Management in health
XXII/2/2018; pp. 18-20

BUSINESS CONTINUITY PLANNING ACTIVITIES (COOP)

Assoc. Prof. Nicolae Steiner MD, PhD
NATO International expert in Disaster Medicine
Former member of Health Security Committee of EU
Honrary member of National Disaster Medical System of USA

Planning the continuity of the work of governmental or regional authorities is an old concern of Civil Defense during the Second World War and long afterwards, expanding and improving continuously to the present day. This is because of the strategic importance of the problem.

Keywords: planning, strategy, continuity.

Continuity of activities, Planning, strategy.

Business continuity Planning (or business continuity and resilience planning) is the process of creating prevention and recovery systems to deal with potential threats to a company. [1]
Any event that may have a negative impact on operations is included in the plan, such as supply chain disruption, critical infrastructure loss or damage (major machines or computing / network resources). As such, the BCP is a subset of risk management. [2] In the US, government entities refer to the process as a continuity of operations planning (COOP). [3] A Business Continuity Plan describes a series of disaster scenarios and the steps the enterprise will take in any scenario to return to regular trade. Business Continuity Assurance Plans are written before and may include precautionary measures to be implemented. They are usually created with the help of key staff and stakeholders. Business Continuity Assurance Plan is a set of unforeseen situations to minimize potential business damage during adverse scenarios [4].

Current standards

In December 2006, the British Standards Institution (BSI) launched an independent standard for the Business Continuity Assurance (Business) Plan. Prior to the introduction of BS 25999, industry professionals relied on the BS 7799 Information Security Standard, which only approached the Business Continuity Assurance Plan (BUSINESS) of the activities to improve the procedures of the information security organization. The applicability of BS 25999 extends to all organizations. In 2007, BSI published the BS 25999-2 Business Continuity Management Specification document, which specifies the requirements for the implementation, operation and improvement of a documented business continuity management system (Business Continuity Management (BCMS)).
Business Continuity Management is standardized in the UK by British Standards (BS) by BS 25999-2: 2007 and BS 25999-1: 2006. BS 25999-2: Business Continuity Management 2007 is the UK Business Continuity Management Standard in all organizations. This includes industry and its sectors. The standard provides a framework of best practices to minimize disturbances during unexpected events that could bring businesses to a standstill. The document provides a practical approach to addressing most of the possible situations - from extreme weather to terrorism, IT system failure and staffing [5].

This document was superseded in November 2012 by the British Standard BS ISO22301: 2012, the current standard for business continuity planning [6]

Civil Emergency Law

In 2004, following the crises of previous years, the British government adopted the Civil Emergency Law of 2004 (the Act). It provides for UK civil protection legislation: Enterprises must have continuity planning measures to survive and continue to thrive while working to keep the incident as low as possible [7].

The law was divided into two parts: Part 1 focuses on local civil protection arrangements, setting a legal framework for roles and responsibilities for local respondents. The second part focused on emergency skills, setting a modern framework for the use of special legislative measures that may be needed to cope with the worst emergency situations.

Analysis

The analysis phase consists of impact analysis, threat analysis and impact scenarios.

Business Impact Analysis (BIA)

Business Impact Analysis (BIA) differentiates critical (urgent) functions from non-critical (non-urgent) activities. Critical functions are those whose disruptions are considered unacceptable. Perceptions of acceptability are affected by the cost of recovery solutions. A function can also be considered critical if it is dictated by law. For each critical function (within the scope), two values are assigned:

Point of Recovery (POR)

Acceptable latency of data that will not be recovered. For example, is it acceptable for the company to lose 2 days? [8]

The recovery time goal (RTO)

Acceptable time for restoring the function.

The objective of the recovery point must ensure that the maximum loss of tolerable data for each activity is not exceeded. The recovery time goal must ensure that the maximum perturbation tolerance period (MTPoD) for each activity is not exceeded.

Further, the impact analysis results in the recovery requirements for each critical function.

Recovery requirements consist of the following information:

- Business requirements for critical function recovery and / or
- Technical requirements for critical function recovery.

Hazard and Hazards Analysis (HHA)

The impact of an epidemic can be seen as purely human and can be mitigated by technical and business solutions. However, if the people behind these plans are affected by the disease, then the process may sting.

During the 2002-2003 SARS epidemic, some organizations grouped staff into separate teams and rotated teams between primary and secondary workplaces with a rotation frequency equal to the incubation period of the disease. Organizations also prohibit face-to-face interprofessional contact during business and non-business hours. Clearing has increased resistance to the threat of quarantine if a person in a team has been exposed to the disease.

Impact scenarios.

After identifying the applicable threats, impact scenarios are considered to support the development of a business recovery plan. Business Continuity Test Plans can document scenarios for each identified threat and impact scenarios. Several localized impact scenarios - eg loss of a specific floor in a building - can also be documented. Business (Business) Activity Plans should reflect the requirements to recover the business with the most possible damage. The risk assessment should contribute to the development of impact scenarios applicable to the enterprise or premises in which it operates. For example, it might not be logical to consider the tsunami in the Middle East because the likelihood of such a threat is negligible.

Recovery requirements

After the analysis phase, requirements for the recovery of commercial and technical activities precede the solution phase. Asset inventories allow quick identification of available resources. For an office-based and intensive IT business, plan requirements can include offices, human resources, applications, data, manual solutions, computers and peripherals. Other business environments such as production, distribution, storage, etc. will have to cover these elements, but they will probably have additional problems.

