Agris on-line Papers in Economics and Informatics

Volume III Number 4, 2011

Disaster Recovery Planning as part of Business Continuity Management

J. Pinta

Department of Information Engineering, FEM CULS in Prague

Abstract

Nowadays, a well functioning ICT infrastructure belongs to the most critical factors of companies across all branches of business. An importance of ensuring the continued operation of information systems, or the rapid recovery of the systems in the case of emergency, has increased. These needs require creating business continuity management plan and disaster recovery planning. This paper describes the creation of emergency and recovery plans and setting recovery objectives significantly affecting their efficiency.

Key words

Business Continuity Plan (BCP); Disaster Recovery (DR); Recovery Measures

Anotace

Fungování ICT infrastruktury je dnes pro většinu podniků kritickým faktorem a je zde kladen stále větší důraz na zajištění jejího provozu a dostupnosti, stále častěji spojovanou s plánováním rychlé obnovy chodu ICT během havarijní situace a jejího uvedení do stavu před touto událostí. Této problematice se věnuje řídící proces Řízení kontinuity činností organizace, který zahrnuje i oblast havarijního plánování ve vztahu k informačním technologiím jako kritickému zdroji v organizaci. Toto plánování je nazýváno Řízení kontinuity IT služeb (IT Service Continuity Management) nebo také Plánování obnovy ICT (Disaster Recovery Planning). Tento příspěvek popisuje tvorbu havarijních plánů a stanovení parametrů zásadně ovlivňujících jejich efektivitu.

Klíčová slova

Řízení kontinuity, havarijní plány, plány obnovy, parametry strategie obnovy.

Introduction

The operation of ICT systems is important part of most businesses. Given the increasing dependence of enterprises on IT services and information systems this part of the infrastructure becomes more critical and it is important to ensure business continuity and availability of these systems and also ensure high-quality preparation of their fast recovery in case of emergency situations. Increasing demands for availability of these resources generates requirements for the continuity of ICT (Business Continuity), and these requirements result in creating plans for Business Continuity Management, which are also part of emergency and recovery plans ICT (Disaster Recovery Planning). However, the construction and following usability and success of these plans depends on many factors. What are the prerequisites and requirements for quality recovery plans? What should the plans contain? How to test their applicability in business environment?

Methodology

During the implementation of BCM and DRP is important to pay attention to two facts. The first is of course expected knowledge of the issues and terminology, good orientation in an environment where the implementation of this style of management will be performed and finally allocating resources and determining the roles. The second important task is a plan creation itself according to individual needs of the organization or company, including setting of all key parameters.

This paper describes both the mentioned facts. According to BS 25999 standards describes and outlines a possible way of preparing the organization before the introduction and implementation of those plans according to business continuity planning life cycle, as well as an explanation of the role and possibilities of establishing relevant functions and parameters for their implementation.

BCM

Firstly, it is important to become familiar with the concept of Business Continuity Management (BCM) and unify the meaning of related terms.

Business continuity management is the planning process and identification of potential impacts of internal and external threats and consequential losses, which could be due to disruption or loss of key business processes from the accident, attack or disaster. BCM has evolved in response to the technical and operational risks that threaten an organisation‘s recovery from hazards and interruptions as a form of crisis management since the 1970s (Herbane 2010). This managerial discipline establishes operational and strategic framework, adapted to the needs of the organization, ensuring continuous improvement and resistance to mentioned disruption. These disruptions can be predictable and unpredictable character. The most frequently reported incidents and emergency events could be of different nature and scale, classified as short-term interruptions such as power outages, minor faults in the network, or failure of any element in the technological chain, as well as mid serious events, which may be e.g. fire in a room, to the real accident with devastating effect in the form of floods, cyber attacks, theft of equipment or loss of sensitive data. All of these threats, including many others, have a common effect in the form of threat to the continuity of the processes of the organization. This deals with “Use of simulation in a factory for Business Continuity Planning” (Tan, Takakuwa 2011) following: “Companies can suffer significant losses as a result of unanticipated business disruptions caused by natural disasters or outbreaks of disease. In order to restore the organization‘s critical functions and minimize the impacts of a disruption, it is important to establish business continuity planning and recovery planning.” The aim is to create a plan and an environment that ensures continuity and recovery of critical processes at a predetermined minimum level, ideally to the original level. In addition to solution and recovery consequences caused by those incidents or accidents, it is also about prevention and planning how to prevent these threats, both as a preventive actions (redundancy, virtualization, backup, spare parts and spare buildings) as well as setting policy organization and expanding awareness of these plans and procedures. In short, in the case of an accident implemented business continuity management is used for recovery operations with minimal negative impact on the performance as quickly as possible according to requirements of business plans, contractual obligations to customers or legislation.

