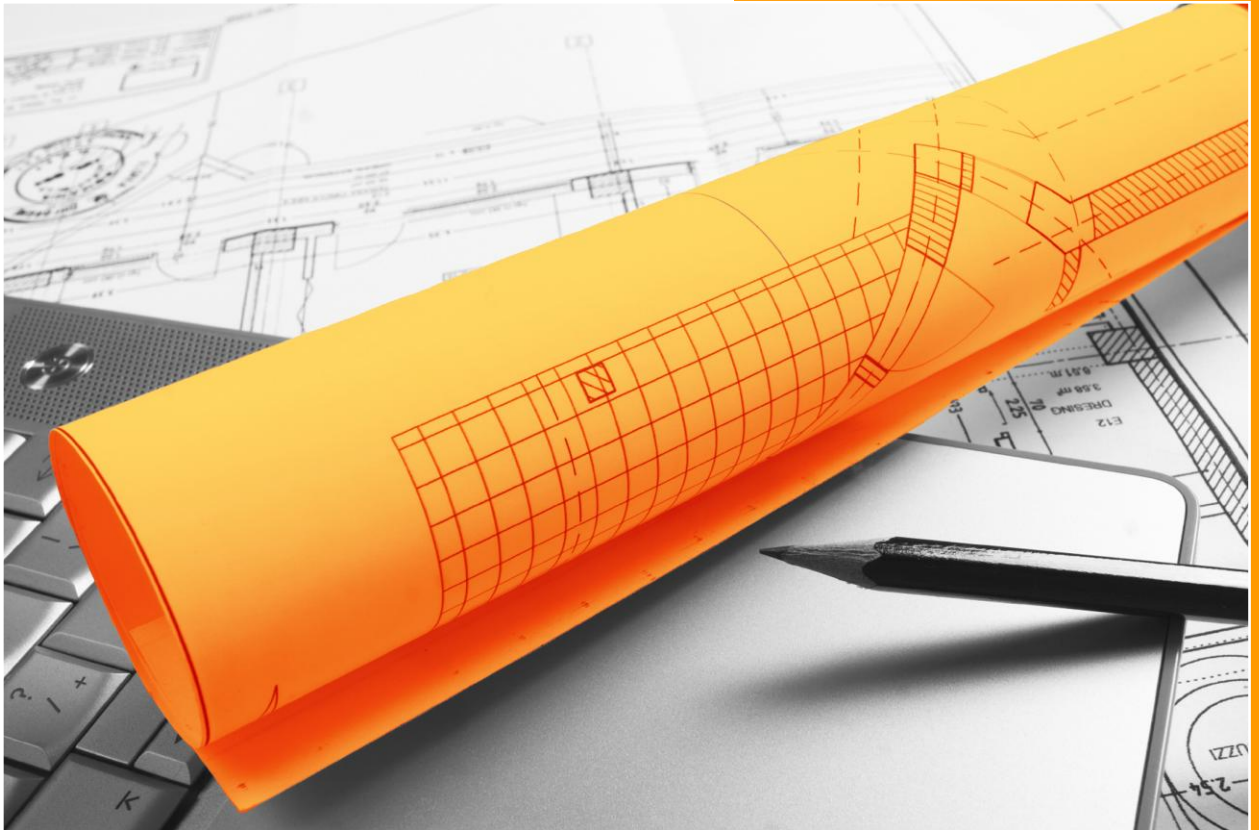


How to Deploy BS 25999

second edition



**Authored By Avalution Consulting and
BSI Management Systems America**

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. *Planning the BCMS* 7

 3.2.1. Program Requirements 7

 3.2.2. BCM Policy..... 7

 3.2.3. Provisioning Resources and Competency of Personnel 7

 3.2.4. Embedding BCM..... 8

 3.2.5. Documentation and Records..... 8

 3.3. *Implementing and Operating the BCMS* 9

 3.3.1. Understanding the Organization 9

 3.3.2. BIA and Risk Assessment 9

 3.3.3. Business Continuity Strategy 11

 3.3.4. Planning Activities 13

 3.3.5. Exercising and Maintaining BCM Arrangements 15

 3.4. *Monitoring and Reviewing the BCMS* 16

 3.4.1. Internal Audit 16

 3.4.2. Management Review 16

 3.5. *Maintaining and Improving the BCMS* 17

 3.5.1. Preventive and Corrective Actions 17

 3.5.2. Continual Improvement 17

4. KEY PROGRAM IMPROVEMENT OPPORTUNITIES..... 18

5. TAKING THE NEXT STEP: THE CERTIFICATION PROCESS 19

6. CONCLUSIONS 22

ABOUT AVALUTION CONSULTING..... 23

ABOUT BSI MANAGEMENT SYSTEMS..... 23

This second edition of “How to Deploy BS 25999” addresses changes to the BS 25999-2 Specification, finalized in late 2007, after the initial release of the white paper. This edition also takes advantage of lessons learned from recent BCMS development projects designed to meet BS 25999 requirements.

