DESIGNING A MODEL OF BUSINESS CONTINUITY POLICY IN AN ORGANIZATION BASED ON MACHINING BUILDING DESIGN

Alina Bianca POP[a] , Ștefan ȚÎȚU[b], Aurel Mihail ȚÎȚU[c*], Gheorghe Ioan POP[d], Sebastian STAN[e]

[a] SC TEHNOCAD SA, Baia Mare, România
[b] The Oncology Institute "Prof. dr. Ion Chiricuță", Cluj-Napoca, România
[c] Lucian Blaga University of Sibiu, Romania
[d] SC Universal Alloy Corporation Europe SRL, Dumbrăvița, România
[e] Nicolae Bălcescu Land Force Academy, t, Sibiu, România

ABSTRACT

The activity continuity of any organization contributes to increasing the society resilience. The purpose of this paper is to present the importance of designing and implementing a policy and action plan to be undertaken by designated personnel within an organization with a field of activity - designing in machine building in the event of an emergency situation. In this paper are presented some aspects regarding the organization preparation in the event of activity disruptions caused by uncontrollable factors, like: natural disasters, unexpected attacks, serious accidents, etc. to return, as soon as possible, with minimal loss to the normal business course. This research identifies the vulnerabilities and recommends the necessary measures to prevent the disruption of the organization's activities. The presented issues should be followed by the organization's management in case of significant incidents of activity discontinuation with a view to resuming it without significant loss or with minimal consequences.

KEYWORDS: *building, business continuity policy, business continuity plan, machine, organization.*

1. INTRODUCTION

Business continuity and disaster recovery planning are critical activities for organizations of any size. Rather than addressing problems only after a crisis strikes, a business continuity policy can help the organization recover from a disaster faster and get the systems up and running more smoothly (Free business continuity policy template, 2018).
Business continuity planning is the process of creating systems of prevention and recovery to deal with potential threats to a company. Any event that could negatively impact operations is included in the plan, such as supply chain interruption, loss of or damage to critical infrastructure (major machinery or computing /network resource). As such the business continuity plan is a subset of risk management (Intrieri, 2013).
The three basic elements every business continuity policy should address are resilience, recovery and contingency planning (Free business continuity policy template, 2018). As the (Free business continuity policy template, 2018) says "Business continuity and disaster recovery are two sides of the same coin". In figure 1 is presented the business continuity and disaster recovery planning.