2.1. BS 25999

The uniform standard that describing the correct procedure for incorporating BCM into the infrastructure of the organization was published in 2006 in Great Britain under the name „BS 25999 - Code of Practice for Business Continuity Management“ by British standards Institute (BSI), in collaboration with the Business Continuity Institute (BCI). This standard consists of two parts, the first section labelled „BS 25999-1:2006 Code of practice for business continuity management“ [1] establishes the general principles, terminology and recommendations for implementation of the BCM in an organization. The second part, published in 2007, called „BS 25999-2:2007 Specification for business continuity management“ [2] describing the requirements for certification of business continuity management and requirements that can be objectively and independently audited.

2.2 Business Continuity Planning Life Cycle

Complete processing and final form of business continuity plan will vary according to the needs and nature of the organization. And this fact is essential to business continuity planning (BCP), BCM according to BS 25999-1:2006 can be implemented in all types of organizations regardless of size or area of business. It is important to compliance with the recommendations and standardized continuity. In BCM, this management process is called the business continuity life cycle. For proper functioning of business continuity management is important to its integration into all levels of an organization from top management (BCM support, set the scope and objectives, resource reservation...) to average workers through training, awareness and overall consciousness raising of its importance. The top management of the organization has responsibility of the functioning of the entire organization just as a business continuity management. There should be a designated manager responsible for the complete program of BCM.

The individual steps of BCM life cycle (Fig. 1) and subsequent implementation are as follows:

Understanding and awareness activities in the organization

This step in the process of business continuity management, primarily including an analysis of

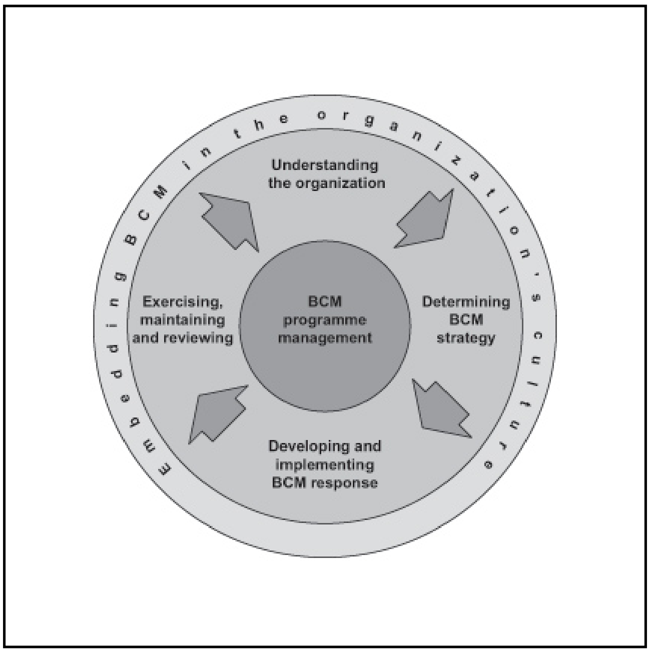
Embedding BCM in the organization's culture
Understanding the organization
Determining BCM strategy
Developing and implementing BCM response
Exercising, maintaining and reviewing
BCM programme management

Figure 1: BCM life cycle.

the current situation, consists of several sub-steps, which have a crucial influence on the efficiency generated by the plan, and therefore is placed maximum emphasis on the consistency of their implementation. These individual steps are as follows:

- Statement and willingness of management to implement the project, determine the structure of the project and way of its leadership.
- Identification of key processes, resources and critical activities of an organization that directly affect business continuity and delivery of products or services to the customer.
- Business Impact Analyses (BIA) is intended to separate the important (critical) functions and activities of the organization from the less important (non-critical). The function can be considered important when the threat can cause unacceptable risk to the results of the organization. The function can also be considered critical if it is subject of law. Primary results of the analysis used in the next step of implementation of BCM are to set Maximum Tolerable Period of Disruption (MTPD) and Maximum Tolerable Data Loss (MTDL). For each critical function are also assigned two values - Recovery Time Objective (RTO), which represents the maximum acceptable amount of time to restore function, together with the Recovery Point Objective (RPO) indicating the maximum acceptable level of data loss. The established RPO must ensure that MTDL not exceeded for any activity. Similarly, the RTO to ensure that the MTPD is not exceeded. Process of RTO and RPO parameters setting will be given later in this article.
- Threat Analysis is the next recommended step in the form of documentation of potential threats, along with detailed specifications of the individual steps of recovery. The most frequently mentioned threats are discussed in chapter 2.
- Risk Assessment is the quantitative or qualitative determination value of risk associated with specific situations and documented threats. Quantitative risk assessment requires calculation of two components - the risk and size of potential losses, together with the probability that the loss occurs. Methods of risk assessment varies according to the defined objectives of the organization in various sectors, along with a defined financial plan and taking into account possible threats in the sense public health, environment and ecology.
- The final selection of appropriate risk management measures to reduce their probability of occurrence, time minimizing disruption and impact on critical processes of the organization.

Determination of BCM strategy

Following the previous steps an appropriate strategy should be designed at this stage to identify possible forms of incidents and responses to them. Reaction means the activation of business continuity plan (BCP) and the subsequent variations and methods of recovery of critical activities in defined times.

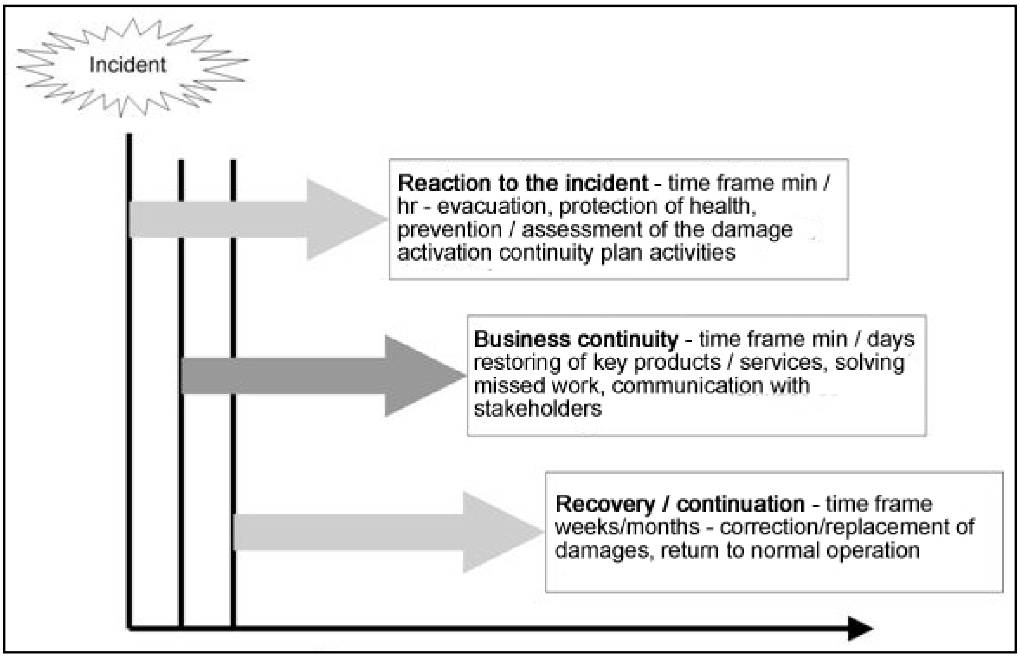
Incident
Reaction to the incident - time frame min / hr - evacuation, protection of health, prevention / assessment of the damage activation continuity plan activities
Business continuity - time frame min / days restoring of key products / services, solving missed work, communication with stakeholders
Recovery / continuation - time frame weeks/months - correction/replacement of damages, return to normal operation

Figure 2: Timeline response to the incident.

