the Availability Digest

www.availabilitydigest.com

Business Continuity from A to Z

December 2010

Business Continutiy from A to Z is a five-part series of white papers[1] (more accurately, a five-chapter, 100-page book) that discusses best practices for Business Continuity Planning (BCP). Written by Greg Livingston, ABCP, CDRP, Managing Director of Centurion Compliance Partners, LLC, his book follows the standard approach to BCP and explores the responsibilities of all of the stakeholders in the plan.

The five parts include:

- Part 1: Contingencies: Are your bases covered?
- Part 2: Business Impact Analysis: The all-important foundation.
- Part 3: Think it Through: Effective strategy, development & documentation.
- Part 4: Your BC Toolkit: Options and integration.
- Part 5: The Final Countdown: Rollout, testing, and results.

Implementing a comprehensive business continuity (BC) plan involves a significant ongoing investment in staff time, technology, tools, and training. These white papers provide a roadmap for navigating through the various steps required to build and maintain an effective BC plan.

Part 1: Contingencies: Are your bases covered?

Recognizing the need for companies to survive debilitating disasters, various industry associations and governments began developing in the early 1990s guidelines and even regulations for achieving business continuity. BC planning is now its own industry and includes organizations providing hot sites, data-backup services, communications, software tools, consulting, and dedicated publications. Educational opportunities abound and lead to a variety of certifications.

Plausible scenarios that can seriously impact a company's operations include:

- Network outages
- Website failures
- Flooding and fires
- Power failures
- Earthquakes
- Hurricanes
- Epidemics
- Volcanic eruptions
- Hacking
- Theft of intellectual property
- Street protests
- Careless construction errors

[1] Greg Livingston, Business Continuity from A to Z, *Centurion Compliance Partners and MIR3 white paper*. www.mir3.com/bcwhitepaper1, www.mir3.com/bcwhitepaper2, www.mir3.com/bcwhitepaper3, www.mir3.com/bcwhitepaper4, www.mir3.com/bcwhitepaper5

Potential costs of downtime include loss of revenue, loss of customers, loss of employee productivity, compensatory payments, drop in credit rating, drop in stock price, litigation, and loss of reputation. When it comes to business interruption, it is not a matter of if but of when. *Failing to plan is planning to fail.*

What is Business Continuity Planning?

BC planning is the *continuous* process of

1. identifying risks and their impacts on critical business functions,
2. developing strategies for mitigating these risks, and
3. developing procedures for restoring business functions as quickly as possible.

Business continuity is not the same as disaster recovery (DR). DR is an important part of business continuity and deals with recovering IT systems, applications, and data. BC planning encompasses:

- risk management
- disaster recovery
- facilities management
- mass absentee planning
- quality management
- health and safety
- knowledge management
- emergency management
- security
- crisis communications
- public relations

The most important reasons to implement a business plan are the saving of lives, the survival of the business, the obligations to stakeholders, regulatory compliance, maintaining customer service, and minimizing financial loss. A good BC plan will allow a company to:

- identify and mitigate risks before a disaster occurs.
- minimize decision time during a disaster.
- maintain a calm preparedness when a disaster occurs.
- provide for an orderly recovery following a disaster.
- ensure organizational stability.
- reduce reliance on key personnel.
- reduce potential for legal liability.
- meet customer expectations and service level agreements.
- safeguard reputation and brand.
- maintain competitive position.
- provide early warning of vulnerabilities to disasters.
- potentially realize better insurance costs and coverage.

Regulations and Standards

Many regulations and standards covering numerous industries have been published. The author lists many of these. A leading reference is the Federal Financial Institutions Examination Council (FFIEC) BCP Handbook.[2]

Management Support

It is not in the nature of many organizations for support of a BC plan to come from below – staff has too many other responsibilities and duties to make business continuity a priority. Rather, BC planning has to be mandated from the top. Getting management to support a BC plan can often

[2] Business Continuity Planning: IT Examination Handbook, *Availability Digest*; October 2006. http://www.availabilitydigest.com/public_articles/0101/bcp-it_examination_handbook.pdf.

be a frustrating experience. The author discusses several tips for gaining top management buy-in.