1. INTRODUCTION

Business continuity programs, similar to other enterprise risk management 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 both credibility and viability to a continuity program. This white paper explores a new international code of practice (and its associated specification document), the British Standard Institution's British Standard (BS) 25999, viewed by a growing body of practitioners as a complete description of a mature, repeatable and actionable business continuity management 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 and/or increase the maturity of an existing program.

BS 25999 provides a basis for understanding, developing and implementing business continuity within an organization, integrates risk management disciplines and processes with business continuity and provides confidence in business-to-business and business-to-customer dealings. BS 25999 is written in two parts. Part 1, the Code of Practice, outlines the standard's overall objectives, guidance and recommendations. Part 2, the Specification, details the activities that should be completed in order to meet business continuity objectives within the context of an organization's risk management philosophy. Part 2 is designed to be "auditable", meaning only objective, measurable requirements are included in the Specification.

Background: From Business Continuity Planning to a 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 also matured. A few years ago, business continuity planning (BCP) was the latest term to articulate the growing role continuity played in protecting critical business processes from failure. As this practice grew and established itself as a key risk management discipline, a movement toward standardization 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

"The purpose of BS 25999 is to provide a basis for understanding, developing and implementing business continuity within an organization..."

continuity, resulting in a new term: Business Continuity Management System (BCMS). While BCMS sounds like some new class of pricy business continuity 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 holistic systems thinking.

Support Grows for BS 25999 Internationally

Prior to formal publication, most draft British Standards draw an average of 250 downloads. BS 25999-1 (the Code of Practice), however, logged some 5,000 downloads, twenty times more than normal. This extraordinary number of downloads demonstrates how important this issue is to a large number of organizations. Additionally, since the release of BS 25999-2 (the Specification) in November 2007, over 4,000 copies have been purchased. Another important consideration is that two of the largest American insurance brokerages, Aon Corporation and Marsh Inc., 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 from the U.S. insurance industry. It is a benefit to insurance providers if they can persuade their customers to develop and maintain a strong, viable BCMS; business interruption-related risk decreases, thereby decreasing claim payments.

As you read this white paper, 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).

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:

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 risk analysis and 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 key components of an internationally-accepted business continuity management system, as well as how to achieve key risk management objectives?
6. Does the standard focus on program development, long-term program management and continuous improvement?

2.2. HOW BS 25999 ANSWERS THESE QUESTIONS

BS 25999 provides an organization with guidance and details necessary to build and improve its BCMS. Read the following statements 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 a program on key activities designed to increase responsiveness, resiliency and recoverability. BS 25999 provides a straightforward framework and specification to follow and focuses attention on the most critical business activities. When developing a business continuity program, it is essential to know the differences between a business continuity management system and a business continuity plan. Business continuity plans, by definition, are documents focusing solely on the recovery from an interruption, leaving the residual risks of an interruption occurring unmitigated. BS 25999 outlines a system to address and reduce the risk of an interruption occurring, as well as respond to the risks that occur following an interruption.
3. An organization should select a standard that reflects the entity's current approach to risk management. The standard should be geared to achieve risk management by assessing critical activities and objectives. 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 its 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 Specification to further understand the basic terminology used by BS 25999.

- Standards can be confusing, as many are generalized and provide only high-level explanations regarding outcomes. BS 25999 was developed in two parts, the Code of Practice and the Specification, to make the standard easier to understand and implement. Part 2, the Specification, sets out minimum objective requirements for an effective BCMS and provides a framework for its implementation, management and continuous improvement. It is written in such a way to enable compliance measurement. Part 1 of the standard outlines a “good practice”, moves beyond the minimum requirements and discusses risk management opportunities and methods of meeting business objectives.

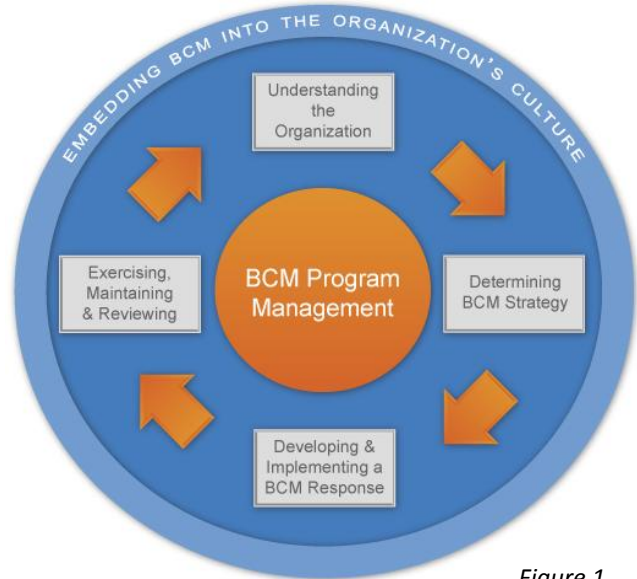


Figure 1

- BS 25999 outlines a BCMS continuous lifecycle approach to improvement, defining the system as a living and continuously evolving program. Figure 1 depicts this lifecycle.