The objective is to establish such procedures, under which an organization would be able in the shortest possible time to react to a certain incident, maintain control over the situation and ensure the required level of continuity of critical activities. To determine these strategies is essential to plan engagement, the type and amount of key resources such as people, finance, alternative energy sources and technologies, and contracted third party services.

Among other things, it is generally recommended to consider the following scenarios when creating strategies:

- Impossibility of physical presence in the building;
- Lack of human resources;
- Failure of technology and equipment necessary for the operation and provision of services;
- Failure of a key service provider.

Development and implementation of BCM

At this stage of the BCM lifecycle is a major step the establishment and implementation of the plans previously built according to analysis and strategies of organizations whose objective is to maintain, or in the shortest time possible recovery of critical processes to an acceptable level in case of their violation. For smaller organizations may be quite sufficient only one comprehensive plan of continuity, while larger organizations may prefer more interconnected plans, either because of the division of roles and responsibilities, as well as simplicity and clarity.

Another integral part of development of BCM is the definition of authorities and responsibilities of participants in the form of emergency management roles and group roles. These can be divided as follows:

- Crisis team.
- Coordination team,
    - a team leader,
    - a team member.
- Operational team,
    - a team leader,
    - a team member.

On the basis of determined roles is necessary to determine who is responsible for electing a crisis team (e.g. leadership organization for crisis management). Furthermore, to determine for what actions is coordinating team responsible, who are members and their representatives, when those representatives are taken on their roles, as well as the determination that the team leader is responsible for tasks coordination team, setting tasks for individual team members, managing the tasks of the coordinating team and ensuring conditions for the efficient performance of tasks of the coordinating team according to technological and organizational perspective. Similar definition of responsibility is necessary to provide for the operating team, its leaders and individual members.

From the perspectives of authorities is necessary to determine their purpose and scope, conditions and procedures for activating the plans, the choice of alternative sites, including the redeployment plan, order and sequence of tasks, a list of important contacts and suppliers of services provided by third parties.

Testing, maintenance and revision of BCM

The objective of this phase of the BCM life cycle is to create a testing program, which is consistent with the subject of business continuity plan. Testing helps especially revealing any discrepancies and omissions before they are used in case of accident. Also serve as a tool used to check the completeness and functionality of the business continuity plan(s), is also used for prediction and subsequent control of various forms of accidents that allows an organization to develop innovative solutions. Each operational team is responsible for testing disaster management and also for reporting the results to coordination team. Coordination team is entitled to change the scope and method of testing. Each test should have clearly defined goals and objectives. After the testing should be organized a meeting to analyse results, where the achievement of goals and objectives of testing will be discussed. After that a report containing recommendations and a timetable for implementation measures should be created. The scope and complexity of testing should be appropriate to the recovery goals of the organization activities. Business continuity plans should be tested, to ensure that they can be properly carried out and that contain the details and instructions. Testing and inspection plans should take place at regular intervals, according to the schedule approved by senior management organization or whenever significant changes occur that may affect business continuity of the organization. Testing should not cause disruption and thus endanger the organization by itself. The course of each test must be recorded in detail; all activities and test results must then be reviewed. Testing can take various forms due to the complexity, process control, and subsequent changes, as well as frequency, or. regularity of its implementation. For an idea may serve the following models:

- Basic check of continuity plan called „from the desk“ - reviewing content, raising objections to the status quo - audit / verification and subsequent updates - at least once a year;
- Mid-complex simulations of individual parts - the use of artificial situations in a lab environment designed to validate the expected results - as needed once or twice a year;
- Mid-complex testing of critical activities - causing controlled situation in a production environment that will not disrupt the normal functioning of the organization - as required annually or less frequently;
- Complex business continuity plan testing - testing across the organization, building, complex of buildings or areas - once a year.

DRP

A special chapter in the BCM is emergency planning in relation to information technology as a critical resource in the organization. This plan is called the IT Service Continuity Management and Disaster Recovery Planning as well. There are combined technological capabilities to ensure recovery of hardware and software, but also some elements from the above methodology. Indicators of Recovery Time Objectives type (RTO) and Recovery Point Objectives (RPO) help us to define the real requirements to ensure operation of our systems and propose appropriate solutions to these requirements. The expected outcome is pre-defined priority recovery of IT functions and components, critical path for their recovery, including the duration of each step.

