

Practical Business Continuity and Disaster Recovery Planning

*The Need for a Simplified and Knowledge Management Based
Approach to Disaster Planning and Mitigation*

White Paper

By Robert Takemura, Vice President
MLC & Associates, Inc.

E-mail: BTAKEM@MLC2RESQ.COM
Web Site: WWW.MLC2RESQ.COM

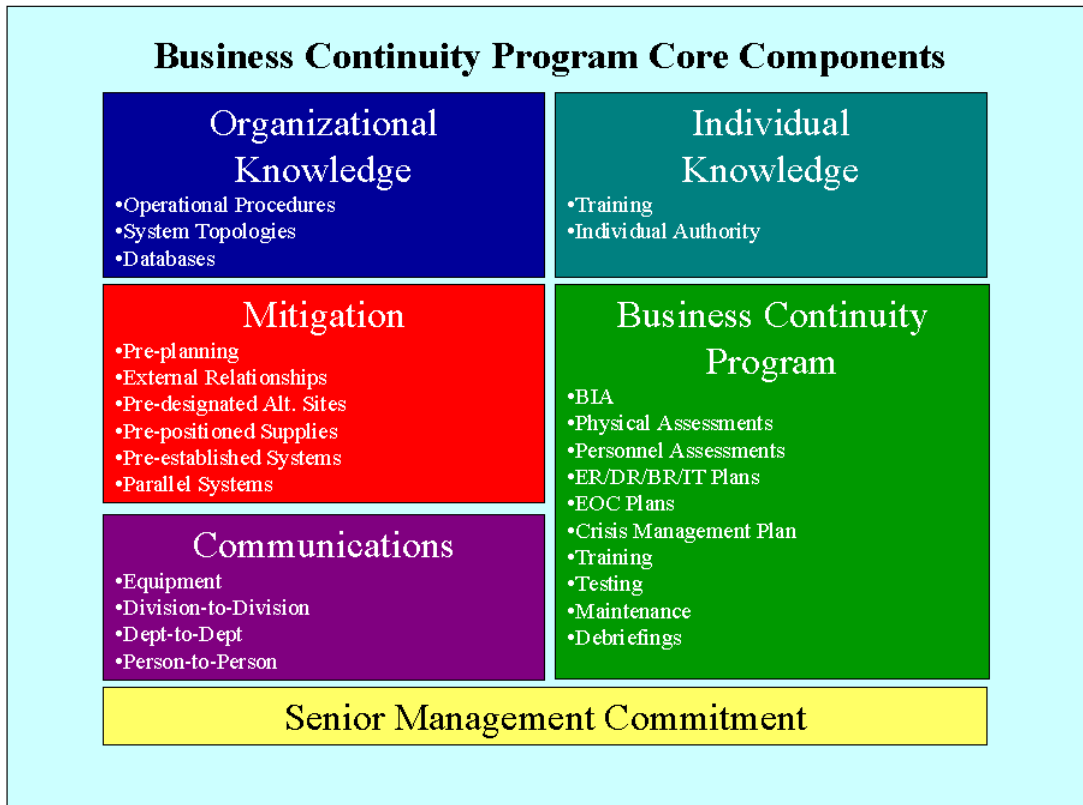
Introduction

In many cases, Business Continuity and Disaster Recovery Plans and Programs have been developed using a rigid structure that often fail to meet the challenge of actual events. While pre-planning (including the development of plans) is essential for audit, training, and other purposes; more often than not it is the planning *process* that provides the most benefit. It is this combination of shared ideas, “What if” planning, infrastructure development, and mitigation techniques that makes the difference between a “plan” that sits on the shelf versus a “program” that actually works or even prevents a disaster from occurring at all. Therefore, a new and pragmatic approach is needed.