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 Specification). By following this framework and the activities within each area, a business continuity professional can build a BCMS that aligns with BS 25999. This section of the white paper provides detail on various approaches to achieve BS 25999 compliance. This overview can provide a business continuity professional with a basic understanding of the BS 25999 content; however, the standard should be read to fully understand specific requirements.

3.1. AN OVERVIEW OF BS 25999

The BS 25999 Specification is organized into four main phases: Planning the BCMS, Implementing and Operating the BCMS, Monitoring and Reviewing the BCMS and Maintaining and Improving 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.

PLANNING THE BCMS

- Program Requirements** – identifying the scope and objectives of the BCMS, taking into account the organization’s strategic objectives, key products and services, risk tolerance, and any regulatory, contractual or stakeholder obligations
- BCM Policy** – documenting management commitment to the BCMS and the identified objectives and scope, setting out required review intervals and communicating the policy to all company employees
- Provision of Resources and Competency of Personnel** – allocating sufficient resources to implement, oversee and maintain the BCMS, including training required to increase and continue the competence of assigned resources
- Embedding BCM** – establishing ongoing awareness and role-specific training to ensure all employees understand the BCMS policy and objectives and their role in achieving the organization’s BCM objectives
- Documentation and Records** – developing the processes to manage the documentation and records created as a part of the BCMS to ensure completeness, availability, currency and security

IMPLEMENTING AND OPERATING THE BCMS

- a. **Business Impact Analysis** – determining the impact of a (threat-independent) disruption of critical organizational activities in order to assign recovery objectives
- b. **Risk Assessment** – understanding the threats and vulnerabilities to the organization’s critical activities and supporting resources
- c. **Determining Choices** – identifying risk treatments to mitigate risk by reducing the likelihood of an interruption, limiting its timeframe or reducing its impact
- d. **Determining Business Continuity Strategy** – defining how the organization will respond to and recover from disruptions, including relationships with key internal and external stakeholders
- e. **Incident Response Structure** – identifying personnel, developing plans and allocating resources to respond to incidents, trigger an appropriate business continuity response and communicate with stakeholders
- f. **Business Continuity and Incident Management Plans** – documenting how the organization will manage an incident and recover or maintain activities to a predetermined level
- g. **Exercising** – validating that plans and arrangements meet business requirements and generating action items to improve and update plans
- h. **Maintaining and Reviewing BCM Arrangements** – reviewing and revising BCM arrangements at defined intervals to ensure continuing suitability, adequacy and effectiveness

“It is important to note that BS 25999 is an international standard, not a European standard – which is a common misconception.”



MONITORING AND REVIEWING THE BCMS

- a. **Internal Audit** – ensuring that the organization conducts independent reviews of the BCMS at planned intervals to determine whether it conforms to planned arrangements, has been properly implemented and maintained, and meets the organization’s policy and objectives
- b. **Management Review** – reviewing the organization’s BCMS at planned intervals to ensure continuing suitability, adequacy and effectiveness

MAINTAINING AND IMPROVING THE BCMS

- a. **Preventive and Corrective Actions** – improving the BCMS through the application of preventive and corrective actions
- b. **Continual Improvement** – continually improving the effectiveness of the BCMS through the review of policy and objectives, audit results, analysis of monitored events, preventive and corrective actions and management review

After reading and fully understanding BS 25999’s requirements, the business continuity professional should determine the process necessary 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 four sections as section 3.1.

3.2. PLANNING THE BCMS

3.2.1. PROGRAM REQUIREMENTS

The first step in developing a BCMS is identifying scope and objectives, taking into account the organization's strategic objectives, key products and services, risk tolerance, and any regulatory, contractual or stakeholder obligations. To best understand these factors, one large manufacturing organization formed a steering 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. Establishing a steering committee not only provides business-wide consensus, but also demonstrates upper management commitment to the BCMS.

3.2.2. BCM POLICY

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 establish and demonstrate management's commitment to a BCMS and include the organization's business continuity objectives and the scope of the program. Additionally, a more detailed BCM manual (or standard operating procedure) should be developed to provide more detailed guidance in support of the organization's BCMS policy statement, including:

- Program definition and scope
- Analysis (business impact and risk assessment)
- Strategy definition
- Strategy implementation
- Program management

Actionable procedures, specific requirements and firm timelines should be documented for all required program elements.

“Establishing a steering committee not only provides business-wide consensus, but also demonstrates upper management commitment to the BCMS.”