The robustness of an emergency management plan depends on the amount of money that an organization or an enterprise can place in the plan. The organization must balance realistic feasibility with the need for appropriate training. Generally, every $ 1 entered into an emergency management plan will prevent the loss of $ 7. [9]

Design solution

The solution design stage identifies the most cost-effective disaster recovery solution that meets the two main requirements of the impact analysis phase.

For IT purposes, it is typically expressed as the minimum application and data requirements and when the minimum application and application data must be available.

Outside the IT field, it is important to consider keeping paper information, such as contracts, qualified personnel, or restoring the technology embedded in a processing plant. This phase overlaps with the methodology of disaster recovery planning.

The solution phase determines:

- crisis management command structure;
- secondary jobs;
- Telecommunication architecture between primary and secondary jobs;
- Data replication methodology between primary and secondary jobs;
- Applications and data requested at the secondary workplace;
- physical data requirements at the secondary workplace.

Applying

Implementation phase involves policy changes, material purchases, personnel and testing.

Organizational testing and acceptance

The purpose of the tests is to obtain organizational acceptance that the solution meets the recovery requirements. Plans may fail to meet expectations due to insufficient or inaccurate recovery requirements, design solution failures, or solution implementation errors. Testing may include:

The crisis command team calls for testing

The technical swing test from primary to secondary jobs

Technical swing test from secondary to primary locations

Management in health
XXII/2/2018; pp. 18-20

Mass Exercises

Table exercises typically involve a small number of people and focus on a specific aspect of a BCP. They can easily host complete teams in a particular business area.

Another form involves a single representative from each of several teams. Typically, participants work through simple scenarios and then discuss specific aspects of the plan. For example, a fire is discovered from work hours. The exercise consumes only a few hours and is often divided into two or three sessions, each focusing on a different theme.

Average exercises

An average exercise takes place in a "virtual world" and brings together several departments, teams or disciplines. It usually focuses on several aspects of the BCP, determining the interaction between teams. The scope of an average exercise may range from several teams in an organization co-located in a multi-team building that operates in dispersed spaces. The environment must be as realistic as possible and the size of the team should reflect a realistic situation. Realism can extend to simulated news shows and websites.

An average exercise usually takes a few hours, although these may extend over several days. These typically involve a "scenario cell" that adds pre-scenarios of "surprises" throughout the exercise.

Complex exercises

A complex exercise aims to have as few limits as possible. Includes all aspects of an average exercise. Exercise stays in a virtual world, but maximal realism is essential. This may include unannounced activation, actual evacuation, and the actual invocation of a disaster recovery site.

While start and stop times are pre-arranged, the actual duration may be unknown if events are allowed to run.

Maintenance

Maintaining the biannual or annual maintenance cycle of the BCP manual is divided into three periodic activities.

Confirmation of testing and verification

Testing and verifying the technical solutions set up for recovery operations. Elements found during the test phase should often be reintroduced into the analysis, information and targets as well. The BCP manual must evolve with the organization. Enable the call tree checks the effectiveness of the notification plan, as well as the accuracy of the contact data. Like most business processes, business continuity planning has its own jargon. Understanding the business continuity jargon is vital and glossaries are available. [10] The types of organizational changes that should be identified and updated in the manual include: • Staff • Major customers • Suppliers / suppliers • Changes in organization structure • Company investment portfolio and mission statement • Communication and transport infrastructure such as be roads and bridges

Technical resources

Special technical resources should be maintained. Controls include:

- Distributions of virus definitions;
- Application security and patch service distribution;
- Hardware functionality;
- Application functionality;
- Checking data;
- Applying data.

Testing and verifying recovery procedures

As work processes change, previous recovery procedures may no longer be appropriate. Controls include:

- Are all working processes for critical functions documented?
- Have the systems used for critical functions changed?
- Are document checklists documented meaningfully and accurately?
- Are the objectives of recovering the documented work process and supporting disaster recovery infrastructure enable staff to recover during the predetermined recovery target?

References:

1. ***Business Continuity Planning, FEMA***, Retrieved: June 16, 2012
2. ***Continuity of Operations Planning (no date).*** U.S. Department of Homeland Security. Retrieved July 26, 2006.
3. ***Purpose of Standard Checklist Criteria For Business Recovery (no date).*** Federal Emergency Management Agency. Retrieved July 26, 2006.
4. ***NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs*** — PDF[*dead link*] (2010). National Fire Protection Association.
5. ***United States General Accounting Office Y2k BCP Guide (August 1998).*** United States Government Accountability Office.
6. JAMES C. BARNES. ***A Guide to Business Continuity Planning.*** ISBN 978-0471530152.
7. KENNETH L FULMER. ***Business Continuity Planning, A Step-by-Step Guide***. ISBN 978-1931332217.
8. RICHARD KEPENACH. ***Business Continuity Plan Design, 8 Steps for Getting Started Designing a Plan.***
9. JUDY BELL. ***Disaster Survival Planning: A Practical Guide for Businesses***. *ISBN 978-0963058003.*
10. DIMATTIA, S. ***(November 15, 2001). Planning for Continuity.***"Library Journal: 32–34.