BUSINESS CONTINUITY AND RISK – A USER GUIDE FROM BSI

The management of business risk is vital; risk management is defined as identification, assessment, and economic control of those risks that endanger the assets and earning capacity of a business. Planning and preparing for those identified events is a 'must do' task.

What is a Business Continuity Plan?

An organization's Business Continuity Plan comprises of documented procedures for responding to a disruptive incident including how it will continue or recover its activities within a predetermined timeframe. Such procedures should address the requirements of those persons who will use them.

We hope that your business continuity plan is never needed, but the ability to recover, resume operations, and eventually return to a normal business environment should be considered a major concern. Your business continuity plan needs to deliver a quick and smooth restoration of business operations, addressing actions to be taken before, during, and after an incident.

We hear a lot about natural disasters such as tornadoes, floods, and fires, as well as, man-made disasters such as terrorist attacks, but the most frequent disruptions to a business are less sensational - power outages, cut cables, equipment failures, theft, or accidental damage. A Business Continuity Plan is intended to protect against any incident that may cause an extended disruption of your business.

Well-managed management systems have reliable recovery plans; however, they need buildings, staff, services, and communications to operate. Rapid recovery of individual systems or processes is of little value if your building is still in the dark. Deploying point solutions intended to fix specific problems is not business continuity; business continuity should include all of the businesses critical products and services and all of the risks.

Through good planning, you can identify and reduce risks, make the right decisions quickly, cut down time and financial losses, and perhaps save the business.

The Four-Step Process

Step 1: Establish your core planning team

You will need to identify an individual or group in charge of developing the Business Continuity Plan. The size of the planning team will depend on your business operations, requirements, and resources. It may be one person or perhaps several; each should deliver a particular skill or knowledge set. At this early stage of the plan, determine who should be an active member and who can serve in an advisory capacity.

These members should be appointed in writing by senior management and their job descriptions specifically modified to reflect the additional responsibility. From the outset, senior management must be both supportive and proactive in promoting the success of the program. They should issue a clear statement to the organization that:

- Sets out the purpose of the plan and how it will involve the entire business
- Establishes a high priority for the program
- Details the authority, reporting, and structure of the team
- Empowers the team to take the steps necessary to develop a plan, establish work schedules, plan deliverables/deadlines, and budget parameters

The planning of staff and roles within the Business Continuity team is very important and care should be taken when choosing members. Project management, diplomacy, and common sense are skills needed as the team will be dealing with the whole company, asking awkward questions, and in some cases changing work practices. Explaining why and selling these changes to those affected needs to be done firmly, but with sensitivity and understanding.

Step 2: Understanding your capabilities and the risks you face
This step entails conducting an initial threat assessment to determine your organization's vulnerability to possible hazards, emergencies, and disruptions.

a. Review internal plans and policies that have been established by your business already. Try and understand what the current policies and procedures were created for and by whom. Often existing internal processes require special attention. If someone has already taken the time to design and document something, it's likely to be important. Just because a document is old does not mean it is out of date or unimportant. Lots of plans within a company cover what should happen; rarely do they cover what should happen if things go wrong.

Look for documents covering:

- Evacuation
- Fire
- Occupational Health & Safety
- Environmental policies
- Equipment maintenance guides
- Security procedures
- Insurance
- Office closing plans
- Staff manuals
- Hazardous material plans

b. Meet with local government advisors, community organizations, and your local utility providers to determine their disaster recovery plans and resources available to respond to any incident.

Identify applicable local regulations such as:

- Fire plans
- Flood tables
- Environmental regulations
- Evacuation plans

c. Identify the critical products, services, and operations within your business and network, which enable you to operate your business.

Areas to review:

- Company products/services and the facilities and equipment needed to produce them
- Products and services provided by suppliers, especially sole source suppliers
- Critical services, such as electrical power, water, sewage, gas, telecommunications and data connections
- Vital equipment and personnel for the continued functioning of the facility

d. Identify your organization's internal resources and capabilities that may be needed in the event of an emergency or business disruption.

These could include:

- Personnel assigned as fire marshals, hazardous materials response team, security evacuation team, and a public information officer
- Equipment used in fire protection and suppression, communication devices, first aid supplies, warning systems, emergency power, and decontamination supplies
- Facilities designated as emergency operating centers, media briefing areas, and shelters
- First-aid stations
- Addresses, numbers, and contact details for all relevant suppliers, contacts, and staff
- Back-up systems available to provide payroll, communications, production, customer services, shipping and receiving, information processing, and recovery support
- Identify challenges and prioritize your activities, then determine how you will address the problem areas and resource shortfalls that were identified in the vulnerability analysis

e. Identify external resources that may be needed, and determine if formal agreements may be required to define a relationship with these resources.

- Local emergency management office
- Fire department
- Hazardous materials response organization
- Hospitals
- Local police
- Utilities
- Contractors/suppliers
- Insurance contacts

f. Perform an insurance review of all policies and identify cost/benefits of coverage.

Step 3: Develop a plan to control what happens

When something does happen, a clear plan will be needed to guide you. You may not have the time to decide what to do and how to do it; the plan will be there to help you provide fundamental tasks, processes, and guidance.