3.2.3. PROVISIONING RESOURCES AND COMPETENCY OF PERSONNEL

While determining the resources necessary to implement, operate and maintain the BCMS, the optimal structure of the business continuity organization, including executive responsibility for BCMS oversight, should be identified. Some larger organizations have dozens of personnel dedicated to business continuity, in groups specializing in business continuity training, tool development and quality assurance. However, smaller organizations may have, at most, only one full-time person to address business continuity coordination. Whatever structure is used, it is important to determine what these roles will require and ensure that sufficient resources have been allocated to enable key activities to occur, including assessment, planning and exercising. It is also important to ensure that key personnel have the knowledge and background to perform these roles. Personnel should be evaluated and provided with any necessary training to ensure effectiveness, either internally or from an external source.

3.2.4. EMBEDDING BCM

All other employees, regardless of their role within the BCMS, need to receive a minimum level of information and role-specific training to ensure that the organization embeds business continuity into its routine operations and management processes. At a minimum, the training program should communicate to all employees the importance of meeting BCM objectives, conforming to the BCM policy and the need for continual improvement, as well as how they contribute to achieving BCM objectives. Potential training methods are highlighted in the following table (Figure 2), with a guide to their use and applicability.

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

Figure 2

3.2.5. DOCUMENTATION AND RECORDS

All aspects of the BCMS must be documented. The goal is to provide clear evidence of the effective operation of the BCMS and the organization’s implementation of business continuity strategies. Controls should be put in place, such as backup strategies for electronic records or off-site storage for physical records, to protect the records themselves, as well as to provide version control and a clear revision history. This can be completed simply by adding a revision block to each document (as shown in Figure 3) 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 and tracking changes to documents serves as an effective solution, though it requires strict monitoring by the business continuity team.

“Organizations that do not have the resources to implement a document repository have found that developing a process around updating and tracking changes to 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 documentation revisions be emailed to a central administrator after noting 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 Lyfert</i>
1.1	Ann Horner (Administrative Assistant)	Personnel Contact Information Update	<i>Susanne Lyfert</i>
2	Bob Smith (Plan Owner)	Annual Review	<i>Susanne Lyfert</i>

Figure 3

3.3. IMPLEMENTING AND OPERATING THE BCMS

3.3.1. UNDERSTANDING THE ORGANIZATION

Prior to beginning the analysis, strategy and planning effort, a key activity is determining the business units into which the organization will be divided for the purposes of analysis and planning. Some organizations, such as financial institutions, evaluate and plan for individual lines of business, such as commercial lending and retail operations. Other organizations, such as manufacturing companies, 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 way to start defining 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 who is responsible for continuity-related activities. As each business unit and owner is identified, the professional should document the initial scope and begin to involve each owner in the development of the BCMS.

3.3.2. BIA AND RISK ASSESSMENT

The business impact analysis enables an organization to identify the critical processes that support its key products and services, the interdependencies between processes and the resources required to operate the processes at a minimally-acceptable level. 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 the maximum tolerable period of disruption for each activity, as well as outline process/technology specific recovery objectives.

In order to facilitate this analysis, some organizations interview key subject matter experts for each business unit, collecting the key information via small group discussions. This information is documented so an overall analysis can be completed and presented to the BCMS steering committee. This works well for organizations that are smaller in size and have personnel to conduct the interviews. Although in-person interviews are one of the best methods for analysis,

“Prior to beginning the analysis, strategy and planning effort, a key activity is determining the business units into which the organization will be divided for the purposes of analysis and planning.”

some larger organizations, due to size, complexity and geographical dispersment 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 4.

Interviews	Surveys
Pros of each method	
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
Considerations if either method is chosen	
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, Section 4.1.1 of the BS 25999 Specification for detailed requirements as to 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 business unit. Present this report to the steering committee overseeing the BCMS for review, input and approval.	

Figure 4

Establishing and implementing a documented method for conducting risk assessments and identifying appropriate risk treatments is also an important element of BS 25999. An emphasis on risk treatment is one (significant) area where BS 25999 differs from most standards. Risk assessments should evaluate the likelihood of threats resulting in a business interruption for each analyzed business unit, and the corresponding severity of each threat’s potential impact. Risk assessment activities should also take into account the controls currently 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 to identify and prioritize proactive risk treatment activities. Risk treatments can take the form of mitigation activities, such as the installation of redundant equipment in key processes to reduce the likelihood of a disruption or maintaining security stock to reduce the impact of a disruption on the business’ customers. Other treatments, such as developing business continuity, emergency response and incident management plans, can reduce the period of a disruption to levels that are acceptable to the organization.

Similar to the business impact analysis, the risk assessment can be conducted utilizing an interview or survey format; however, the greatest efficiency and value is often realized in a workshop format that allows multiple subject matter experts to share perspectives on a threat, its impacts, controls and potential mitigation strategies. The risk assessment should focus on individuals who are most aware of the threats and controls within each unit, while the business impact analysis should focus on those with detailed knowledge of current-state process characteristics and the impact of the interruption caused by threat-independent outages.

