goals of the BCMS, including what factors will be used to determine criticality of activities, what locations or functions will be considered within scope of the program, and who has overall responsibility of the BCMS. Furthermore, it’s important to outline the responsibilities of all participants, including those responsible for activities such as analysis and planning as well as those responsible for implementation activities. Lastly, if not fully covered within another policy in your organization, the business continuity policy should outline the document retention, review and management processes and requirements for all BCMS documents/data. A strong policy should enforce many of the standards described in BS 25999.

While determining the roles and responsibilities within the business continuity policy, the optimal structure of the business continuity organization should be identified. Some larger organizations have dozens of personnel dedicated to business continuity, in groups such as business continuity training, tool development and plan quality assurance. However, smaller organizations may have only one full-time person to address business continuity. Whatever structure is used, it is important to determine what these roles will be and who will be responsible for carrying out key activities such as assessment, planning and exercising. It's also important to ensure that key personnel have the knowledge and background to perform these roles. Personnel should be evaluated and provided with the training needed either internally or from an external source. Throughout the course of defining the planning structure and the roles involved in it, these key decisions should be documented so they will be available for review later.

### 3.3. IMPLEMENTING AND OPERATING THE BCMS

#### 3.3.1. SCOPING THE BCMS

Prior to beginning the analysis, strategy and planning, a key activity is determining the business units into which the organization will be divided for the purposes of planning and analysis. Some organizations, such as a financial institution, evaluate and plan for individual lines of business, such as financial reporting and call center operations. Other organizations, such as a manufacturing organization, evaluate and plan for each facility, and in some cases for individual production lines. The business continuity professional, with the support of a steering committee, can divide the organization however it makes the most sense, including a mix of functional units and locations. The easiest place to start in developing the analysis and planning structure is to review the structure outlined within hierarchical organization charts. In most cases, organizational charts provide a good overview of the organization's processes or areas of practice. Each business unit will need to identify an owner that is responsible for continuity-related activities for that unit. As each business unit and owner is identified, be sure to document the initial scope and begin to involve each owner in the development of the BCMS. A key part of BS 25999 compliance is validating that personnel involved in continuity have the appropriate skills; knowledgeable business unit owners are key to meeting this requirement.

#### 3.3.2. ANALYSIS

The purpose of a business impact analysis is to understand the affects of an interruption on the organization's critical activities. The factors influencing criticality, including revenue contribution, regulatory compliance, operational effects, and customer priority, should be identified during the development of the BCMS. The business impact analysis should use these factors to provide an understanding of and justification for which functions or locations have priority over others based on quantitative and qualitative impact estimates.

In order to facilitate this analysis, some organizations interview key subject matter experts for each business unit, collecting the key information in a small group discussion. This information is documented so an overall analysis can be completed and presented to the management committee responsible for the BCMS. This works well for organizations that are small in size and have personnel

*"A key part of BS 25999 compliance is validating that personnel involved in continuity have the appropriate skills; knowledgeable business unit owners are key to meeting this requirement."*

to conduct the interviews. Although this is one of the best methods for analysis, some larger organizations use online surveys to allow subject matter experts to provide information without significant direct interaction. This method runs the risk of capturing less concise and aligned data, though it can be effective with the right level of preparation. Regardless, a hybrid approach is often chosen where both surveys and interview techniques are used to collect needed information. The pros of each method along with key considerations for implementing either method are depicted in Figure 2.

Interviews	Surveys
<b>Pros of each method</b>	
Provides a more in depth analysis	Requires less personnel resources
Provides a more concise and aligned analysis since one or a small number of people are collecting the data	Allows business personnel to participate at a time that is convenient for them
<b>Considerations if either method is chosen</b>	
Develop an analysis worksheet or template that will be used to analyze each unit. The template should include all key areas or questions. Reference Part 2 of BS 25999 for detailed requirements on what areas need to be assessed.	
Once all analysis is collected, review and document a summary of the analysis noting the key findings across the entire organization, as well as key findings within each unit. Present this report to the management committee overseeing the BCMS for review and input.	

Figure 2

Assessing the threats or vulnerabilities that would cause an interruption to critical activities is also an important analysis activity. Risk assessments should evaluate the likelihood of a threat resulting in a business interruption for each analyzed business unit, and the corresponding severity of each threat’s potential impact. Risk assessment activities should not only take into account the threat environment, but also the controls in place to mitigate the likelihood and severity associated with an interruption. This analysis provides an understanding of the threats that pose the most risk to the organization. This information can then be used in the next phase of planning to identify risk reduction activities. While this process seems straightforward, not all outcomes are this obvious. A New York City law firm was surprised with their risk assessment results when they learned that the basement of their building, where their technology infrastructure is located, frequently floods during periods of heavy rain. By identifying this threat as a high risk factor, the organization was able to make strategy decisions to both decrease the likelihood of an interruption and increase recovery capabilities.

Similar to the business impact analysis, the risk assessment can be conducted utilizing an interview or survey format; however, the analysis may include different subject matter experts. The risk assessment should focus on individuals that are most aware of the threats and controls within each unit, while the business impact analysis should focus on current-state process characteristics and the impact of the interruption caused by the threat. Introducing business impact analysis and risk assessment conclusions enable effective management decision-making regarding BCMS scope, requirements and eventually strategy decision-making.

Another common challenge associated with conducting a risk assessment is dealing with unlikely threats. New York City alone has recently dealt with a steam pipe explosion and a tornado, both of which have not occurred in 100 years. Executives will frequently observe these events and inquire if the company is prepared for them. Because a number of low probability threats will most likely be missed initially, consider evaluating “classes” of threats and their relationship to the effects on categories of resources. For example, an organization might be concerned about explosions/fires, air or water contamination, threats of terrorism, a health event or adverse weather. Looking at each of these classes of threats, consider the qualitative impact on facilities (and facilities access), people, technology, communications, utilities and transportation. The response strategy, should any of these classes of threats occur, can then be established. This approach may not yield specific control improvements, but it does paint a high-level picture of organization-specific threat characteristics and response strategies. Figure 3 depicts an example of this approach.