Your plan should include these basic components:

- An executive summary that provides an overview to senior management and all employees
- Purpose of the plan
- Emergency management policy of your business and each organization, if different
- Roles, responsibilities, and authorization for select group of employees
- Potential emergencies

Location of response and recovery site An Emergency Management section defines how your company or organization will deal with operational issues. This section serves as a basis for the development of procedures necessary to protect personnel and equipment, and accelerate operational recovery.

- Leadership and administration of Emergency Management Team
- Communications
- Life Safety
- Property protection
- Recovery
- Administration

Emergency response procedures set out how your business will respond to emergencies and the responsibilities that need to be addressed immediately in the event of a disaster. Specific procedures should be developed for specific potential emergencies. These will act as templates or guidance for others.

At a very minimum, you should cover the following procedures:

- How you initially assess the disruptive situation
- Preferred method of protecting employees, customers, vendors and business partners, equipment, information, and records, etc.
- How to report emergencies
- How to warn employees
- An evacuation plan
- How to decide when and how to shut down operations
- How internal and external communications must be handled
- Specific actions of specialized groups of employees
- Executive Committee
- Business Continuity Coordinator and Emergency Management Team Leader(s)
- Emergency Management Team Members, Alternative Team Members and Leaders Plans and support documents should be available for immediate reference as needed.
- Documents such as:
  - Emergency contact details
  - Building/facility/site maps identifying floor plans, network cables, stairways, designated escape routes, restricted areas, utility shutoffs, fire extinguishers and suppression systems, water mains, etc.
  - Resources needed for emergencies
  - Mutual aid/support agreements with other businesses and government organizations

Now write the plan. This activity should be shared among the members of this team, each one bringing a particular skill or understanding. Goals and a time-line will need to be set out early to include preliminary drafts, review, final draft, approvals, printing, and distribution. Training and understanding in the business are vital. Staff needs to know what to do and understand why they are doing it. Develop, schedule, and conduct training on the business continuity plan at all levels. This is very important for the success of all your planning efforts. The plan needs to be finally and publicly approved by senior management. This is not an invitation to change it. The program team must continue to own the process and the document. Once approved you can distribute the plan in both electronic and printed form. The final distribution list should include the managing director, all other directors of the company, senior management, emergency team members, and supporting personnel.

BSI/USA/326/MS/0113/E

Step 4: Implement the plan

This step is more than simply putting the plan away until something happens, an emergency or business disruption. Your business should be acting on recommendations made during the vulnerability analysis and reducing the risks whenever possible.

Integrating the plan into everyday company operations is an important function, as your business changes, so should the business continuity plan. By constantly improving/testing the plan, your ability to recover will improve.

Conduct training for all employees at periodic intervals, the training should include the procedures set out in the plan for individual employees. Technical training in equipment, evacuation drills, and full-scale exercises all play their part. After implementation, test how well the plan has been integrated by asking questions of senior management as well as general staff members, run periodic live testing such as deck top testing, and scenario testing and determine what's been left out, needs to be improved, or changed.

Conclusion

The information and actions described in this 4-step process can now be reviewed and fed back into your plans. This feedback loop is a key feature of any successful management system.

Business continuity is an ongoing task and can be complex; it is also one of the most important things a company possesses. For some organizations a simple step-by-step approach as described here is enough; for others, a formulated and independently inspected approach is needed.

ISO 22301 is the international standard for Business Continuity Management (BCM). The international standard provides a management system that allows you to identify potential threats to your organization and make sure you have the resources, procedures, and training in place to deal with an unexpected disruption. Your organization will be able to maintain operations during a disruption, stand apart from competitors, and protect your brand. This standard represents years of research and development, setting out defined processes and best practices in the form of a common approach.

ISO 22301 is suitable for organizations of all sizes, across all industries, public or private, manufacturing or service. It provides a common approach to and language for BCM, allowing global organizations to achieve internationally recognized best. Based on the 'Plan-Do-Check-Act' model, the standard enables you to continually improve your organization's effectiveness.

Whatever route you decide to take, Business Continuity is a must-do task. Without it an organization is vulnerable and unprepared for even simple disruptions.

bsi.

For more information call 1 800 862 4977 or visit www.bsigroup.com/ISO-22301-us

BSI Group America Inc.
12950 Worldgate Drive, Suite 800
Herndon, VA 20170
USA
Tel: 1 800 862 4977
Fax: 1 703 437 9001
Email: inquiry.msamericas@bsigroup.com
www.bsiamerica.com

BSI Group Canada Inc.
6205B Airport Road, Suite 414
Mississauga, Ontario
L4V 1E3
Canada
Tel: 1 800 862 6752
Fax: 1 416 620 9911
inquiry.canada@bsigroup.com
www.bsigroup.ca
www.bsigroup.ca/fr

The BSI certification mark may be used on your stationery, literature and vehicles when you have successfully achieved certification and conform with applicable guidelines.

The mark shall never be applied directly on the product or service.

Copyright © 2013 The British Standards Institution. *All Rights Reserved.*