The current form of Business Continuity and Disaster Recovery Planning developed from a combination of external and internal factors. Externally, governmental regulators and trade groups developed requirements for the protection of data in the financial services industry. Later, additional stipulations were established for general business continuity. In addition, other requirements for developing response plans (for events such as hazardous materials releases) impacted many different business sectors. Internally, all businesses eventually realized that the potential costs and liabilities incurred due to an interruption in normal operations could be financially devastating. With these two motivating factors, the issue went from “Should we prepare?” to “How do we prepare?”.

Plans vs. Programs

Many organizations have responded to the need for business continuity and disaster recovery planning by assigning responsibility and developing internal plans. However, the types of plans generated and the level of detail often vary considerably. Most organizations have established emergency response plans to take care of life/safety issues. Others have developed specific plans for key issues such as Data Center recovery, server recovery, and telecommunications recovery. Nevertheless, many organizations fail to take the critical step from developing individual plans to developing a “Program”. Comprehensive Disaster Recovery and Business Continuity Programs are comprised of a multitude of components and are only effective if all these components are in place. Furthermore, an integrated approach is required that focuses not on disasters alone, but also enterprise-wide recoverability, reliability, and sustainability. In addition, comprehensive programs are not driven only by disasters, but rather by a day-to-day philosophy and mindset emphasizing



good business practices that protects employees, maintains revenues, protects market share, and safeguards customer goodwill.

These components include internal knowledge and focused action steps:

- Knowledge – Organizational and Individual
- Mitigation – Internal and External Planning
- Communications – Equipment and Procedures
- Business Continuity – Analyses, Assessments, Planning, Training, Testing, Maintenance, and Debriefings.
- Senior Management Commitment – Funding, Time Allocation, Support, and Approval

Knowledge

There are two basic levels of knowledge. Organizational knowledge is the sum total of the group's plans, operating procedures, tools, and databases. Individual knowledge is the cumulative learning and wisdom that each person possesses. A detailed discussion of each of these concepts is provided below.

Organizational Knowledge Level

Most organizations and internal departments possess a certain level of inherent knowledge to conduct their internal operations. Most Business Continuity Programs re-write this existing information. However, businesses function in a *dynamic* rather than *static* environment. Consequently, maintenance is always a problem. In fact, many individuals resist any efforts to convert or re-write information that already exists and they feel comfortable with (and use day to day). Furthermore, the level of detail included in most business continuity plans is too granular for most people to grasp. As a result, no one pulls the "book" off the shelf. Instead, people tend to draw on their ingrained knowledge and make up recovery strategies "on the fly". Therefore, business continuity plans should be structured to be as simple as possible and ideally, will be so ingrained that the written document won't even be needed unless a specific detail is required (such as a telephone number or vendor name). This leads into the concept of Individual Knowledge Level.

Individual Knowledge Level

The fundamental requirement for effective recovery lies within the employees. It is imperative that each member of the organization understands his or her role in an emergency, a basic set of easy to remember "rules of engagement", and has been provided ongoing training.

- In a military sense, a crisis is managed by senior management (the generals and colonels). At this level the overall goals and policies are set, i.e., strategic planning.
- Additional tactical plans to implement the strategic goals are developed by mid-level management (the majors and captains).
- The actual implementation to accomplish tactical plans lies with the staff and low-level management (the lieutenants, NCO's, and privates).

Senior Management must understand that a “crisis” is by definition a stressful and uncertain period of time. Senior Management must consistently communicate to their employees that it is acceptable for them to make small mistakes in their efforts to restore normal operations. The key is for them to understand the overall needs of the organization and to prevent them from making the big mistakes.

For example, if a Data Center Supervisor or Operator cannot reach their Division Manger (or other designated person) and activates the hot-site prematurely, it is acceptable as long as the person has made reasonable efforts at communicating, has weighed the consequences, and has taken action that they believed (at the time) was necessary to safeguard the immediate and long term needs of the organization.

Mitigation

Mitigation involves pre-planning internally and externally. Internally, the implementation of parallel functions and connectivity must be a high priority for all mission critical areas. This may involve regional work centers that essentially perform the same function but are geographically separated. Parallel functions also include the use of multiple systems, data paths and methods to ensure continual access.

