

Business Continuity Planning

Business Continuity Planning (BCP) is an interdisciplinary peer mentoring methodology used to create and validate a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical function(s) within a predetermined time after a disaster or extended disruption. The logistical plan is called a Business Continuity Plan.

In plain language, BCP is how an organization prepares for future incidents that could jeopardize the organization's core mission and its longterm health. Incidents include local incidents like building fires, regional incidents like earthquakes, or national incidents like pandemic illnesses. BCP may be a part of an organizational learning effort that helps reduce operational risk associated with lax information management controls. This process may be integrated with improving information security and corporate reputation risk management practices. A completed BCP cycle results in a formal printed manual available for reference before, during, and after disruptions have occurred. Its purpose is to reduce adverse stakeholder impacts determined by both the disruption's scope (who and what it affects) and duration (how bad, implications last for hours, months etc). Measureable business impact analysis (BIA) "zones" (areas in which hazards and threats reside) include civil, economic, natural, technical, secondary and subsequent. Prior to January 1, 2000, governments anticipated computer failures, called the Y2k problem, in important public utility infrastructures like banking, power, telecommunication, health and financial industries. Since 1983, regulatory agencies like the American Bankers Association and Banking Administration Institute (BAI) required their supporting members to exercise operational continuity practices (later supported by more formal BCP manuals) that protect the public interest. Newer regulations were often based on formalized standards defined under ISO/IEC 17799 or BS 7799. Both regulatory and global business focus on BCP arguably waned after the problem-free Y2K rollover. Some believe this lax attitude ended September 11th 2001, when simultaneous terrorist attacks devastated downtown New York City and changed the 'worst case scenario' paradigm for business continuity planning. BCP methodology is scalable for an organization of any size and complexity. Even though the methodology has roots in regulated industries, any type of organization may create a BCP manual, and arguably every organization should have one in order to ensure the organization's longevity. Evidence that firms do not invest enough time and resources into BCP preparations are evident in disaster survival statistics. Fires permanently close 44% of the business affected. In the 1993 World Trade Center bombing, 150 businesses out of 350 affected failed to survive the event. Conversely, the firms affected by the Sept. 11 attacks with well-developed and tested BCP manuals were back in business within days. A BCP manual for a small organization may be simply a printed manual stored safely away from the primary work location, containing the names, addresses, and phone numbers for crisis management staff, general staff members, clients, and vendors along with the location of the offsite data backup storage media, copies of insurance contracts, and other critical materials necessary for organizational survival. At its most complex, a BCP manual may outline a secondary work site, technical requirements and readiness, regulatory reporting requirements, work recovery measures, the means to reestablish physical records, the means to establish a new supply chain, or the means to establish new production centers. Firms should ensure that their BCP manual is realistic and easy to use during a crisis. As such, BCP sits along side crisis management and disaster recovery and is a part of an organization's overall risk management. The development of a BCP manual can have five main phases:

- Analysis
- Solution design
- Implementation
- Testing and organization acceptance Maintenance. The above list is not exhaustive. There are a number of other considerations that could be included in your own plan / manual: - Risk Identification Matrix - Roles and Responsibilities (ensuring names are left out but titles are included, e.g. HR Manager) - Identification of top risks and mitigating strategies. - Considerations for resource reallocation e.g. skills matrix for larger organizations. Much of the BCP material on the internet is sponsored by consultancies who offer fee-based services for BCP solution development, however basic tutorials are freely available on the internet for properly motivated organizations.

AnalysisThe analysis phase in the development of a BCP manual consists of an impact analysis, threat analysis, and impact scenarios with the resulting BCP plan requirement documentation.

Impact analysisAn impact analysis results in the differentiation between critical and non-critical organization functions. A function may be considered critical if the implications for stakeholders of damage to the organization resulting are regarded as unacceptable. Perceptions of the acceptability of disruption may be modified by the cost of establishing and maintaining appropriate business or technical recovery solutions. A function may also be considered critical if dictated by law. Next, the impact analysis results in the recovery requirements for each critical function. Recovery requirements consist of the following information:

- The time frame in which the critical function must be resumed after the disaster
- The business requirements for recovery of the critical function, and/or
- The technical requirements for recovery of the critical function

Threat analysisAfter defining recovery requirements, documenting potential threats is recommended to detail a specific disaster's unique recovery steps. Some common threats include the following: Disease Earthquake Fire Flood Cyber Attack Bribery Hurricane Utility outage Terrorism All threats in the examples above share a common impact: the

potential of damage to organizational infrastructure - except one (disease). The impact of diseases can be regarded as purely human, and may be alleviated with technical and business solutions. However, if the humans behind these recovery plans are also affected by the disease, then the process can fall down. During the 2002-2003 SARS outbreak, some organizations grouped staff into separate teams, and rotated the teams between the primary and secondary work sites, with a rotation frequency equal to the incubation period of the disease. The organizations also banned face-to-face contact between opposing team members during business and non-business hours. With such a split, organizations increased their resiliency against the threat of government-ordered quarantine measures if one person in a team contracted or was exposed to the disease. Damage from flooding also has a unique characteristic. If an office environment is flooded with non-salinated and contamination-free water (e.g., in the event of a pipe burst), equipment can be thoroughly dried and may still be functional.