* Corresponding author. E-mail address:mihail.titu@ulbsibiu.ro

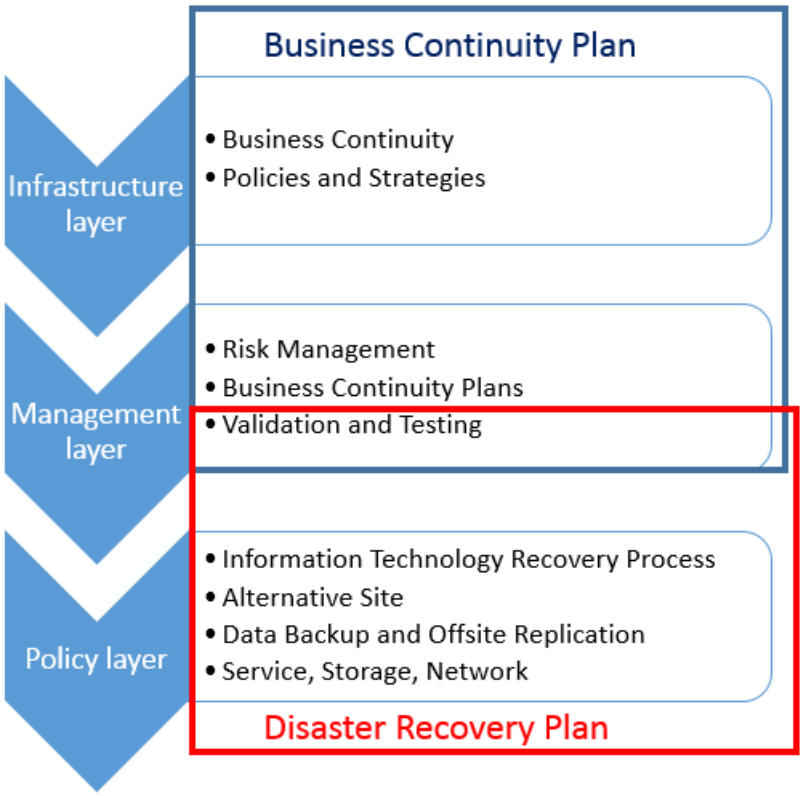

Figure 1. Business continuity and disaster recovery planning
Source: author after Kirvan and Miller (2017)

2. BUSINESS CONTINUITY POLICY- CREATING STEPS

The necessary steps to create a business continuity policy are the following (Free business continuity policy template, 2018):
- To make the top management aware of the plan and get their approval;
- Outline emergency action steps to take in case of an incident;
- Detail the types of incidents that will launch the business continuity plan;
- List key business processes to protect;
- Specify critical technologies to safeguard;
- Recovery point objectives;
- Identify key vendors, stakeholders, regulators and other third parties;
- Implement step-by-step procedures for various recovery activities;
- Develop processes for procuring emergency funds;
- Compile lists of vital records the organization requires to operate;
- Include references to all business recovery activities, such as data backup procedures and those for training, updating, testing, auditing and reviewing your business continuity strategies and plan.

3. THE BUSINESS CONTINUITY POLICY COMPONENTS

Most of the organizations wants their policies for business continuity and disaster recovery be relatively simple. The components of the continuity management policy outline are:
- An introduction that states the fundamental reasons for having a business continuity policy;
- The policy's purpose and scope;
- Statement of policy with clear and unambiguous terms;

- Policy leadership which states who is responsible for approving and implementing the policy, as well as levying penalties for noncompliance;
- Verification of policy compliance;
- Penalties for noncompliance;
- Other additional reference information (lists of contacts, service-level agreements and additional details on specific policy statements).

4. CASE STUDY

4.1. The activity continuity policy

The business continuity management process must embrace risk, emergency, and recovery planning if an organization is going to be able to manage a crisis or disaster event and have any hope of returning to business as usual operations. Undertaking any of the above business continuity activities should form part of a wider planning structure and process and is not an end in itself, but rather a means to an end (Doughty, 2001).

Others relevant references on recent literature which shows the interest of researchers on this topic belong to Cliff Ferguson (Ferguson, 2018), Hojat Rezaei Soufi (Hojat et al., 2018), Engemann (Engemann, 2018) and Zhiguo Zeng and Enrico Zio (Zeng & Zio, 2017)

Today, business continuity plans are no longer a luxury, but an essential element of the organization's risk management program. For many organizations, the decisions to invest in a business continuity plan is being forced upon them (Doughty, 2001).

Next, a business continuity policy implemented in an organization based on the machine building assisted design, will be presented.

The organization in which the case study was made, has the competence, technical and human capacity necessary to carry out the computer-aided design in three directions: Mechanical Engineering Design (CAD / CAM / CAE); design in the field of geographic information systems and multimedia design. Therefore, it is essential for this society to maintain the ability to carry out key activities in line with the expectations of the main stakeholders.

The business continuity policy is based on EN ISO 27031:2014 (Elliot et al., 1999).

The business continuity policy is to maintain the business continuity capabilities to ensure a prompt and efficient recovery of essential activities caused by any physical incidents or disasters. The incident response capability is periodically tested.

The roles and responsibilities of each authorized member which is responsible for the management of perturbation incidents are clearly defined.

Methods and procedures are documented, communicated and effectively measured.

The purpose of the company's Continuity Policy is to prepare the organization in the event of activity disruptions caused by uncontrollable factors like natural disasters, unforeseen IT attacks, serious personal injury, etc. to return, as soon as possible, with minimal losses, to the normal business course.