Other internal mitigation steps involve considerations for alternate work sites. This may involve pre-designated sites from within the organization or facilities provided by third parties (such as data processing hot sites). Whenever possible, an organization should thoroughly consider its internal capabilities first. Furthermore, it is important that alternate site plans *not* be too detailed if only general office space is required. This reduces the amount of training and updates required for the program. Instead, a general knowledge of potential alternate sites is often sufficient for most business units. The exception is when highly specialized facilities, data processing, or other unique requirements are needed. Examples include Data Centers, Call Centers, and Electronic Funds Transfer facilities. In addition to alternate sites, mitigation may include the pre-positioning of supplies and equipment at the alternate site or the development of emergency acquisition plans (such as vendor quick ship agreements).

Additionally, today’s business environment relies heavily on the development of external relationships including the concept of “business partners”. Small, medium, and large business

partners (vendors and suppliers) must be identified. In some cases, this process reveals external dependencies and highlights the need for developing contingency arrangements for sole source providers. Mitigation involves the use of multiple vendors and suppliers for key supply chain requirements.

Furthermore, external relationship building is essential and may include vendors, trade organizations, public sector contacts, and even competitors. The goal is to pre-establish these relationships so that they will be in place during a crisis.

Communications

All organization's need and have equipment and systems for their internal communications. This includes telephone systems, voice mail, company Intranets, the Internet, cellular telephones, and pagers. However, disaster communications must be considered and equipment/systems are only a part of the solution. Alternate capabilities if the primary system is down are essential. More importantly, the actual needs (i.e., response to a crisis) for communication must be considered. For example, using the W₃H[®] method¹, if a situation occurs:

- When do you communicate? (disaster notification and declaration criteria)
- Where did the incident occur (disaster information and determination component)
- Who communicates the information and with whom do you communicate? (disaster notification)
- What happened? (disaster information and determination component) and What information do you need to convey? (status)
- Why is activation of the program needed? (disaster notification and declaration criteria) and Why did it occur? (future mitigation component)
- How do you respond and/or correct the situation? (implementation process)

In addition, communications skills are also an issue. It is not always what you say but also how you say it. Many problems occur during planning and even implementation when people don't communicate effectively. In some cases, negative communications skills lead to a lack of participation and stifles teamwork. In other cases, individuals or whole departments refuse to participate in the process.

¹ W₃H[®] method courtesy of MLC & Associates, Inc.

Unique terminology and acronyms can also add confusion. This problem is most evident when third parties are involved. Sometimes this “clash of cultures” appears when the private and public sectors interact. At other times, confusion occurs between the organization and their business partners. Everyone involved in the program must have a clear understanding of any terms used. This information should be a part of the training curriculum or avoided.

Business Continuity Programs

Comprehensive Business Continuity and Disaster Recovery Programs include a variety of different, yet integrated components². The Business Impact Analysis (BIA) provides a basic assessment of risks and provides a prioritized list of the functions performed by the organization. The Physical Assessment provides a snap shot of the facilities and itemizes the types of risks inherent for a particular site. The Personnel Assessment is a planning tool that documents individual employee skill sets. Plans include: Emergency Response Plans (life/safety issues), Disaster Recovery Plans (facilities issues), Business Resumption Plans (operations issues), Information Technology Plans (data processing and communications issues), Crisis Management and Emergency Operations Center Plans (disaster management issues).

In the past, plans have been relegated to large paper documents or proprietary software. Today, technology offers a variety of choices from internal intranet-based plans that can be accessed from any workstation to off-site Intranet hosting services. The advantages of these types of systems include ease of access, familiarity (most employees use their company intranet or the Internet on a daily basis), and ease of use (such as standard HTML pages). Hosting services can add the benefits (for disaster recovery purposes) of off-site storage, third party maintenance, and site redundancy.