In the context of a BCMS, an effective risk assessment approaches threats, impacts and controls from the perspective of critical business activities, as opposed to “traditional” risk assessments that focus on threats (storms, utility outages, etc.) and the vulnerability of the organization without reference to business impact. One potential risk assessment methodology, a sample of which may be found in Figure 5, focuses the analysis by first asking participants to think in terms of consequences – the “inability to produce” or “inability to perform” a critical product or service. For each process step identified, participants are encouraged to discuss how the step could be impacted and what the effect of the failure mode could be on critical processes. Once these elements have been established, workshop participants brainstorm potential causes of the failures and any controls currently in place to mitigate the risks. Finally, recommendations can be developed to address identified weaknesses. A ranking system can also be applied to the process to develop a relative order of threats and the value of potential mitigation activities.

Process Step	Potential Failure Mode	Potential Effects of Failure	Potential Causes of Failure	Current Controls	Recommended Actions
Inability to produce product	Unavailability of raw materials	Inability to source, locate or deliver key raw materials	<ul style="list-style-type: none"> • Loss of vendor • Backorder of key materials • Transportation interruption • Vendor discontinuation or specification change • Product recall 	<ul style="list-style-type: none"> • Identified single source suppliers • Safety stock of key single source raw materials stored onsite and at local offsite warehouse location 	Develop plans to split key inventory items between primary and offsite storage and provide ongoing monitoring
Inability to perform core business support activities	Inability to process payroll	<ul style="list-style-type: none"> • Inability to pay employees • Potential long term loss of employee loyalty 	<ul style="list-style-type: none"> • Loss of payroll vendor • Facility inaccessible • Loss of telecommunications capability • Loss of PC with payroll connectivity software 	Manual check processing of base pay amounts	<ul style="list-style-type: none"> • Establish alternate payroll submission method with ADP • Equip an additional PC (offsite) with proprietary ADP software for payroll submission

Figure 5

While BS 25999 does not prescribe a particular risk assessment approach, any approach selected must enable the organization to understand the threats to and vulnerabilities of its critical activities and supporting resources. It also must enable the organization to identify risk treatments to reduce the likelihood, duration or impact of a threat.

3.3.3. BUSINESS CONTINUITY STRATEGY

After requirements have been established through a business impact analysis and residual risk levels and appropriate risk treatments have been determined by a risk assessment, strategies can be developed to identify arrangements that will enable the organization to protect and recover critical activities based on organizational risk tolerance and within defined recovery time objectives. Strategies should be developed to establish an incident response and management structure, manage relationships with key stakeholders and external parties and recover critical business activities.

Response strategies enable management to react swiftly to an event, protecting people and resources, and efficiently evaluate the situation in order to trigger an appropriate business continuity response. Primary employee-focused response activities commonly include the procedures associated with an employee safety and facility evacuation program. Facility-focused response activities typically involve coordination with civil authorities, damage assessments and stabilization of resources to prevent further loss or damage. Incident management (also referred to as crisis management) plans focus on facilitating the business recovery process and communicating with stakeholders, both internally and externally.

The development of business continuity strategies is best understood by focusing on critical activity recovery objectives and the resources required to facilitate recovery. A list of resources and their recovery objectives, developed during the business impact analysis, serve as the basis for considering which methods fulfill recovery requirements. 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 6 for a listing of resource types and the most common strategies that organizations consider for business recovery.

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

Figure 6

Overall, business continuity professionals develop strategies to minimize risk in line with organizational tolerances and to satisfy recovery objectives. 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 strategies and document plans.

3.3.4. PLANNING ACTIVITIES

Planning is the activity that many new business continuity professionals focus on because it is most familiar (and the most obvious “deliverable” from the business continuity process). However, as established in the BS 25999 standard, a significant number of essential tasks must take place before planning activities are possible. Planning should only occur after risk and impact analyses have been completed and resulting risk mitigation strategies are selected. The objective of planning is to provide the documentation to implement mitigation, response and recovery strategies that meet management-approved requirements.

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 essential to delivering critical products and services, or to ensure safety and meet regulatory requirements. Depending on the size and structure of the organization, the planning structure may be simple or complex. 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 fifty facility recovery plans and twelve country level management plans. A much smaller property 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. These are commonly referred to as emergency response and incident management (or crisis management) plans. These plans and associated strategies summarize the processes that a group of management-level personnel will complete in order to assess the impact of an incident, stabilize the situation, determine if recovery plans need to be implemented, assess priorities of recovery, provide resources for recovery and manage communications during the incident. This group of management personnel, commonly referred to as the incident or crisis management team, should represent all key decision makers across the organization. Figure 7 depicts a common list of team members and their primary responsibilities. An international lending firm used a similar incident 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 response and 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.