The key objectives of the Company's Continuity Policy include ensuring that the organization's key services are available in line with stakeholders' expectations and business objectives, as well as maintaining the organization certification and good reputation on the market.

4.2. The business continuity plan

The studied organization has defined its own business continuity plan and this subject issues are presented below.

In this business continuity plan the vulnerabilities are identified and the necessary measures are recommended to prevent the disruption of the company's activities.

The presented issues of this plan should be followed by the company's management in case of significant incidents of activity discontinuation with a view to resuming it without significant loss or minimal consequences. However, the plan's purpose is limited to issues described. The presented

plan is not a document with procedures in order to solve the daily company problems. This document is kept in a safe place and is immediately accessible after a disaster. Disaster represents any loss of utilities (energy, water, gas, etc.), connectivity (locations of communications system on various environments), or catastrophic events (weather, natural disasters, vandalism) causing an interruption in the activities and services offered by the company.

The main objectives pursued by the plan:

- To be a guide for rescue teams;
- Present the critical data points and places;
- Indicate the procedures and resources needed to restore the situation after interruptions;
- Identify providers and customers to be notified in case of disasters;
- Assist with documents, data and recovery procedures during crises;
- Identify alternative supply sources, resources and locations.

In the emergencies event, the Emergency Team enters into action of which components and responsibilities are determined by the top management decisions.

The company has the competence, technical and human capacity necessary to carry out the computer assisted design activities, in three directions:

- Mechanical engineering design (CAD / CAM / CAE);
- Geographic information systems design (GIS);
- Multimedia design.

The main customers are private industrial companies. The company has research activities in partnership with higher education institutions, research institutes and research centers, as well as with other private companies in the country and abroad.

Related to the complex relationships with other organizations as partners, customers or suppliers, the organization has implemented and maintains an integrated management system including the EN ISO 9001:2015 and the ISO CEI 27001:2013 in order to ensure the conditions and ways to prevent the security risk effects and to ensure the return conditions with minimum losses after incidents. At least once a year, a possible and probable risk analysis is carried out according to the severity of their consequences as well as an information classification by the importance category so as to ensure their protection, integrity and availability according to the classification.

The main dangers and risks are:

- Epidemic;
- Earthquake;
- Fire;
- Flooding;
- Cyber attack;
- Sabotage (internal or external);
- Major Weather Event (Storm);
- Interruption of utilities;
- Terrorism / Piracy;
- War;
- Theft (of material or vital information);
- Inappropriate operation of vital systems.

In the epidemics case, the impact is on the people and can be mitigated by technical and business solutions. However, if the people with responsibilities are affected, malfunctions may occur. In these situations quarantine and team members' separation are instituted so that they can rotate according to the incubation period of the disease. In the other situations, after the threats defining, scenarios and procedures for rescuing goods and mitigating the impact of possible and probable emergencies are made in the most serious variants. Such procedures are described in the company's integrated management system. After the analysis phase, in the next stage, the technical requirements and the material, human and financial resources needed for each solution are determined. The resource inventory allows a quick identification of the resources deployed. In the

case of a company with a strong activity in assisted design, this plan's requirements should cover the human resources, specialized equipment, applications, databases, user manuals, computers, peripherals, electronic information carriers, etc. All of these requirements can be found in the integrated management system documentation.

The organization defines within the integrated management system an information security plan that is mandatory for all organization employees.

In this respect, the organization's management allocates financial and human resources and support for the fulfillment of the following objectives related to information security:

- Compliance with contractual and legal obligations in all the carried out activities;
- Ensure continuity of service delivery to customers and minimize losses in the event of security incidents;
- Ensure adequate protection of the processed information importance and strict confinement of access to confidential information;
- Protect the data integrity generated by support processes and software applications used;
- Protection against cyber attacks and viruses of all kinds;
- Demonstration of compliance with ISO CEI 27001:2013 Information Security Management Systems;
- Strengthen the organization's reputation on the market and increase the stakeholders trust.