Strategies

After the impact analysis and risk analysis is needed to build recovery strategy. This involves setting RTO and RPO parameters with regard to the analysis impacts. As mentioned, the RTO (Recovery Time Objective) represents the maximum acceptable outage time business process, RPO (recovery point objective) the maximum allowable data loss for a defined time. Both parameters can be different.

If the strategy is defined and critical business processes are identified, including links to ICT technologies, then is created a list of technical and organizational measures whose implementation costs must be balanced with the cost of impact analysis. The technical part is about investment in infrastructure, UPS, alternative locations, etc. The organizational measures are about updating of existing internal documents, users familiar with their duties and responsibilities, changes in contractual relationships with suppliers that reflect the new demands for services supplied, etc. In short, RTO and RPO therefore helps to avoid unnecessarily costly measures, e.g. is not needed nuclear cover on a server room, if there is a duplicate one in another location and RTO is set to 24 hours. Optimal expenditures are shown in figure 3.

Disaster recovery plan

Disaster recovery plan describes the activities that need to begin to implement immediately after detection of an incident for which a DRP is drawn up (e.g. air conditioning failure in the datacenter). It must be mentioned in them, who can run the emergency plan, who participates this plan, what is the purpose of the plan and what is the target state after implementation of the emergency plan. The Recovery Plan assumes completion of the disaster (emergency) plan. It is a technically oriented plan designed for ICT workers, which allows recovery of ICT business processes and return to normal operation. Emergency operation plan defines the working methods and activities that can keep critical business processes at least on a limited level until the information system is restored so that the impact on the operation of the organization is minimal. Defines alternative techniques, which perform critical activities without ICT for a specified period of time. The plans should include the approximate timeline of the sequence of events leading to fulfilment of RTO and RPO. To ensure quality, efficiency and up-to-date of business continuity management process is needed maintenance, testing and updating plans and further education of interested users focused on understanding the processes associated with the DRP.

Conclusion

As already mentioned, the dependence of enterprises on ICT infrastructure across all sectors is increasing. Many organizations did not feel the need to to deal with the DRP in the past, because the dependence on ICT was not so big and production could run for some time regardless of a data network in the organization. With the advent of new technologies for manufacturing automation and production is growing demand for cooperation with ICT. Due to the mentioned dependence is therefore necessary to plan and think about situations that may arise as a result of accident or disaster and try to avoid these situations by business continuity and DRP. For example, even in the classic and often conservative environment of agricultural holdings the trend of ICT usage is still on the rise and companies implements and uses these technologies both in production and for common use such as web browsing, e-mail, e-banking, etc. (Šimek, Vaněk, Jarolímek, 2008). Along with the implementation of these technologies and their increasing dependence (e.g. collection of data stored in the database, the implementation of ERP systems, data evaluation for future development, etc.) is thus important to protect critical data and to keep business continuity in case of disruptions or threats. Therefore, even here in the agricultural environment, is important to think about potential threats and plan for possible situations, and especially their progress and solutions using BCP and DRP. It is always important to make these plans individually to the needs of the organization and to find the optimal amount of costs and determine the maximum tolerable period of disruption and recovery time from which the specific measures will be based on. To determine the optimal amount of costs are available properly set up parameters RTO and RPO. The specific results of the chosen strategy may