Approach management with specific objectives, but take what you can get. Present the benefits, and be prepared in advance to overcome objections. Research the competition to find out what they are doing – BC can be a competitive advantage. Point out the legal ramifications, including criminal liability, heavy fines, and even jail time.

BC Planning

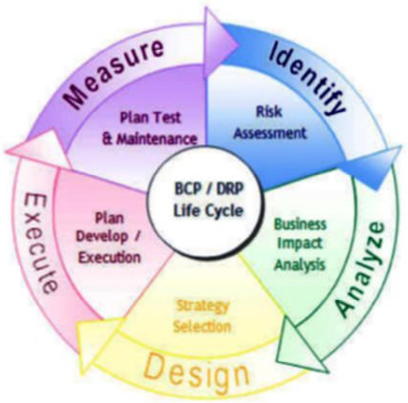
Once planning has obtained management support, the BC implementation team must be assembled. This should include a top-management representative, a BC coordinator reporting to the management representative, and lower-level teams representative of the various business functions.

BC planning follows five distinct phases:

1. *Identify* potential hazards that could disrupt the business. This is the Risk Assessment discussed later in this part.

2. *Analyze* the impact of these risks on the various business functions. This is the Business Impact Analysis (BIA) that establishes the Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), the minimum operating resources, and the internal and external dependencies for each business function. The BIA provides the foundation for the BC plan and is the subject of Part 2.

3. *Design* the mitigation and recovery strategies to protect people, assets, and business functions. Part 3 addresses the Design phase.



4. *Execute* the development of the plan. There are a number of tools available to help with the organization, documentation, and implementation of the plan. Part 4 discusses the range of tools available (with no specific reference to any particular tool).

5. *Measure* the plan via a sequence of test strategies ranging from examination to simulated disasters. Testing is covered in Part 5.

These five phases are continuous. As the company evolves, so must the BC plan.

The Risk Assessment Phase

The first phase is the Risk Assessment. In this phase, the risks to the organization caused by various hazards are identified. Hazards include natural threats such as hurricanes, earthquakes, and floods; human threats such as operator errors, vandalism, and terrorism; and technical threats such as server or software malfunctions, power or cooling losess, and network failures.

The likelihood of each hazard is estimated. Various attributes for each hazard are then scored. Attributes include the speed of onset and the consequent degree of forewarning (hurricanes are predicted well in advance, but earthquakes provide no warning), the duration of the hazard and its consequences, and the impact on the business. The result is an overall score for each hazard, which allows the threats to be prioritized for the Business Impact Analysis.

BC Best Practices

Part 1 concludes with some BC best practices. Don't cut corners – BC planning is a continuous process. Keep the plan simple – nobody will read a 100-page plan. Control the costs of recovery by using available assets. Follow a standard or a handbook such as the FFIEC BCP handbook. Make use of available tools for BCP preparation and event management. Test the plan, and plan tests at times that are convenient to the stakeholders. Practice the BCP plan frequently.

Part 2: Business Impact Analysis: The all-important foundation

For each risk identified in the Risk Analysis, the Business Impact Analysis (BIA) documents which business processes will be disrupted, the severity of the disruption to each business process, and how long the business can survive without those processes. It identifies the processes that are most critical to the company's operations and the interdependencies of processes.

The BIA then establishes the minimum resources required to recover business processes to a minimum acceptable level. It prioritizes the allocation of recovery activities and resources to restore the most critical processes first, which is the basis of a sound recovery strategy.

The recovery requirements set forth in the BIA – required resources, process interdependencies, maximum allowable downtime, and so forth – become the test criteria against which the recovery plan and those of critical suppliers must be judged. It is imperative that the recovery requirements not overstate the criticality of business processes and their required recovery times since recovery costs escalate parabolically as the required recovery times decrease.

