



The SYSTEMS CONSULTING CONSORTIUM, Inc.
P.O. Box 519, Orinda, CA 94563-0519
925-254-0760 ofc, 510-409-2888 mobile
Please visit our website at www.scc.cc

BUSINESS CONTINUITY PROGRAM

A CASE STUDY

AN SCC WHITE PAPER BY
SCC PRINCIPAL HARVEY SCHMIT
REV #0, OCTOBER 18, 2007

Described below is a Business Continuity Program (BCP) effort that SCC Principal Harvey Schmit was recently involved in. Mr. Schmit has led several BCP efforts since 2005.

This SCC BCP effort was triggered by a specific comment in the Management Letter from the company's audit firm regarding the lack of a BCP for the company. There had been at least three prior attempts to create a BCP. Some had failed after substantial out-of-pocket cost. This had gone on for some years when the CIO, who is part of the company's executive team, was given the charter to resolve it "once and for all."

Initially, a small internal team was put together to address the effort, but evolved over time into a one person internal "team" plus one external person (a BCP consultant). The qualifications of the internal person were a Critical Success Factor - a senior IT professional who had very good business knowledge and business connections across the entire company. Consequently, he was able to bring resources to bear from the IT side and from the business side when necessary. He was also able to challenge the business regarding the recovery objectives and the IT organization regarding recovery capabilities.

The scope was set very specifically and carefully up front to be the two most important business processes in the eyes of the CIO (reflecting the desires of the Top Management of the company). This scope was verified and validated by a Business Impact Analysis (BIA) mini-study. The BIA evaluated the importance of these business processes vis-à-vis their impact on the Critical Success Factors of the company. The in-scope processes selected were the revenue generation process and the after sales support process.

With the scope set, the team put in place a two-level Business Continuity Plan (a Command-and-Control level, and a Business Process Recovery level) that involved business activities as well as IT and Facilities capabilities. In this particular case, there were good emergency policies and procedures already in place (covering things like evacuations, first responder notifications, etc.). There were also good IT problem handling procedures in place, covering everything from help desk calls to high impact problem resolution. The Command-and-Control instructions were coordinated with these existing policies and procedures.

Creation of Command and Control instructions began with understanding which sites are involved in the "in scope" business processes. Crisis Management Teams (CMT's) were named for each of these sites. These Command and Control instructions included roles for CMT members, priorities on meeting sites and team communication methods, resources for assessment of problem situations and priority setting. Communication is a major role of the CMT, both to the executives and the Board, as well as employees and outsiders (media, customers, etc.). A CMT was named for each site, since crises are most likely to be site oriented, and the best way to manage a crisis is "on the ground"

where the crisis has occurred. The CMT becomes the responsible management structure during a crisis. The CMT was given spending authority (up to a level) to facilitate the recovery.

The Business Continuity Planning process at the business process level is largely one of identifying dependencies. With the business processes identified, we focused on driving out the dependencies of those processes. A thorough understanding of the process is critical. This understanding is developed by defining, at a “medium” level of detail, the business process steps. Then each process step is examined IN GREAT DETAIL to understand what the process step is dependent upon. This was done iteratively. First, we drafted and cleaned up the process, using documentation (IT project flowcharts, ISO procedures, etc.). Secondly, we met with targeted business people to clarify areas of doubt, and to help drive out more dependencies. These dependencies include IT applications, IT core services (email, etc.), required manual documents and spreadsheets, work spaces and other facilities, outsourced manufacturing, etc., etc.

In order to keep the environment stable while plan development was going on, we established a target future point in time when the plan would be put into effect. Without this, the project can get mired in the day-to-day changes within a company, impeding forward progress.

After the dependencies were identified, line personnel from the business were consulted to understand how quickly these dependent resources were needed in order to resume the business process operation, initially at a reduced level. Having business line personnel buy into these recovery goals is critical “business validation” of your data and direction.

The BCP development team analyzed a broad spectrum of the company’s capabilities, including:

1. The ability of each department involved in the “in scope” business processes to maintain business process output in spite of high absenteeism (such as might occur during a pandemic).
2. Analysis of the need and availability of alternate work spaces (e.g. are all employees equipped to work from home? Has HR thought through the compensation implications of extended periods of working from home?).
3. The ability of each department involved in the “in scope” business processes to employ workarounds to keep the business process alive at a reduced level.
4. The ability of IT to recover applications and core services required by the “in scope” business processes.
5. The ability of key suppliers and outsourcers to recover (does their contract include business continuity/disaster recovery?).

With this data, we were in a position to create the two outputs of the Business Continuity planning process: 1) the recovery instructions themselves for each particular business process, and 2) the list of gaps in the recovery capabilities.

A “gap” might be, for example: the business may need a particular application system back in operation in eight hours to support the revenue generation process whereas, in fact, there are no comprehensive IT disaster recovery procedures in place, and recovering this application will take at least a week. Closing this gap becomes, obviously, a priority, if the BCP is going to be meaningful and of business value. This gap list was used, in this case, as an input to annual budgeting. Not all gaps resolutions were funded in the first budget cycle; however, awareness of the business continuity gaps was established.

Gap resolution does not necessarily involve expenditures. In the case of outsourced activities, closing the gaps may mean working with the supplier to develop and/or document their BCP. In our case, the large IT outsourcer was experienced in BCP and was agreeable to making contractual commitments in this area.

The final step in plan development was training and testing. Following the training, the applicable BCP documents were distributed to the teams. (The distribution of documents, in this case, was in hard copy form).

The first test was a simple conference room walkthrough with the teams. Some team members found the plan documents unclear or not user friendly. As a result of these testing walkthrough’s we created a “quick reference guide” accompanying each document. The testing also spawned a project to streamline the updating of cell phone address books with team member’s contact information. The objective of the test (and any test) was not to “grade” the effort but rather to find areas where the plans can be improved. As testing progresses, more complex tests can and should be done.

A side issue: It is better to mitigate the threats than to deal with the consequences. So far this case study has dealt with a plan for mitigation of the consequences of a disaster. We also established a priority list for funding on mitigation of threats. This is one place in Business Continuity Plan creation where scenario descriptions are required. We documented many scenarios, and assigned relative probabilities and impacts to them. This allowed a rank ordering by severity (probability x impact) and indicated where it would be most advantageous to make expenditures to mitigate the threat. For example, the probability, impact, and severity of power outages in a data center are well known. Data center management commonly mitigates this threat by having a secondary power generation facility on standby. Likewise, fire threats can be mitigated through training and inspecting for good housekeeping habits. Intentional data center sabotage can be mitigated by physical security and effective processes to “close-out” access privileges employees and contractors may have had. Some terrorist threats can be mitigated by installing physical barriers.