Impacts	Threat: Contamination	Threat: Explosion	Threat: Weather
<b>Facility Access</b>	Example Content: Contamination outside the company headquarters may result in a shelter-in-place situation, or water contamination may lead to an evacuation; technology infrastructure would be unaffected		
<b>People</b>	Example Content: Authorities may ask people to limit travel and remain inside, affecting travel to/from work and home		
<b>Technology</b>	Example Content: While technology infrastructure would be unaffected, remote access capabilities may be strained based on number of remote users.		
<b>Communications</b>	Example Content: Pervasive work from home strategies may strain “last mile” communications (voice and data), as well as mobile communications		
<b>Utilities</b>	Example Content: Water could be adversely affected, however other utilities would remain operational (power and natural gas); air handling would be terminated if contamination is airborne		
<b>Transportation</b>	Example Content: Public transportation would most likely cease, and road closures may be imposed by authorities		

Figure 3

An unlikely event can act as a catalyst for a number of management questions. “Did our risk assessment address this threat?” “Do our plans address something like this?” “Do we have controls in place to minimize the probability of a business or technology interruption, or the severity of such an event?” Ultimately, the traditional risk assessment can help answer some of these questions, but so can an analysis that describes the potential adverse characteristics associated with classes of threats. Look at your organization’s critical infrastructure and the potential causes of an interruption to determine if any response strategy gaps exist. Consider a traditional risk assessment, but consider the complimentary approach described above. It can act as a business continuity roadmap, assist in identifying strategy gaps and help answer management’s questions regarding business continuity scope and readiness.

**3.3.3. RISK REDUCTION ACTIVITIES**

Risk reduction can occur in three forms – risk treatments, response processes (including emergency response and incident/crisis management) and business continuity strategies. Each form is important and mitigates its own area of risk. Specifically, risk treatments decrease the likelihood that a threat will cause an interruption. Response processes enable management to react swiftly to an event, protecting people and resources. Business continuity strategies work to mitigate the severity of a potential interruption. Collectively, these risk management processes should be developed to mitigate risks and impacts exposed during analysis activities, specifically the business impact analysis and the risk assessment. It is important not to develop just one strategy option for each area of exposure, but a set of options, so that the management body overseeing the BCMS can make decisions on what degree of risk mitigation matches their risk tolerance.

Risk treatments can take many forms, such as enabling process redundancy across multiple locations, purchasing backup power so that an interruption does not impact critical processes or protecting unique equipment that is critical to the production of a high value product. Whatever the form, risk treatments should mitigate the likelihood of an interruption and provide a first defense against business continuity risks. However, reducing the likelihood of an interruption tends to be more costly and more difficult to implement since it affects day-to-day operations. Risk treatments should be prioritized and chosen by management for implementation after a cost benefit analysis confirms they are worth the cost of implementation.

Response activities enable management to react swiftly to an event, protecting people and resources. Employee-focused response activities commonly include the activities associated with an employee safety and fire evacuation program. However, it is important to ensure that the processes outlined in these plans align with the strategies chosen as a part of the BCMS. A large industrial manufacturer recognized a critical need for equipment and product safeguard strategies in their southeast locations. They developed a very basic plan to move all assets off the floor and cover them with plastic wrapping. Although simple, with proper planning and preparation, they were able to protect critical assets through five hurricanes since the implementation of these strategies.

The development of business continuity strategies is best understood by thinking about the resources required to recover critical activities. This list should have been developed during the business impact analysis and documented as a key outcome. Most organizations group these strategies by resource, such as workspace, equipment, consumables, technology needs (to include communications and email requirements) and people. Refer to Figure 4 for a listing of resources types and the most common strategies that organizations consider for business recovery.

Resource	Recovery Strategy
<b>Emergency Operations Center</b> <i>(a workspace for the management group responsible for managing the incident)</i>	<ul style="list-style-type: none"> <li>• A conference room onsite (for incidents that do not destroy the entire facility)</li> <li>• A local hotel or conference facility</li> <li>• Another company facility, located nearby</li> <li>• Another company facility, located about 60 miles away</li> <li>• A hotel or conference facility, located more than 60 miles away</li> </ul>
<b>Workstations</b> <i>(workspace for the office employees, including a desk, chair, internet connection, and telephone)</i>	<ul style="list-style-type: none"> <li>• All of the emergency operation centers are possible</li> <li>• Offsite workspace provider</li> <li>• Mobile workspace delivery</li> <li>• Personnel's homes</li> </ul>
<b>PCs</b> <i>(both laptop and/or desktop, supplied with the local application suite required by personnel)</i>	<ul style="list-style-type: none"> <li>• Pre-purchase a critical quantity that is required within the first few days of recovery</li> <li>• Borrow from an alternate company location</li> <li>• Purchase PCs with your external workspace purchase</li> <li>• Plan to use personnel's home PCs</li> <li>• Instruct all personnel to take their laptops home with them nightly, and when evacuating the building</li> </ul>
<b>Specialized Equipment</b> <i>(this could include manufacturing equipment, testing equipment or specialty printers, as examples)</i>	<ul style="list-style-type: none"> <li>• Move back-up equipment to an offsite location</li> <li>• Locate and contract with suppliers to purchase equipment on short notice</li> <li>• Locate equipment available from other company locations</li> </ul>
<b>Office Supplies</b> <i>(develop a list, with quantities per person or team, including pens, paper, printers, faxes, etc.)</i>	<ul style="list-style-type: none"> <li>• Pre-purchase a critical quantity that is required within the first few days of recovery</li> <li>• Borrow from an alternate company location</li> <li>• Purchase supplies from your external workspace provider</li> <li>• Plan to purchase at the time of the event from your regular provider</li> </ul>

Figure 4

Overall, risk mitigation strategies are developed to guide the planning efforts. By considering all possible risk treatments together, as an overall risk management effort, senior leadership can make prioritized decisions based on a cost benefit analysis. Following management's decisions, the business continuity professional should be prepared to implement the chosen risk strategies and document plans ensuring repeatability.