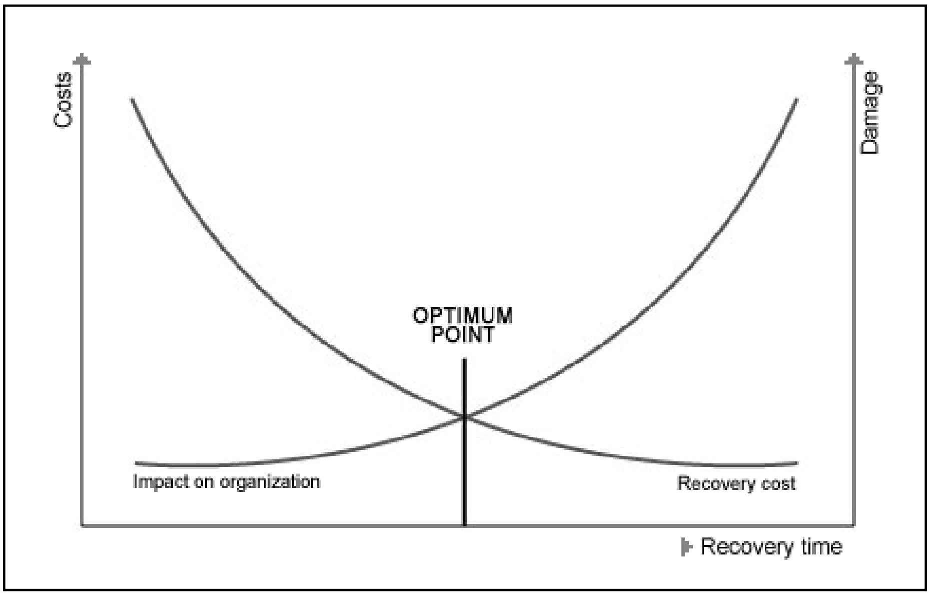

Figure 3: Optimal spending on business continuity.

include, for example, settings of backup policy, data replication, high availability systems, active and passive devices, Local mirrors of systems and/or data and use of disk protection technology such as RAID technology, implementation of surge protectors and uninterruptible power supplies and backup generator eventually, fire protection, server virtualization for easier backup and recovery (the recovery time decreases from the order of hours to order of minutes in this case), database server backup and eventually redundant instance of ERP system, suitable anti-virus and firewall protection, etc. This short list is far from definitive, and as already mentioned, it is necessary to create suitable and optimized solutions to the needs and possibilities of each particular company or business.

Corresponding author:
Jan Pinta
Department of Information Engineering, FEM CULS in Prague
Kamýcká 129, 165 21 Praha 6 - Suchdol
pinta@pef.czu.cz

References

[1] BS 25999-1:2006, Business continuity management – Part 1: Code of practice. London: British Standards Institution, 2006.

[2] BS 25999-2:2007, Business continuity management – Part 2: Specification. London: British Standards Institution, 2007.

[3] Cannon, L. David. CISA Certified Information Systems Auditor STUDY GUIDE, Second Edition. Wiley Publishing, 2008, ISBN: 978-0-470-23152-4.

[4] Herbane, B. (2010): The evolution of business continuity management: A historical review of practices and drivers. Business history. 52(6): 978-1002. ISSN: 0007-6791.

[5] Neudorfer, W. - Marinos, L. - Schaumuller-Bichl, I. (2010): Business and IT Continuity Benchmarking. Communications and multimedia security, proceedings / Lecture Notes in Computer Science. 118-129. ISSN: 0302-9743. ISBN: 978-3-642-13240-7.

[6] Office of Government Commerce (OGC). Continual Service Improvement. TSO (The Stationery Office), 2010, ISBN: 978-0-11-331049-4.

[7] Office of Government Commerce (OGC). Service Design. TSO (The Stationery Office), 2007, ISBN: 978-0-11-331047-0.

[8] Office of Government Commerce (OGC). Service Strategy. TSO (The Stationery Office), 2007, ISBN: 978-0-11-331045-6.

[9] Office of Government Commerce (OGC). The Introduction to the ITIL Service Lifecycle, 2nd Edition. TSO (The Stationery Office), 2010, ISBN: 978-0-11-331131-6.

[10] Sharp, John. Jak postupovat při řízení kontinuity činností. Praha: Risk Analysis Consultants, 2009. ISBN 978-80-254-3992-0.

[11] Tan, Y., Takakuwa, S. (2011): Use of simulation in a factory for Business Continuity Planning. International Journal of Simulation Modelling. 10(1): 17-26. ISSN: 1726-4529.

[12] Šimek, P., Vaněk, J., Jarolímek, J. Information and communication technologies and multifunctional agri-food systems in the Czech Republic. Plant, Soil and Environment, 2008, roč. 54, č. 12, s. 547 - 551. ISSN: 1214-1178.

[13] Vaněk, J., Jarolímek, J., Šimek, P. ICT technologie v českém zemědělství. Zemědělec 33/09 – Informační a komunikační technologie [online]. 2009, 9, [cit. 2011-11-28]. Available at: < http://www.agroweb.cz/ICT-technologie-v-ceskem-zemedelstvi__s403x34314.html>.