Definition of impact scenarios After defining potential threats, documenting the impact scenarios that form the basis of the business recovery plan is recommended. In general, planning for the most wide-reaching disaster or disturbance is preferable to planning for a smaller scale problem, as almost all smaller scale problems are partial elements of larger disasters. A typical impact scenario like 'Building Loss' will most likely encompass all critical business functions, and the worst potential outcome from any potential threat. A business continuity plan may also document additional impact scenarios if an organization has more than one building. Other more specific impact scenarios - for example a scenario for the temporary or permanent loss of a specific floor in a building - may also be documented.

Recovery requirement documentation After the completion of the analysis phase, the business and technical plan requirements are documented in order to commence the implementation phase. A good asset management program can be of great assistance here and allow for quick identification of available and re-allocateable resources. For an office-based, IT intensive business, the plan requirements may cover the following elements which may be classed as ICE (In Case of Emergency) Data: The numbers and types of desks, whether dedicated or shared, required outside of the primary business location in the secondary location The individuals involved in the recovery effort along with their contact and technical details The applications and application data required from the secondary location desks for critical business functions The manual workaround solutions The maximum outage allowed for the applications The peripheral requirements like printers, copier, fax machine, calculators, paper, pens, etc. Other business environments, such as production, distribution, warehousing etc will need to cover these elements, but are likely to have additional issues to manage following a disruptive event.

Solution design The goal of the solution design phase is to identify the most cost effective disaster recovery solution that meets two main requirements from the impact analysis stage. For IT applications, this is commonly expressed as: The minimum application and application data requirements The time frame in which the minimum application and application data must be available Disaster recovery plans may also be required outside the IT applications domain, for example in preservation of information in hard copy format, or restoration of embedded technology in process plant. This BCP phase overlaps with Disaster recovery planning methodology. The solution phase determines: the crisis management command structure the location of a secondary work site (where necessary) telecommunication architecture between primary and secondary work sites data replication methodology between primary and secondary work sites the application and software required at the secondary work site, and the type of physical data requirements at the secondary work site.

Implementation The implementation phase, quite simply, is the execution of the design elements identified in the solution design phase. Work package testing may take place during the implementation of the solution, however; work package testing does not take the place of organizational testing.

Testing and organizational acceptance The purpose of testing is to achieve organizational acceptance that the business continuity solution satisfies the organization's recovery requirements. Plans may fail to meet expectations due to insufficient or inaccurate recovery requirements, solution design flaws, or solution implementation errors. Testing may include: Crisis command team call-out testing Technical swing test from primary to secondary work locations Technical swing test from secondary to primary work locations Application test Business process test At minimum, testing is generally conducted on a biannual or annual schedule. Problems identified in the initial testing phase may be rolled up into the maintenance phase and retested during the next test cycle.

Maintenance Maintenance of a BCP manual is broken down into three periodic activities. The first activity is the confirmation of information in the manual, roll out to ALL staff for awareness and specific training for individuals who's roles are identified as critical in response and recovery. The second activity is the testing and verification of technical solutions established for recovery operations. The third activity is the testing and verification of documented organization recovery procedures. A biannual or annual maintenance cycle is typical.

Information update and testing All organizations change over time, therefore a BCP manual must change to stay relevant to the organization. Once data accuracy is verified, normally a call tree test is conducted to evaluate the notification plan's efficiency as well as the accuracy of the contact data. Some types of changes that should be identified and updated in the manual include:

- Staffing changes
- Staffing persona

- Changes to important clients and their contact details
- Changes to important vendors/suppliers and their contact details
- Departmental changes like new, closed or fundamentally changed departments.

Testing and verification of technical solutionsAs a part of ongoing maintenance, any specialized technical deployments must be checked for functionality. Some checks include:Virus definition distribution Application security and service patch distribution Hardware operability check Application operability check Data verification

Testing and verification of organization recovery proceduresAs work processes change over time, the previously documented organizational recovery procedures may no longer be suitable. Some checks include:Are all work processes for critical functions documented? Have the systems used in the execution of critical functions changed? Are the documented work checklists meaningful and accurate for staff? Do the documented work process recovery tasks and supporting disaster recovery infrastructure allow staff to recover within the predetermined recovery time objective?

Treatment of test failuresAs suggested by the diagram included in this article, there is a direct relationship between the test and maintenance phases and the impact phase. When establishing a BCP manual and recovery infrastructure from scratch, issues found during the testing phase often must be reintroduced to the analysis phase.