### 3.3.4. PLANNING ACTIVITIES

Planning is the activity that many new business continuity professionals focus on because it is most familiar. However, as seen by reading BS 25999, a significant number of essential tasks must take place before planning activities are even started. Planning should only occur after risk and impact analyses have been completed and resulting risk mitigation strategies are determined. The objective of planning is to provide the documentation to implement response and business continuity strategies to meet management-approved downtime tolerances. When developing business continuity plans, there are two primary issues to consider:

1. What is the optimal planning structure (the scope of a plan, as well as its layout/format)?
2. Who will be responsible for documenting and maintaining the plans?

Just as in analysis, planning should occur for each business unit that is essential to delivering critical products and services and avoiding unacceptable organizational risk. Depending on the size and structure of the organization, the planning structure may be complicated or simple. A large international lending firm organizes its planning structure by facility, documenting a plan for each office location and then forming an overall management level plan for each country. In total, this firm has 50 facility recovery plans, and 12 country level management plans. A much smaller development organization that primarily operates out of one facility documents its recovery in seven function/process level plans and one overall management level plan. The key in determining the planning structure is to understand day-to-day decision-making and how facilities and processes interact to deliver value to key stakeholders.



*“The key in determining the planning structure is to understand day-to-day decision-making and how facilities and processes interact to deliver value to key stakeholders.”*

On top of function or location based recovery plans, it is important to document the management-level decision-making and response activities that need to occur. This is commonly referred to as Crisis Management or Incident Management. This plan and associated strategy summarize the processes that a group of management-level personnel will complete in order to assess the impact from an incident, determine if recovery plans need to be implemented, assess priorities of recovery, provide resources for recovery and manage communications during the incident and recovery. This group of management personnel is commonly referred to as the crisis or incident management team and should represent all key decision makers across the organization. Figure 5 depicts a common list of team members and their primary responsibilities. An international lending firm used a similar crisis management team structure at the corporate level, but also developed a local management structure for each country. They determined a need to have a group of management-level personnel convening to guide recovery efforts around the world at the corporate level, as well as a need for a local team to guide unique decisions that are country specific.

### Crisis Management Team Members and Responsibilities

**CMT Leader** – Responsible for managing the recovery effort.

**Administration** – Provides administrative support to the CMT by screening communications and coordinating travel arrangements.

**Human Resources / Internal Communications** – Coordinates all employee aspects of recovery, such as monitoring injured personnel, establishing working hours and managing payroll issues.

**Legal and Regulatory** – Provides advice regarding legal implications of recovery decisions and coordinates the involvement of regulatory agencies.

**Information Technology** – Manages the recovery of technology, such as computers for employees and enterprise applications.

**Finance** – Manages the financial aspects of recovery, such as tracking disaster related purchasing, identifying disaster related costs, and maintaining control over financial reporting.

**External Communications** – Coordinates communications with external stakeholders, such as investors, customers and the media.

Figure 5

### Basic Recovery Plan Outline

1. Recovery Strategy Overview
  - 1.1. Recovery Time Objective
  - 1.2. Recovery Location
  - 1.3. Recovery Strategy
2. Dependencies / Requirements
  - 2.1. Internal Processes
  - 2.2. External Providers
  - 2.3. Applications
  - 2.4. Equipment
  - 2.5. Documents / Data
3. Contact Information
  - 3.1. Internal
  - 3.2. External
4. Recovery Team
5. Recovery Procedures
6. Restoration Procedures

Once a planning structure has been developed, it is important to determine who will be responsible for documenting and maintaining the plans. Frequently, the recovery plans are documented by the personnel who completed the analysis, although this is not required. What is required is that the personnel designated to develop the plans have the time and resources available to them to be able to develop an actionable recovery plan. The best way to start any planning effort is to establish a plan template or worksheet.

A plan template provides a business unit planner with instruction, a starting format and the key sections to be documented. It also provides symmetry amongst all of the plans so they can be implemented by any person who understands the basic planning structure. If the organization struggles to develop a recovery plan template, the business continuity professional can obtain assistance from different types of providers, including software solutions that can provide a workflow to document plans and consulting services that can provide templates and assistance. A basic unit level recovery plan outline is displayed in Figure 6.

Figure 6

**3.3.5. EXERCISING ACTIVITIES**

Exercising is the process of validating plan content to ensure strategies are capable of providing recovery within the timeframes agreed to by management. Exercising can also provide training to the personnel responsible for response and recovery activities.

Exercising can occur in many forms and at many different levels. Each form has a cost and benefit that typically is directly related, i.e. an exercise with a higher level of value will have higher costs than a less value adding exercise. Organizations utilizing offsite recovery locations for their workplace recovery strategies may run a full simulation exercise annually. During this type of exercise, the organization recovers at the offsite location or tests to see if critical activities can operate offsite using documented plans. At the end of this exercise, the organization knows if the offsite recovery location provides effective capabilities, if the plans are adequate to recover the critical workplaces and if the established timeframes are achievable. A much simpler exercise would be to test an emergency notification process. Most organizations implement strategies to notify employees in the event of a disaster or business interruption. This could be as simple as a physical list of all home and cell phone numbers, with instructions on how to contact everyone using a top down tree process. A simple test would be to implement the communication chain. Figure 7 shows a matrix of all of the types of exercises and which plans or activities they work best with. Figure 7 also lists the cost benefit trade off for each type of exercise, noting that the easier to implement exercise types have less strategic value.