Preparing a good BIA is resource-intensive and must be supported by top management. Approach top management with an executive summary recapping the reasons that the organization bought into the BCP effort initially. Review the threats uncovered in the Risk Analysis, and explain how the BIA will be used with the Risk Analysis to provide the basis for an effective recovery plan. Explain how staff will be used to gather the requisite data while minimizing the impact to their work day and how they will share in the ownership of the recovery process. Show how the BIA can be used for other purposes such as vulnerability assessment and incident response.

Gathering the Data

The BIA requires that the following data be obtained and documented:

- All business processes performed by each department.
- The resources – technologies, people and supplies – required by each process to function properly.
- The interdependencies of processes within departments, across departments, and with third-party vendors.
- The criticality of each business process to the health and survival of the organization.
- The maximum allowable downtime for each process (the Recovery Time Objective, or RTO).
- How current does the data have to be following recovery (the Recovery Point Objective, or RPO).

This data can be gathered via questionnaires, one-on-one interviews, or group sessions. Someone from each business function within each department should participate. Include both business and IT staff. Focus on process, not procedures. The BIA is concerned with what each department does, not how it does it.

Impact Assessment

Assess the impact to the organization when each process is interrupted and how the cost of the disruption may escalate with time. Focus on the impact of a disruption, not its cause. Impact scenarios are likely to be loss or denial of physical access, failed technology, or both.

Impact consequences include:

- *Financial* - lost revenue and recovery costs.
- *Operational* – the ability to carry out functions based on available resources and interprocess dependencies.
- *Legal and Regulatory* – prosecutions, fines, and lawsuits as a result of failed processes.
- *Customers* – customer defection, SLAs.
- *Reputation* – good will, brand loyalty, and stock value.

Recovery Requirements

The recovery objectives include RTO, the maximum allowable time to recover, and RPO, the maximum allowable data loss. Consider scenarios in which partial recovery of business functions is acceptable and buys time, thus freeing recovery resources for other recovery efforts. Note that RTOs and RPOs may vary with the season.

Another important class of recovery requirements is the resources – technology, people, supplies, vendors – that must be in place to restore each process.

The BIA Matrix

The results of the BIA data gathering can be summarized for management review. The BIA matrix should include the following information for each business function:

- Business function name and description.
- Outage duration.
- Financial, operational, regulatory/legal, customer, and reputation impact.
- Dependencies.
- RTO and RPO established by business unit.
- Technology to be used.
- Can the RTO and RPO be met?

Part 3: Think it Through: Effective strategy, development & documentation

Once the Risk Analysis and the Business Impact Analysis have been completed, the full recovery plan can be prepared. The first step is to compare the organization's IT capabilities with the requirements of the business units. Recovery strategies can be categorized and may range from High Availability (hot offsite servers) to Continuous Data Protection (offsite backups with journals), remote disk backups, and remote tape backups. The higher the level of protection, the more expensive is the solution. Each business process is mapped into the least expensive recovery capability that provides the RTO and RPO needed.

Recovery procedures should begin with manual procedures for carrying on business as full recovery efforts are under way. The next step is to restore the organization's technological capabilities. This may require moving employees to an alternate site if the first site has been rendered nonoperational.

Staff issues must also be planned. This includes medical treatment as a result of the incident, notification of family members in the event of death, evacuation plans that include accounting for personnel, relocation of staff to an alternate site (travel, housing, and expenses), daycare services for children of displaced staff, and continuation of payroll.

A crisis communication plan must be established to allow the coordination of recovery efforts. Mass notification and response products are available to help fulfill this need. Communications must also be maintained with vendors, relatives of employees, local public safety agencies, regulatory agencies, the financial markets, and the press.

It is important to document all actions taken in response to the incident and as recovery progresses. This can help safeguard the company and its management in the event of a regulatory audit or litigation.

The resulting plan should include:

- Conditions under which the plan should be activated.
- The initial response to the disruption:
  - Emergency assessment.
  - Evacuation procedures.
  - Emergency medical response.
- The recovery team structure and its command and control.
- Crisis communications.
- Recovery procedures:
  - Notification of staff, stakeholders, vendors, authorities.
  - Facilities, equipment, and supplies needed.
  - Restoration of data-processing capabilities.
  - Restoration of data networks.
  - Public relations.
- What to do after recovery.
- Salvage operations.
- Plan distribution.
- Plan maintenance and version control.
- Plan testing.