Although plans are essential to any program, it is often the planning process, training, and testing of the plans that provide the most benefits to the organization. Additionally, most businesses must increase the knowledge level within their organizations to enable all levels of employees to respond to a disaster. This will help to ensure recoverability, reliability, and sustainability of the organization.

² Proprietary planning method developed by MLC & Associates, Inc.

Other benefits include increased communication, teamwork, and an assurance that employees will be able to effectively execute tactics (either pre-developed or spontaneous) to meet the overall strategic goals of the organization.

Finally, no Business Continuity and Disaster Recovery Program is complete without procedures for plan maintenance. Debriefings after actual events can be an invaluable resource for updating plans, reviewing tactics, and making modifications. Again, technology can assist in this area by providing a means for rapid feedback and updates to recovery plans.

Senior Management Commitment

Obviously, Senior Management must fund and allocate resources to a Business Continuity and Disaster Recovery Program. However, this type of support is only marginally effective. All employees must understand and believe that Senior Management is committed to them and the organization. Consequently, business continuity and disaster recovery planning is a fundamental part of day-to-day operations. Furthermore (as mentioned previously), Senior Management must allow individuals within the organization to make decisions and take action. The key is to ensure that all employees are continually trained and have been provided with practical experience, either through actual situations or simulations.

Conclusion

A simple, yet effective approach is needed to provide a knowledge management based approach to Business Continuity and Disaster Planning. Pre-written plans are important but actual implementation during a crisis relies on the ability of individuals to assess the situation, make decisions, and take action. Furthermore, Senior Management must be committed enough to the process to allow decision-making and actions to occur at the field level.

As the use of technology increases, the threat of disasters as well as our ability to respond to catastrophic situations increase. Technology often subjects us to higher risks (such as a decreased tolerance for down time and a smaller recovery “window”) but also provides a vehicle for more effective response. The key will be to provide employees with the information and procedural “tools” they need when they need them. Company intranets and the Internet will take a larger role

during crises. In fact, as the Internet continues to grow in importance for day-to-day functioning, more businesses will turn to innovative solutions such as third party hosting services to enable them to maintain 24x7 connectivity to their employees, even during a disaster.

Robert Takemura is Senior Vice President of MLC & Associates, Inc. and has over 10 years experience in the field of Disaster Recovery and Business Continuity Planning and Program Development. He can be reached via E-mail at: mlc@mlc2resq.com.

Key Concepts

- Use existing procedures and documentation as much as possible. Reference where to find the information and ensure that the information is complete and current.
- Add information that is useful, necessary, and unique to the needs for response, recovery, or resumption.
- Mitigate whenever possible to prevent disasters. Install generators, UPS equipment, surge protectors, etc. Diversify risk when practical, i.e., use parallel processing (information technology), spread inventory between diverse locations, implement dual operations when justified.
- Pre-position and pre-plan as a contingency. For example, if an alternate site is selected for a particular operational area, pre-position supplies, add data lines and voice lines, and determine a priority system for which operations must be restored first. Understand what the site capabilities are. It is not necessary to go into the detail of knowing the exact number of people or departments that will be accommodated by the alternate site (as long as the basic requirements can be met) since the actual situation will almost certainly be different than reality. The exception is if special needs are required such as a wire terminal or dedicated system (such as an Automated Call Dialer).
- Establish a thorough communications plan and structure for internal communications, i.e., pagers, message paging, satellite telephones, cell phones, company intranet, and the Internet.
- Establish a media crisis management plan and strategies for foreseeable crises. Designate responsible personnel and (when necessary) establish a relationship with an advertising or media expert in the field of crisis management.
- Establish vendor and business partner relationships in advance. Quick ship agreements and individual Service Level Agreements should be implemented whenever possible.
- Utilize in-house resources whenever possible to build necessary redundant capabilities.
- Train and Exercise on a continual basis. Implement a basic set of instructions that all employees can remember and use under stress.
- Perform debriefings after every exercise and actual crisis event to define any lessons learned as well as what went right for future planning.