Exercise Type	Best Use	Cost/Benefit
<b>Plan Walkthrough</b> – reviewing the layout and contents of a plan.	To introduce someone to the concept of a recovery plan, and the specifics of a particular recovery strategy.	Easiest and least time consuming / Provides the least amount of value in terms of proving response and recovery capabilities.
<b>Table Top</b> – using a scenario, discussing what actions and decisions would be made through the use of a documented plan.	To validate the contents of a plan, ensuring accuracy and completeness.	Fairly easy to prepare for and perform / Provides a good initial validation of a plan.
<b>Process or Plan Simulation</b> – using a scenario, acting or carrying out an activity or process recovery plan (typically using recovery locations and resources).	To validate the contents of a plan or the process recovery strategy, ensuring it is actionable and verifying the time allocations.	More difficult to prepare for, sometimes costly if involving external provider / Provides a more “real-life”, actionable test.
<b>Full (End-to-End) Simulation</b> – using a scenario, carrying out the response and recovery activities for an entire organization.	To validate the interaction between groups during a recovery effort, as well as validate the overall recovery time objectives.	Most difficult to prepare for and perform due to its involvement of many people and for an extended period of time / Best test of strategies and plans.

Figure 7

Overall, it is important to document how often plans and processes will be exercised, and to document lessons learned to ensure efforts are made to fix issues and errors. Developing even the simplest exercise documentation template with sections such as exercise objectives, outcomes and follow-up actions items can formalize the exercise process and provide assurance that exercises are being conducted and providing the value they are meant to achieve.

### 3.3.6. STRATEGY AND PLAN REVIEW ACTIVITIES

In addition to exercising plans, it is important to ensure that the documents are updated on a regular basis. The review of strategies and plans is one of the most common areas of failure for business continuity planners, primarily due to their lack of an ability to track “if” and “when” documents undergo review. As discussed in Section 3.2.1 (Development of the BCMS), a business continuity policy should document a change management process and timeframes required for each document. However, a policy is only the first step in ensuring the constant review and maintenance of documentation. In order to ensure that the policy requirements can be implemented, the organization should define a process for clearly documenting who and when documents are reviewed and updated.

Many larger organizations utilize a central documentation repository that provides an ability to see when documents were changed and who changed them. A central location also ensures that everyone can access the most up-to-date electronic version. Document repositories can be as simple as document storage locations with shared access, such as an intranet site or a shared drive. Some more complex document repositories can also provide unique features such as document templates and workflow/approval processes.

If a document repository is too complex of a solution for an organization, they should develop a document control/modification block that is printed on the cover of every document. This is a process that was adopted by a mid-sized accounting firm with a total of twelve recovery plans. The BCMS administrator was responsible for reviewing the documents to ensure that they were reviewed and signed off on in accordance with policy guidelines. An example of this document modification block is in Figure 11 on page 19.

*“The review of strategies and plans is one of the most common areas of failure for business continuity planners, primarily due to their lack of an ability to track “if” and “when” documents undergo review.”*



### 3.3.7. BCMS REVIEW AND MAINTENANCE ACTIVITIES

Not only do business continuity plans and strategies need to be reviewed and updated, but the BCMS structure and processes do as well. By evaluating the BCMS as a whole, the business continuity professional can confirm the organization is meeting objectives, that processes are being implemented correctly and that they are operating as efficiently as possible.

Reviewing a BCMS is similar to other internal departmental reviews, typically carried out by internal audit or another independent entity. Self-assessments can be very beneficial, such as reviewing for compliance with roles and responsibilities, as well as other activities and their associated timelines as outlined in the policy. One large financial institution dedicates a portion of its business continuity team to ensuring the quality performance of the BCMS, including the completeness of plans, efficient use of budget and overall mitigation of the interruption risks. Smaller organizations tend to bring in external organizations to provide a third party review of the structure and performance of their program. Third party assessments can be helpful in that they do not take time away from the business continuity team and can compare the organization with industry benchmarks or standards.

## 4. MATURING YOUR BUSINESS CONTINUITY PROGRAM

As described at the beginning of section 3, BS 25999 describes both the “big picture” process expectations (the Code of Practice) and the details on how to meet the expectations (the Specifications). If an organization has an implemented business continuity program, it can utilize a standard for benchmarking purposes, defining gaps and identifying areas of growth. By using an internationally accepted standard, as well as goals and objectives of the organization, it is likely to be easier to achieve consensus on new initiatives or resource requests for business continuity efforts. The following sections provide details on an approach to completing a self-assessment using BS 25999 specifications. Also provided are common gaps and suggestions on how to address each.

### 4.1. HOW TO EVALUATE YOUR ORGANIZATION

Many areas of an organization are evaluated by internal bodies, such as a compliance organization or internal audit. The approach used by these bodies can be applied to evaluating a business continuity program with a standard or set of requirements. The key to a self-assessment is outlining the key requirements clearly and succinctly and creating consensus on the requirements prior to the assessment.

In order to develop an easy to understand requirements list, utilize a matrix format outlining the requirement, its source and a reference number to use throughout the documentation. For British Standard 25999, the requirements can be divided into the five main areas of practice:

1. Program Management
2. Understanding the Organization
3. Determining Business Continuity Strategy
4. Developing and Implementing a BCM Response
5. Exercising and Maintaining BCM Arrangements

Review Figure 8 to see an example of this type of matrix assessment format.

Audit #	Requirement Source	Requirement	Current Practice	Mitigation Plan
1	BS 25999 – BCM Program Management	The organization has assured that its key suppliers and outsource partners have effective BCM arrangements in place.	All suppliers’ business continuity capabilities are assessed prior to being approved by procurement.	None
2	BS 25999 – BCM Program Management	The organization has made the policy available to relevant stakeholders.	The organization does not have a policy that covers business continuity efforts and responsibilities.	Develop a policy that covers all applicable business continuity efforts, roles, responsibilities and timeframes.

Figure 8

During a self-assessment, it may be helpful to include organizational goals and objectives, such as a focus on product development, client delivery or employee safety. By including company goals, management is more likely to be able to see the value of the assessment findings and therefore approve requests for resources to mitigate identified gaps. Wherever requirements originate, once they are clearly documented, they should be presented to a team of the key decision makers to determine agreement on the key areas of the assessment.