The resulting plan should be reviewed and approved by the department managers. It should be immediately available in the event of an emergency. One suggestion is to distribute it to the required personnel on USB key-chain thumb drives.

Part 4: Your BC Toolkit: Options and integration

Business continuity planning is an ongoing process. As the company evolves, so must the plan. There are a variety of tools available to help with plan development and execution. The tools do not drive the plan. Rather, they aid in the various activities involved with planning and execution. Some tools are hosted as an outside service, and others are available for in-house use.

Tools can be categorized into two categories – preparatory tools and event-management tools. Preparatory tools provide planning templates, document control, and version control. Event management tools are available to aid in incident response and recovery efforts including incident management, command-center management, notification, crisis management, communication, and auditing.

Factors to consider when choosing a tool include:

- Security – does the tool fit within the security requirements of the organization (for instance, can the plan be hosted on an offsite service)?.
- Is the tool provider financially sound?
- If the plan data is stored offsite, can it be moved to another service or to an in-house tool?
- If the plan is stored offsite, is the backup plan of the tool vendor sufficient?
- Is the tool compatible with the company's IT infrastructure?
- Do the contract terms lock the company in for an unacceptable duration?
- Who owns the plan data?
- Does the tool vendor have the appropriate certification (for instance, SAS 70 for financial institutions)?

In addition, there are many certified consultants available to help with the creation of the plan and with the choice of tools for plan preparation, incident management, and recovery.

Part 5: The Final Countdown: Rollout, testing, and results

A business continuity plan is no good if it doesn't work when needed. Therefore, it is imperative to test the plan. Testing is not a one-time effort. As the company evolves, things change. The BC plan must be continually updated and expanded to reflect the changes. It is also modified in response to audit recommendations and to the results of prior testing.

It is important to periodically test the plan to continually ensure that it is workable. The BC plan test is not a pass/fail test. Rather, it is a mechanism for discovering faults in the plan and for improving it. It is the procedure that ensures that the plan is kept current. It is also an important tool for training staff in the documented response and recovery procedures.

Business-recovery testing can be expensive. Staff must devote perhaps days to a full-blown test. Additional resources must be obtained or commandeered from operational systems. The company's operations may be impacted during the test. Vendor activities must be coordinated.

Consequently, the author suggests a layered approach to testing, starting with nonintrusive tests and progressing to less-frequent full tests.

- Checklist Test

  This test is a tabletop drill. The recovery team meets to determine whether the plan is current, whether adequate supplies and equipment are available at the backup site, whether telephone numbers are current, and whether everyone has access to the most current plan documentation.

- Structured Walk-Through Test

  This test is typically carried out on a departmental basis. It involves a detailed walk-through of the procedures called for in the plan by each team member. During this test, a disaster scenario is specified; and team participants describe or act out their responses as dictated by the plan. Normal operations are not affected.

- Emergency Evacuation Drill

  The facility evacuation plan is exercised with all company personnel to ensure that they know the exit routes, the procedures for handling personnel with physical limitations, the assembly locations, and the verification procedures.

- Recovery Simulation

  Recovery simulation is the most extensive, expensive, and disruptive testing but also the most important. It requires the greatest amount of planning and may entail some risk to current business operations. In response to a specified disaster, recovery teams use equipment, supplies, and facilities as they would during an actual disaster to carry out recovery and restoration of company operations. A set of actors may be used to provide a sense of reality to the simulated incident.

The scope of each type of test and the responsibilities of the recovery team personnel for each test are detailed by the author. These tests should be scheduled well in advance according to a time schedule. The simpler tests should be scheduled more frequently, with the more complex tests scheduled frequently enough to ensure the viability of the living BC plan.

Summary

Some sort of business interruption is bound to affect every company, ranging from simple server failures to a data-site disaster. Without proper planning, even simple failures can cause serious disruptions to a company's operations.

A properly developed and tested business-continuity plan can go a long way toward mitigating the impact of a disruptive event. It could even save the company from the ultimate disaster - its demise.