the Availability Digest

Business Continuity Planning: IT Examination Handbook

October 2006

22 pages plus appendices

What better way to learn about what should go into a good Business Continuity Plan than to peek at the handbook that the auditors use. The booklet entitled “Business Continuity Planning: IT Examination Handbook,” published by the FFIEC (the Federal Financial Institutions Examination Council), is just that. It is complete, concise, and easy to read. It may be found at http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus_continuity_plan.pdf. Though focusing on the BCP requirements for financial intuitions, it is an excellent reference for any industry.

Federal Financial Institutions Examination Council

FFIEC

Business Continuity Planning BCP

MARCH 2003

IT EXAMINATION HANDBOOK

Though a good Business Continuity Plan, or BCP, is a regulatory requirement for some organizations such as large financial institutions, it should nevertheless be seen as mandatory for any organization that wants to survive an unanticipated interruption to its business processes. According to the Handbook, a BCP should be the direct responsibility of a BCP team in a large organization or a BCP coordinator in a smaller organization.

The BCP should detail an organization’s response to any sort of threat, whether it be human, natural, or technological. Contrary to some common practice, it should not focus simply on technological recovery of the data processing environment. It should focus on recovering an entire business process which has been disrupted. In addition to the data center, consideration should be given to such matters as moving personnel; substituting replacement personnel for those not available for some reason; housing people; the availability of public transit or access to backup facilities by private means; communication with the organization’s staff, customers, and business partners; and media relations, among others.

The BCP should not focus on the recovery from a specific threat but rather focus on the recovery of a business process that has been interrupted.

The FFIEC Handbook details the four basic steps to be followed in creating a BCP:

- The Business Impact Analysis
- Risk Assessment
- Risk Management
- Risk Monitoring

Business Impact Analysis

The first step in creating a BCP is to perform a Business Impact Analysis, or BIA. The BIA identifies the potential impact of unanticipated disruptions to one or more critical business processes. For each such process, the BIA establishes the maximum allowable downtime (Recovery Time Objective, or RTO), the maximum allowable data loss (Recovery Point Objective, or RPO), and the maximum allowable backlog of transactions that can build during the interruption. The BIA also establishes the costs associated with downtime for each critical business process, whether these costs be financial, customer relations, loss of property or life, public image, regulatory infractions, or whatever.

The BIA should consider the following questions:

- What equipment is required at the recovery site?
- How would a department function if it were denied computing or network access?
- Where are the single points of failure?
- What are the critical outsourced relationships?
- What are the minimum requirements for staff and space at the recovery site?
- What special forms and supplies will be required at the recovery site?
- What communication facilities are needed at the recovery site?
- Is there public transportation to and housing available at the recovery site?
- What critical operational and security controls require implementation prior to recovery?
- Is there a conflict for services of a common recovery site shared by multiple lines of business?
- Have employees received cross-training for backup roles?
- Are emotional support and family care needs considered?

Risk Assessment

The Risk Assessment prioritizes potential business interruptions based on the severity of the disruption and the likelihood that it will occur. This analysis is followed by a gap analysis that compares the organization’s existing BCP to the needs identified by the BIA.

Threats include malicious or accidental human activity, natural disasters, and technical malfunctions. However, the nature of a specific threat is not as important as the severity of a disruption to business services, no matter what the cause of the disruption. In this way, the Risk Assessment can be quite broad. It can be independent of the type of threat and be applicable to threats that cannot even be envisioned at this point.

Threat scenarios are analyzed as a combination of the probability that the threat will occur and the severity of its impact on the business. The most difficult threats to assess are those having a major impact but which are expected to occur with a very low probability of occurrence.

Following the analysis of the business risks, a gap analysis is performed. The gap analysis is a comparison of what types of plans the organization needs to maintain, resume, or recover normal business operations versus what is provided by the current BCP.

At the conclusion of this phase, a prioritized list of business processes and the threats that may impact them has been created.

Risk Management

Risk Management is, in fact, the creation of the Business Continuity Plan. It should be disseminated to everyone who will be involved in its implementation. It should be specific in what conditions would trigger the implementation of the plan and what immediate steps should be taken in the event of a disruption. It should be flexible enough to respond to unanticipated threat scenarios and be focused on how to get the business up and running rather than on the precise nature of the disruption. For instance, it should not be focused on what to do in the event of a hurricane but rather on what actions to take should the company's online store go down.

Recovery scenarios should include how the organization will respond if:

- critical personnel are not available.
- critical facilities are not accessible.
- equipment should malfunction.
- software or data are not accessible or are corrupted.
- vendor assistance or service from an outside provider are not available.
- utilities (power, air conditioning, telecommunications) are not available.
- critical documentation or records are not available.

Business continuity planning should also be incorporated into other corporate policies:

- The System Development Life Cycle should include business continuity considerations in project plans so that new applications will be designed to permit easier continuation of business in the event of a disruption.

- Likewise, the Change Control process should include business continuity specifications that might be affected by the change.

- The backup of data and other critical information is an integral part of business continuity.

- It should be ensured that employees are trained in the execution of the BCP.

- Insurance policies should be periodically reviewed to ensure that they reflect the current business environment.

- There should be polices in place to coordinate with government and community officials.

Risk Monitoring

Once the BCP is in place, it should be subject to an independent audit review; and it must be practiced and tested regularly. It must also be updated whenever there is a change to the business environment or to involved personnel.

The frequency and complexity of testing is based on the risks to the organization. There are several testing levels that can be considered:

- O*rientation/Walk-through* is simply a discussion of the plan with a group of involved people.

- *Tabletop/Mini-drill* involves role-playing to an imagined threat and consequent disruption.

- *Functional Testing* tests the emergency management capabilities to a simulated disruption and the actual or simulated responses of the groups involved.

- *Full-scale Testing* uses the BCP to actually recover to the backup site.

Summary

The Handbook concludes with the six factors that are the critical aspects of business continuity planning:

- Business continuity planning should be an enterprise-wide activity.

- A thorough business impact analysis and risk assessment are the foundation of an effective BCP.

- Business continuity planning is more than the recovery of the technology. It is the recovery of the business.

- The effectiveness of a BCP can only be validated by thorough testing.

- The BCP and test results should be subjected to an independent audit.

- The BCP should be periodically updated to reflect and respond to changes in the business environment.

Appendices

The Handbook contains five appendices:

- Examination Procedures
- Glossary
- Internal and External Threats
  - malicious activities
  - natural disasters
  - technical disasters
- Interdependencies
  - telecommunications
  - third-party providers
  - key suppliers
  - business partners
- BCP Components
  - technology
  - data-center recovery
  - backup recovery
  - geographic diversity
  - backup and storage
  - data file backup
  - software backup
  - offsite storage
  - facilities
  - communications