Once the matrix of requirements is established, the assessment can begin by evaluating the current BCMS against each requirement. As displayed in Figure 8, the suggested matrix format contains a column to document current practice. If the current practice does not meet the requirement, the next column provides an area to document suggested action items or initiatives to mitigate the identified gap.

The assessment matrix, once the audit is completed, should be easily viewable and understandable by management and other decision makers. By providing a clear view of how the organization aligns with accepted standards, it is easier to make arguments for improvement initiatives. The next section outlines common areas of improvement when evaluating systems against BS 25999 and potential ideas on how to manage the gaps.

### 4.2. COMMON AREAS OF IMPROVEMENT

The most common areas of improvement noted during BCMS assessments stem from a lack of resources and time. It is a common theme that business continuity efforts do not receive the support and budget they require to operate at top effectiveness. As a result, business continuity professionals must prioritize efforts. The three efforts commonly yet incorrectly assessed as a low priority include training and awareness, document review and overall program maintenance. The following sections explain why these efforts are important and identifies ways to accomplish them with limited resources.

#### 4.2.1. TRAINING AND AWARENESS

Appropriate levels of training, for both BCMS personnel and employees, is an area that frequently does not receive the focus it deserves. Common training and awareness methods tend to be time consuming for both the trainer and the trainee. Because of this, training ends up at the end of priority lists and is usually ignored.

However, training and awareness activities are one of the most value-added efforts an organization can do, and it can be developed and delivered without being too time consuming and expensive. The key to minimizing cost with training development is to choose the most suitable delivery method. Figure 9 displays a set of most commonly used training delivery methods, and the type of content they are best used for. By matching the appropriate delivery method with your learning objectives, size of audience, frequency of instruction and content change, you can minimize the time it takes to deliver and maintain your training materials.

Delivery Method	Content Complexity	Size and Geographic Distribution of Audience	Frequency of Instruction	Frequency of Content Change
<b>Live (In-Person) Training</b>	Highly complex content	Small, concentrated audiences	Low	High
<b>Web-based Live Training</b>	Highly complex content	Smaller, dispersed audiences	Low	High
<b>Self-led Computer Based Training</b>	Complex content	Large, dispersed audiences	High	Low
<b>Interactive Group Training</b>	Complex content	Small, concentrated audiences	Low	High
<b>Hard Copy Documentation</b>	Detailed content that's not too complex	Medium to large audience – geography independent	High	Low
<b>Web-based Documentation</b>	Detailed content that's not too complex	Medium to large, dispersed audiences	High	High
<b>Physical Reminders (e.g., stickers and magnets)</b>	Not complex	Medium to large audience – geography independent	High	Low

Figure 9

An example of choosing the most appropriate delivery method is when a large financial institutional chose to develop web-based self-driven training modules to educate their branch managers on how to document response plans for their facilities. In contrast, the organization also chose to distribute magnets outlining the emergency notification system process to every employee so that they could keep them at their homes in the event of an incident occurring during non-working hours.

When it comes time to make decisions on what training objectives deserve more time and expense, an organization has a very large variety of specific training delivery methods to choose from, above and beyond the categories of types displayed in figure 9. Figure 10 outlines an exhaustive listing of both common and unique training methods. The table provides a description of how the method can be used and the level of cost and time it requires to develop and implement.

Solution Name	Solution Description	Cost Estimate (\$ to \$\$\$\$\$)	Time Estimate (T to TTTT)
<b>Exercises</b>	Although business continuity professionals may not categorize exercises (or tests) as a training and awareness tool, there is no better way to expose response and recovery personnel to business continuity in a sterile environment.	\$\$	TTTT
<b>Drills / Walkthroughs</b>	Building evacuations and shelter-in-place drills are important life safety activities (and are often mandated by local regulations). Integrate these drills with other business continuity training and utilize the downtime and heightened awareness of need during these drills. Some business continuity teams take the opportunity to provide hand outs and other information to employees while they wait to return to the building during evacuation drill.	\$	TT
<b>Skill Based Training (hands on)</b>	Organize hands-on training to address more complex skills, including BIA participation, plan documentation, first aid performance, call tree execution and crisis communication execution.	\$\$	TTTT
<b>HR Orientation Participation</b>	Deliver a 15 minute presentation during new hire orientation. Alternatively, ask Human Resources to ensure new employees access a computer-based new hire orientation presentation.	\$\$-\$\$\$	TTT- TTTT
<b>On-line Awareness Courses</b>	The business continuity professional's time is limited. Consider building computer-based, multi-media awareness presentations covering key business continuity topics. Post a link on the business continuity team's intranet site and encourage employees to visit. This is particularly useful for annual "refresher" awareness presentations and new hire orientation programs.	\$\$\$	TTTT
<b>"Multiple Choice Tests" and Surveys</b>	Measure knowledge and awareness using an on-line survey. Demand 100% participation and provide links to additional sources of information so that participants who "miss" a question know where to find information on the subject. When paired together, surveys and computer-based training are very effective awareness tools.	\$\$\$	TTT
<b>Intranet Site</b>	Invest some time in developing and updating an intranet site, and post content regarding upcoming events, business continuity strategies and management testimonials. Some organizations create and maintain an externally-facing web site that employees can access during a crisis to obtain situation updates.	\$\$	TTTT
<b>Plan Documentation</b>	A simple form of awareness is disseminating (or providing access to) business continuity plan documentation to response and recovery team members in an easy to access manner. This also familiarizes team members with where to locate plans in the event of a disaster.	\$	T