Incident/Crisis Management Team Members and Responsibilities

IMT/CMT Leader – holds primary responsibility for managing the recovery effort

Administration – provides administrative support to the IMT/CMT by screening communications, coordinating travel arrangements and maintaining a record of team activities and decisions

Human Resources/Internal Communications – coordinates all employee aspects of recovery, such as monitoring injured personnel, establishing working hours, managing payroll and benefit issues and communicating to internal stakeholders, including employees, employee family members and other internal stakeholders

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

Facilities – manages damage assessment efforts, provides liaison with emergency and municipal authorities, provides site security and manages site restoration effort

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 7

Basic Recovery Plan Content

1. Recovery Overview
 - 1.1. Recovery Objectives and Plan Scope
 - 1.2. Plan Owner and Revision Date
 - 1.3. Recovery Strategies
2. Dependencies/Requirements
 - 2.1. Internal Processes
 - 2.2. External Providers
 - 2.3. Applications
 - 2.4. Equipment
 - 2.5. Documents/Data
 - 2.6. Resource and Facility Needs
3. Contact Information/Communications Procedures
 - 3.1. Internal
 - 3.2. External
4. Recovery Teams and Roles
5. First Alert Response Procedures
6. Recovery Procedures
7. Restoration Procedures

Figure 8

Once a planning structure is in place, it is important to determine who will be the responsible plan owner and who will be accountable for documenting and maintaining the plans. Frequently, 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 develop actionable recovery plans, as well as sufficient training to adequately perform the tasks. The best way to start any planning effort is to establish a plan template or worksheet and introduce it to plan owners during individual or group training sessions.

A plan template provides a business unit planner with instruction, a starting format and the key sections to be documented. It also provides consistency 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 8.

3.3.5. EXERCISING AND MAINTAINING BCM ARRANGEMENTS

Exercising is the process of validating plan content to ensure strategies are capable of providing response and recovery results within the timeframes agreed to by management. Exercising can also provide training to the personnel responsible for response and recovery activities, as well as pinpoint plan weaknesses, areas for improvement and areas where BCM arrangements have become dated (and potentially ineffective).

Exercising can occur in many forms. Each form has a cost and benefit that typically is directly related to complexity (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 enable recovery and if the established timeframes are achievable. A much simpler exercise is testing an emergency notification process. Most organizations implement strategies to notify employees in the event of a disaster or business interruption. This can 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 call tree process. A simple test would be to implement the communication chain. Figure 9 shows a matrix of exercise types and which plans or activities they work best with. Figure 9 also lists the cost-benefit trade off for each type of exercise, noting that the easier to implement exercise types often have less strategic value.

Exercise Type	Best Use	Cost-Benefit
Plan Walkthrough – 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	<ul style="list-style-type: none"> • Easiest and least time consuming • Provides the least amount of value in terms of proving response and recovery capabilities
Table Top – 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	<ul style="list-style-type: none"> • Fairly easy to prepare for and perform • Provides a good initial validation of a plan
Process or Plan Simulation – using a scenario to guide the acting or carrying out of 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	<ul style="list-style-type: none"> • More difficult to prepare for, sometimes costly if it involves an external provider • Provides a more “real-life”, actionable test
Full (End-to-End) Simulation – using a scenario to enable participants to carry 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	<ul style="list-style-type: none"> • Most difficult to prepare for and perform due to the large number of participants for an extended period of time • Best test of strategies and plans

Figure 9

Regardless of the type or complexity of exercises, it is important to document how often plans and processes will be exercised and to document objectives and lessons learned to ensure efforts are made to resolve issues and errors. Developing even the simplest exercise documentation template, with sections such as exercise objectives, outcomes and follow-up action items, can formalize the exercise process, provide assurance that exercises are being conducted and provide program validation and maturation value, both of which are crucial to top management and boards of directors to maintain support and demonstrate recoverability.

3.4. MONITORING AND REVIEWING THE BCMS

3.4.1. INTERNAL AUDIT

In order to ensure that an entity’s BCMS remains current and effective (and consistent with management expectations), BS 25999 mandates a regular review of BCMS components and the overall suitability and effectiveness of the entire program. Detailed reviews are usually conducted through a formal internal audit process that is designed to determine whether the BCMS:

- Conforms to planned arrangements for BCM, including requirements of the standard
- Has been properly implemented and is maintained
- Is effective in meeting an organization’s BCM policy and objectives

A typical audit program for BS25999 can be divided into the five main areas of the business continuity lifecycle:

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 10 to see an example of this type of matrix audit format.

Audit #	Requirement Source	Requirement	Current Practice	Recommendations
1	BS 25999 – BCM Program Management	The organization assures 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 specifies business continuity expectations.	Develop a policy that covers all applicable business continuity efforts, roles, responsibilities and timeframes.

Figure 10

3.4.2. MANAGEMENT REVIEW

A regular review of an entity’s BCMS by management, typically the BCM Steering Committee, is required. While BCM policy, scope and objectives can be reviewed directly to validate continuing suitability, adequacy and effectiveness, details regarding the update and compliance of the BCMS are best presented in a consolidated format. The easiest method to bring the information up to a corporate level is to design a scorecard that includes each cyclical activity including BIA reviews, plan updates, exercise activities and application of any necessary corrective actions. The scorecard should employ a numbering system that provides an overall score per planning group, per facility, per organizational unit and for the entire organization. Figure 11 provides one potential scorecard format.