## How to Deploy BS 25999

<b>User Guides</b>	Business continuity planning tools and software are used pervasively in medium to large organizations. Hands-on training is great, but user guides are an important component of the training and awareness process. Make sure end users know where to find them and that they are easy to understand. Store and disseminate in an electronic form so that they are easy to update and re-distribute.	\$\$\$	TTTT
<b>Magnets</b>	Create and distribute “refrigerator” magnets to employees. Include information that an employee may need when they are at home – how to get situation updates (crisis phone numbers and ghost web sites) and general business continuity strategy information.	\$\$	T
<b>Media Handling Training</b>	Organize and provide media handling training to business executives, particularly members of the crisis management team. Familiarize them with the tools available during a crisis and how to access them (e.g. contracted external PR firms, template situation updates, and local media contact information)	\$\$	TTT
<b>Effectiveness Reporting</b>	Effectiveness measurement and reporting processes are a form of awareness? They are a form of awareness geared toward executive management. Develop an effectiveness measurement process and post the results on your intranet. Present the results to executive management on a quarterly or semi-annual basis.	\$	TTTT
<b>Reminder Placards</b>	Place business continuity reminders on employee bulletin boards. “Tips of the Month” can be effective and remind people that business continuity is a 24/7/365 program.	\$	TT
<b>“Booths”</b>	A number of organizations provide awareness exhibits during companywide meetings (or even in the cafeteria). Provide hand-outs and “give-aways”, place stickers on the back of employee ID cards and discuss the business continuity program with interested parties.	\$	TT
<b>Wallet Cards</b>	A small laminated card summarizing key responsibilities and contact information needed during a crisis is a common awareness tool. This “tool” is often limited to members of an executive management team, but can be provided to all employees in a scoped down manner.	\$	TT
<b>“Evacuation Bags”</b>	Business continuity teams are beginning to outfit employees with a small emergency response bag containing key supplies that may prove useful during a building evacuation or a shelter-in-place situation.	\$\$\$\$\$	TT
<b>Stickers on the Back of Badges</b>	A very simple concept – most organizations have building access badges or company identification cards. Place a sticker or print business continuity-related information on the back, to include crisis phone numbers, ghost web sites and building evacuation rendezvous points.	\$\$	T
<b>Conference Participation</b>	Conferences (and local business continuity associations like the Association of Contingency Planners) are excellent sources of information on new and emerging business continuity trends. Unfortunately, the content is tailored to business continuity and other risk management professionals; therefore the applicability of this “tool” is limited to your business continuity team. Some key business continuity conferences include Continuity Insights and Disaster Recovery Journal (DRJ) Fall and Spring World.	\$\$\$	TTTT

Figure 10

**4.2.2 REVIEW OF DOCUMENTATION**

Organizations with limited business continuity resources tend to conduct analysis and plan development efforts but later neglect to revisit them. However, nearly all business continuity standards, including BS 25999, require the review and maintenance of analysis and plan documentation as business and technology changes occur. Organizations change over time, including the personnel, their business processes, the resources that they use, and the customers they serve. All of these changes require modifications to analysis and planning, and thus documentation should be reviewed and updated on a regular schedule.

*“Organizations that do not have the resources to implement a document repository have found that developing a process around updating documents serves as an effective solution, though it requires strict monitoring by the business continuity team.”*

The first step in ensuring that documentation is properly maintained is to ensure policy defines the required documents, appropriate review cycle and responsible parties. By communicating a standard timeframe, personnel will be aware of expectations and make the time to perform their responsibilities. The second step is establishing a way to manage and track document changes. This can be completed simply by adding a revision block to each document (as shown in Figure 11) or by implementing a document repository. Organizations that do not have the resources to implement a document repository have found that developing a process around updating documents serves as an effective solution, though it requires strict monitoring by the business continuity team.



The process side of document management is key and can be highly time consuming to implement properly. One warehousing and distribution company requires that all revised documents are emailed to a central administrator after they document who made and approved the changes in the signature block. The central administrator ensures that the signature block is complete, documents in a register that the plan was updated and notes the date. The central administrator is then responsible for printing the plan and distributing it to the applicable parties as well as saving the new version to the proper location.

DOCUMENT NUMBER	REVISED BY	REASON FOR REVISION	APPROVED
1	Bob Smith (Plan Owner)	First Version – n/a	<i>Susanne Lybert</i>
1.1	Ann Horner (Administrative Assistant)	Personnel Contact Information Update	<i>Susanne Lybert</i>
2	Bob Smith (Plan Owner)	Annual Review	<i>Susanne Lybert</i>

Figure 11

**4.2.3 PROGRAM EVALUATION**

Evaluating a business continuity management system provides an analysis on how effectively and efficiently the program is meeting its objectives. BS 25999 requires that a regular review be conducted through either self-assessment or audit. However, as with the previously discussed areas for improvement, most organizations don't think that they have the time or resources to undertake such an effort.

*“Program evaluation does not have to be a time consuming effort. Some organizations choose to develop a self-assessment scorecard that planners can complete on their own.”*

Program evaluation does not have to be a time consuming effort. Some organizations choose to develop a self-assessment scorecard that planners can complete on their own. See Figure 12 for an example of this type of assessment tool. The scorecard can cover specific tasks that planners are responsible for completing, if they completed it and how much effort it took. It can also evaluate how effectively plans or analysis covered key areas. The easiest method to bring the assessment up to a corporate level is to design the card so that it uses a numbering system that can provide an overall score per plan, per facility, per organizational unit and for the entire organization. If the resources are available, it is also possible to implement a review of the self-assessments by business continuity professionals, either within the organization or subject matter experts outside of the organization.

<b>BCP Scorecard</b>	<b>Date: 8/17/07</b>	<b>Function: Vendor Mgt.</b>	<b>Evaluator: Joe Wells</b>
<b>Requirement #</b>	<b>Requirement</b>	<b>Score (1-10)</b>	<b>Reasoning</b>
1	The BIA was reviewed by each key process owner.	7	The BIA was revised by Joe, but other process owners did not participate. It was assumed that Joe could provide all of the input that was necessary.
2	The BIA defines both the most likely and most severe risks to the function and proposed plan to mitigate.	3	The BIA defines two key risks, however they are high level and have no mitigation plans.
<i>Total Score (out of a potential 100)</i>		<b>67</b>	Yellow – this function is below the preferred level of preparedness. Prepare mitigation plans and provide to the business continuity team for review and input.

Figure 12

### 5. TAKING THE NEXT STEP: THE CERTIFICATION PROCESS

Certification of compliance with BS 25999 is demonstrated by assessment against BS 25999-2 (the Specifications). Like all other certifiable international standards, BS 25999 Certification will require a thorough assessment process to ensure the organization has properly documented and addressed all the elements of the standard and the BCMS is operating effectively.

While the formal certification process has not been approved and published, as of the publication of this paper, it is expected that due to the adoption of ISO 17021 audit guidelines, BS 25999 will follow a process similar to ISO 27001 and is expected to be available in winter 2007.

Certification audits must be carried out by “uninterested third parties” (no conflict of interest) who are accredited by a neutral international accreditation body such as UKAS (United Kingdom Accreditation Service).

#### Initial evaluation of organizational scope

The certification process begins with an understanding of the organization and its BCMS implementation. In order to do this, a request for information should be submitted to BSI. Information will then be gathered about the organization through a company profile and an interview to ensure BSI understands the organization and risks involved. In response to the RFI, a project plan will be submitted with the detailed steps, audit days required and costs involved. A certification plan is sent back to the organization, then the approved plan and application for certification are submitted to BSI.

*“BS 25999 Certification will require a thorough assessment process to ensure the organization has properly documented and addressed all the elements of the standard and the BCMS is operating effectively.”*

Once the application for certification is submitted and approved by BSI, the assessment cycle can be scheduled and carried out.

#### Assessment Cycle

Due to the nature of business continuity, the assessment cycle will be based upon an initial assessment, followed by an annual surveillance visit and reassessment in the third year. It is expected that like ISO 27001, the initial assessment will be broken-up into two stages. The following sections detail the process and objectives of the each of the four types of assessments: Pre-Assessment, Initial Assessment, Surveillance Audit and Reassessment.

#### Pre-Assessment

The option of a pre-assessment visit will be a feature of the BS 25999-2 certification approach. A pre-assessment is a scaled down onsite assessment with the prime purpose of giving the organization an impression of their state of readiness for the full assessment. The client can request a specific audit plan for their pre-assessment. In the absence of this, BSI will carry out the pre-assessment based on best practices and a sampling of some critical elements of the standard. A pre-assessment will typically consist of a brief review of the entire BS 25999-2 set of requirements to ensure that the organization has addressed all aspects of the Specification. Any areas of doubt or omission will be documented in a report to the organization. Nonconformities will not be raised at pre-assessment visit. At the conclusion of the pre-assessment, a written report will be left with the organization detailing the findings.

Business continuity professionals will then have to ascertain how much remediation effort needs to be performed and the resources/ time required to complete these tasks. Once completed, BSI will commence with the initial stages of the audit. The pre-assessment audit cannot be taken into consideration during the initial assessment and all elements of the standard must be covered by the auditor(s).

### Initial Assessment

As mentioned above, due to the adoption of ISO 17021, it is expected that the initial assessment will be done in two stages.<sup>1</sup>

#### Stage 1

The following aspects will be covered:

- Review of the organization's BCMS documentation
- High level evaluation of the organization's readiness for stage 2 assessment
- Review the organization's understanding of the requirements of the standard
- Understanding of the proposed scope of the stage 2 assessment
- Review and confirm the resources needed for the stage 2 assessment
- Plan the stage 2 assessment
- Ensure that Management Reviews and audit/self assessments are being planned and performed

Any areas deemed not in compliance will be raised as nonconformities and must be cleared and approved by the lead auditor prior to moving into the Stage 2 phase of the certification audit.

#### Stage 2

The purpose of the stage 2 audit is to evaluate the implementation, including effectiveness, of the organization's BCMS.

This phase is carried out using the "process audit" approach.

Unlike a "checklist" approach, the audit approach assesses all processes included in the scope of

operation and all linked processes to ensure effectiveness and consistency. This will include interviews with the stakeholders, gathering of "objective evidence" (procedures, reports and test results) and evaluating those findings against the standard.

Any areas deemed not in compliance and/or effective will be raised as nonconformities and must be cleared and approved by the lead auditor prior to being recommended for certification.

*"Any areas deemed not in compliance and/or effective will be raised as nonconformities and must be cleared and approved by the lead auditor prior to being recommended for certification."*



### Surveillance Audit

The first surveillance visit is typically planned to take place yearly after the date of the stage 2 audit.

BSI will perform periodic monitoring audits of the certified organization's BCMS. Typically, an organization may be visited for such an audit once a year. The purpose of these monitoring audits is to verify the certified organization's continued compliance with certification requirements.

---

<sup>1</sup> All steps noted are typical accepted practice based on ISO 17021 and subject to revision at anytime.

Surveillance audits typically cover critical activities that ensure continuous improvement and effectiveness such as:

- Management review and audits/self assessments
- Review of actions taken on nonconformities from previous audits
- Effectiveness of the BCMS
- Progress of planned activities aimed at continual improvement
- Verifying the effective interaction among all BCMS elements
- Continuing operational control
- Review of any changes
- Use of marks and any other reference to certification
- Verifying a demonstrated commitment by the organization to maintaining the BCMS effectiveness

*“The standard can be used as a framework so that those organizations without a BCMS can efficiently establish a workable program, and those that already have a program can ensure it meets best practices where applicable.”*



### Reassessment

The purpose of the reassessment audit is to confirm the continued conformity and effectiveness of the BCMS and its continued relevance and applicability for the scope of certification.

The reassessment audit will typically include the following aspects:

- The effectiveness of the BCMS in its entirety in the light of internal and external changes and applicability to the scope of certification.
- Demonstrated commitment to maintain the effectiveness and improvement of the BCMS in order to enhance overall performance.
- Whether the operation of the certified BCMS contributes to the achievement of the organizations policy and objectives.