BCM Scorecard	Date: 8/17/07	Function: Vendor Mgt.	Evaluator: Joe Wells
Requirement #	Requirement	Score (1-10)	Reasoning
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>		67	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 11

3.5. MAINTAINING AND IMPROVING THE BCMS

3.5.1. PREVENTIVE AND CORRECTIVE ACTIONS

In addition to exercising, auditing and reviewing the BCMS, it is important to ensure that lessons learned, identified issues and organizational changes be incorporated into the BCMS. Preventive actions are most often identified through the regular review of BCMS documentation. Accommodating changes in an entity’s organizational structure, physical plant, customer base or products could necessitate a change in program scope, objectives, or arrangements. Corrective actions, most often brought to light by audit non-conformities or serious gaps in exercise performance, must be tracked to ensure that required program enhancement and maturation activities are occurring.

3.5.2. CONTINUAL IMPROVEMENT

The BCMS is a living system and continual improvement is necessary to achieve full value. Management must ensure the commitment shown in developing a BCMS is maintained through the ongoing review of the business continuity policy and objectives, audit results, analysis of monitored events, preventive and corrective actions and management review.

4. KEY PROGRAM IMPROVEMENT OPPORTUNITIES

Many organizations with business continuity programs struggle to achieve full value from their effort. Programs often fail to meet management requirements and expectations, minimally integrate with other corporate risk management initiatives, or fail to stay current and become ineffective due to a lack of regular attention. Through extensive client interaction and an ongoing BCM assessment program, Avalution identified several consistent areas of weakness when comparing current-state business continuity programs to the BS 25999 Specification.

1. BCM Governance and Risk Management Integration

In many organizations committed to business continuity, BCM programs have matured over time from disaster recovery programs or isolated business continuity efforts at a departmental or facility level. These programs often lack an overall business continuity policy, or the details necessary for appropriate governance and management oversight. Programs without comprehensive corporate policies also show a lack of integration with other corporate initiatives, particularly those involving other areas of operational risk management. Sections 3.2.1 and 3.2.2 discuss BS 25999 program and policy requirements and make the case for governance structures to drive repeatability and continuous improvement.

2. Management Involvement and Review

Often, business continuity responsibility in an organization is assigned at a level that does not have regular exposure to senior management, let alone strategic decision-making. Decisions regarding program direction and program performance monitoring occur at the business unit or facility level, leading to a program that is inconsistent both in its design and execution. Also, a lack of senior management involvement and support reduces the profile and urgency of the program. Section 3.2.1 discusses management involvement and sections 3.4.1 and 3.4.2 discuss program monitoring and review.

3. Focus on Proactive Risk Assessment and Treatment

Business continuity programs, especially those that have existed for some time, focus almost exclusively on reacting to and recovering from an event. Even those programs that focus on “resiliency” as opposed to recovery are still heavily focused on reactive controls. Additional value can be achieved through more proactive risk treatments and closer alignment of BCM with overall risk management objectives. Section 3.3.2 discusses business impact analysis and risk assessment activity requirements of BS 25999, and how strategies should include risk treatment, response and recovery.

4. Employee Training and Awareness

Many organizations spend a large amount of time, energy and money to define and document business continuity programs only to have them perform poorly when called upon during either an actual emergency or exercises, mostly due to a lack of knowledge specific to roles and responsibilities. Training, if there is an organized process, is often limited to incident/crisis management teams, technology recovery teams and possibly business recovery team leaders. The general employee population is often neglected, leading to an overall lack of knowledge specific to safety processes, recovery expectations and crisis communications. Section 3.2.4 discusses BS 25999 requirements for embedding BCM within the organization.

5. Continuous Improvement Processes and Evidence

Business continuity programs become outdated and fail to grow and mature without regular update processes. Yet many organizations, even those that conduct audits and exercises, fail to establish a process to utilize that information for program improvement. Audit recommendations, exercise lessons learned and action items, as well as gaps detected during management reviews, all provide guidance for preventive and corrective actions. Of equal importance, integration with organizational and technology change management efforts enables “real-time” program maintenance. Section 3.5.1 discusses maintaining and improving the BCMS. Exercises are discussed in section 3.3.5 and audit and review in sections 3.4.1 and 3.4.2.

5. TAKING THE NEXT STEP: THE CERTIFICATION PROCESS

BS 25999 compliance certification is demonstrated by independent assessment against BS 25999-2 (the Specification). Like all other certifiable international standards, BS 25999 certification requires a thorough assessment process to ensure the organization has properly documented and addressed all elements of the standard and that the BCMS is operating effectively and consistently.