## 6. CONCLUSIONS

BS 25999 establishes the processes, principles and terminology to address business continuity and availability risk. It also provides a comprehensive set of controls based on industry leading practices that help organizations develop, implement, maintain and mature business continuity processes. The standard can be used as a framework so that those organizations without a BCMS can efficiently establish a workable program, and those that already have a program can ensure it meets best practices where applicable.

The growing consensus regarding BS 25999, combined with the opportunity to become certified in its use, provides unparalleled benefits to companies of all sizes whose customers rely on their products and services.

### Summary of Benefits

<p><b>Framework</b> Provides a common framework, based on international best practices, to manage business continuity.</p>	<p><b>Supply-Chain</b> Ensures that every company in the supply chain understands and consistently applies guidelines and standards consistent with your requirements.</p>
<p><b>Resilience</b> Proactively improves resiliency efforts when faced with disruptions to key value streams.</p>	<p><b>Competitive Advantage</b> Contributes to the opening of new markets through demonstration of compliance with best-in-class standards.</p>
<p><b>Management</b> Delivers a proven response methodology for managing a disruption.</p>	<p><b>Delivery</b> Provides a rehearsed method of restoring an ability to supply critical products and services to an agreed level and timeframe following a disruption.</p>
<p><b>Reputation</b> Helps protect and enhance the organization's reputation and brand.</p>	<p><b>Business Improvement</b> Enables a clearer understanding of how the entire organization operates on a day-to-day bases, which can identify opportunities for improvement (including personnel and knowledge deficiencies and single points of failure).</p>
<p><b>Compliance</b> Demonstrates that applicable laws and regulations are being observed.</p>	<p><b>Cost Savings</b> Creates an opportunity to reduce the burden of internal and external business continuity audits and may reduce business interruption insurance premiums.</p>

### ABOUT AVALUTION CONSULTING



Avalution Consulting is a leading provider of business continuity consulting services and specializes in program startup and increasing program maturity. We differentiate ourselves by taking a holistic view of the business, with a focus on limiting the probability of a business interruption and working to limit event

impact should it occur. We offer clear, unique perspectives that contribute to the protection of your business' key value streams. We design comprehensive continuity strategies and plans characterized as efficient and easily maintained, and deliver related services to ensure they remain viable and current.

Our clients include both the largest global organizations, as well as smaller firms in emerging markets. Our clients operate across numerous industries including banking, insurance, pharmaceutical products, legal, utilities, education, manufacturing, consumer products, healthcare, professional services and government. Many of our clients maintain established, proven business continuity programs, while others are just beginning to address the business risk associated with crisis events and downtime. Regardless of size, program maturity or industry focus, Avalution is positioned to help realize your business continuity objectives.

For additional information regarding our professionals, tools and solutions please contact us at 800.941.0381 or via email at [contactus@avalution.com](mailto:contactus@avalution.com).

### ABOUT THE AUTHORS

#### Robert Giffin

Rob is a Managing Consultant and co-founder of Avalution Consulting. He specializes in the establishment of response and recovery programs in the manufacturing, healthcare and consumer products industries, as well as in government.

Rob currently serves as an officer with the Northern Ohio chapter of the Association of Contingency Planners (ACP). He is a member of the Disaster Recovery Institute, Project Management Institute and IS Audit and Control Association. He has published numerous articles and is an accomplished speaker. Rob can be reached via email at [robert.giffin@avalution.com](mailto:robert.giffin@avalution.com).

#### Susan Yardis

Susan is a Senior Consultant with Avalution Consulting. Susan has four years of business continuity experience delivering crisis management, crisis communications, business resumption and IT disaster recovery solutions. Additionally, Susan focuses on training and awareness development for clients in a variety of industries, particularly mature financial services companies as well as those just starting their BCM effort.

Susan is an active member of the Northern Ohio Chapter of ACP. She is also a member of the Disaster Recovery Institute, IS Audit and Control Association and the Institute of Internal Auditors. Susan's most recent publication is titled *Designing a Business Continuity Training Program to Maximize Value & Minimize Cost*. Susan can be reached via email at [susan.yardis@avalution.com](mailto:susan.yardis@avalution.com).

### ABOUT BSI MANAGEMENT SYSTEMS



BSI is the world's leading management systems certification body. Founded in 1901, BSI has certified more than 60,000 locations in nearly 90 countries. Many 'Global 500' companies have chosen BSI as their preferred ISO 9001:2000, ISO/TS 16949:2002, ISO 14001:2004 or ISO/IEC 27001:2005 certification body. BSI's certification experience covers virtually every industrial and commercial sector (i.e. automotive, aerospace, chemical and allied processes, IT/software, and service). BSI Management Systems America, Inc. is headquartered in Reston, Virginia, with offices in Toronto, Canada, and Mexico City, Mexico to serve the North American market. BSI is truly a pioneering organization.

For further information about BSI Management Systems, please visit [www.bsiamericas.com](http://www.bsiamericas.com)

### ABOUT THE AUTHOR

#### **John A. DiMaria; Certified Six Sigma BB; HISP**

John DiMaria, is the BSI (British Standards Institution) Americas Product Manager of Business Continuity specializing in BCMS, ISMS and ITSM standards. John is a Certified HISP (Holistic Information Security Practitioner) and Six Sigma Black Belt and donates his expertise as a Board Member of the HISP Institution.

He has 24 years in the industry specializing in Information Security, Management System Analysis and Improvement, Regulatory Analysis and Compliance, Risk Assessment and Management, Failure Mode Investigation and Six Sigma strategies on both a national and international level.

Previously he served as a Managing Consultant of Information Security for LECG, LLC a global expert services firm. Spent 4 years as member of the Board of Directors for a multi-million dollar corporation in St. Louis Missouri and prior 16 years managed implementation of SPC, Regulatory Affairs, process controls, information systems and international management systems standards.

John serves on committees that influence legislation and drive international harmonization such as the CSIA (Cyber Security Industry Alliance) and the BITS Shared Assessment Program. He has been featured in many publications such as Computer World, Quality Magazine, QSU, SC Magazine and Campus Technology concerning various topics regarding information security and business continuity.