The BS 25999 certification process follows ISO 17021 guidelines (*Conformity Assessment – Requirements for Bodies Providing Audit and Certification of Management Systems*).

Certification audits must be carried out by “uninterested third parties” (those with no conflicts of interest) who are independent and 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 (RFI) should be submitted to BSI. Information will then be gathered about the organization through a documented company profile and an interview to ensure BSI understands the organization and risks involved. In response to the RFI, BSI develops and submits a project plan with the detailed audit 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 requires a thorough assessment process to ensure the organization has properly documented and addressed all elements of the standard and that the BCMS is operating effectively and consistently.”

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

Assessment Cycle

The purpose of the assessment process is to confirm conformance to BS 25999-2 (the Specification). Due to the nature of business continuity, the assessment cycle will be based upon an initial assessment (broken up into two stages, stage one and stage two) followed by an annual surveillance visit and reassessment in the third year. A pre-assessment is an optional step in the process. 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 its state of readiness for the full assessment. The client can request a specific audit plan for the 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 during the pre-assessment visit. At the conclusion of the pre-assessment, a written report detailing the findings 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 previously, BS 25999 follows guidelines consistent with ISO 17021.

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 of the organization's understanding of the requirements of the standard
- Understanding of the proposed scope of the stage 2 assessment
- Review and confirmation of the resources needed for the stage 2 assessment
- Plan outlining the stage 2 assessment
- Confirmation that management review 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 two 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 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. BCM experts will be employed to act as technical advisors to the assessment team where required. These experts will be, at minimum, Business Continuity Institute (BCI) or Disaster Recovery Institute International (DRII) certified.

"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 two 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.

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
- Verification of the effective interaction among all BCMS elements
- Continuation of operational control
- Review of any changes
- Use of marks and any other reference to certification
- Verification of a demonstrated commitment by the organization to maintain 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 the organization’s products and services.

Summary of Benefits

<p>Framework Provides a common framework, based on international best practices, to manage business continuity.</p>	<p>Supply-Chain Ensures that every company in the supply chain understands and consistently applies guidelines and standards consistent with the organization’s requirements.</p>
<p>Resilience Proactively improves resiliency efforts when faced with disruptions to key value streams.</p>	<p>Competitive Advantage Contributes to the opening of new markets through the demonstration of compliance with best-in-class standards.</p>
<p>Management Delivers a proven response methodology for managing a disruption.</p>	<p>Delivery 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>Reputation Helps protect and enhance the organization’s reputation and brand.</p>	<p>Business Improvement Enables a clearer understanding of how the entire organization operates on a day-to-day basis, which can identify opportunities for improvement (including personnel and knowledge deficiencies and single points of failure).</p>
<p>Compliance Demonstrates that applicable laws and regulations are being observed.</p>	<p>Cost Savings 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 specializes in business continuity strategy design, development, implementation and long-term program maintenance. Working with Avalution immediately

affects the quality, focus and strategic alignment of your organization's risk management and planning efforts.

Avalution is also recognized as a participant in the BSI Americas Associate Consultant Program (ACP). BSI Americas administers the ACP program in order to provide a list of consulting organizations who are "credible and offer an acceptable service in terms of value and performance." As a certified firm, Avalution assists in preparing organizations for BS 25999 certification as well as assessing readiness for the certification process.

In addition to Avalution's project-focused work, its team of professionals is experienced in the delivery of long-term program management solutions. Due to client resource and time constraints, Avalution is able to assist with the execution of recurring business continuity lifecycle tasks, to include testing, training and program maintenance activities. Avalution's professionals are requested in the toughest of situations – aggressive business objectives, resource constraints, immediate need – and of course, the struggle with getting started. They coach, implement and above all, stay engaged to support your evolving needs – before and during crises.

Avalution's professionals deliver proven strategies that decrease the likelihood of business failure and minimize impact should the unforeseeable occur. For additional information regarding Avalution's professionals, tools and solutions please visit www.avalution.com, call 866.533.0575 or email contactus@avalution.com.

ABOUT BSI MANAGEMENT SYSTEMS



BSI Management Systems provides organizations with independent third party certification of their management systems, including ISO 9001:2000 (Quality), ISO 14001:2004 (Environmental Management), OHSAS 18001 (Occupational Health & Safety), ISO/IEC 27001 (Information Security), ISO 22000 (Food Safety) and ISO 20000 (IT Service Management). As one of the world's leading management systems registrars, BSI Management Systems has more than 40,000 clients worldwide thereby helping all kinds of organizations improve their business efficiency and reduce their risk. BSI Management Systems operates from four regional hubs based in the UK, Europe, Asia and America, with the capability to

deliver assessments worldwide, reinforcing BSI's commitment to deliver assessments with an unrivalled level of consistency across the world. This assessment capability is further augmented by training and advisory activities deemed essential to guiding clients towards the successful adoption and implementation of best practice.

For further information about BSI Management Systems, please visit www.bsiamericas.com or call 800.862.4977.