Security information procedures are implemented to implement the Security Plan.

Criteria on which IS risks are assessed are:

- Financial loss;
- Activity Dysfunctions;
- Image loss;
- Litigation with clients,

All resulting in loss of Confidentiality, Integrity and Availability of Information. Implementation of internal measures to ensure information security is carried out by the Commission of Emergency Situations.

All information security activity is conducted in conjunction with the general procedures and work instructions integrated into integrated management system.

The human resource is the highest priority in rescue actions in case of catastrophic situations, because without this resource the continuity of activity can not be questioned. After the disaster the emergency and rescue teams will begin rescuing this resource by paying maximum attention to physically and mentally impaired people by calling the services of specialized institutions. The first measure consists of calling for 112 emergency service. Preventing serious human consequences also involves organizing regular training courses on appropriate behavior in such situations. In the annual training plans of the integrated managerial system, such themes are also foreseen.

The organization respects the privacy and personal employees' data, as well as the Romanian legislation in force, namely Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data, as amended and supplemented.

The confidentiality and protection of the collected information from customers / partners is of vital importance to the organization. The Company undertakes not to disseminate the collected information to third parties without express and prior consent. Employee personal data will only be used for strict business purposes and the right of use is strictly reserved for the Payroll person.

The physical security of the premises in which the company's headquarters is located is ensured by several means and systems that allow real-time alarming of key people at a distance through the mobile network.

In order to eliminate the malfunctions risk (during recovery) between team members involved in business continuity, both communication and co-ordination need to be effective and efficient. This requires a permanent availability of all the communications systems available to the company. All of these systems are permanently operational and daily checked so that in the occurrence of

incidents, it is possible to intervene with promptness and trigger the operations provided in the procedures of the integrated management system.
Access to company information and databases is permitted by their protection system. First, there is an inventory of all this resources type and their classification according to the confidentiality level. Then, depending on the media they are in, the protection mode is set.
In the company development in time, its endowment allows for a highly professional activity.

5. CONCLUSIONS

Within the organization, business continuity after a disruption incident is regulated under ISO CEI 27001:2013 with the main purpose of resuming activities without affecting the company image, loss reduction, processes safely running and honoring obligations of the organization.
The following objectives are envisaged:
- Resources providing to protect employees' health when an incident occurs;
- Establishment of internal and external communication links;
- Information collecting and evaluating on the damage severity;
- Identification of available resources for resuming work;
- Performing actions for the purpose of business continuing without significant loss.

The main stages of the resumption process are:
- Incident warning;
- Incident identification;
- The team mobilizing intervention;
- Strategy reviewing;
- The resettlement decision;
- Work resumption;
- Restoring activities to the pre-disaster level.

It is taken into account that:
- The company has sufficient qualified staff to execute the set of processes and procedures necessary to work resuming;
- The involved staff in the activity resumption is available regardless to the incident time and the involvement duration;
- In the incident event, the activity resumption is performed according to the processes and procedures set presented in the Activity Continuity Plan and the Integrated Management System;
- A high level of promptness is ensured.

Activity resuming in such situations within a time frame that does not threaten the company stability is a top priority. For this plan to be effective it is necessary to have:
- Alternative development (reserve) plans for the activity resumption in the interruptions case;
- Periodic testing of alternative plans to check their availability;
- An incidents classification that may occur depending on the minimum time required to activity resuming;
- Activities identification and the processes carried out;
- Identification of critical functions and locations where they are implemented;
- Identification of alternative (alternative) locations, involving:
    - Alternative sources of power supply;
    - New connections to computer networks;
    - Alternative communication networks;
    - Hardware-software support;
    - Teams establishing that could be involved in the activity resumption in the event of an incident;
    - The responsibilities establishing in each situation to each team, working rules.

The organization shall ensure that the legal requirements and other applicable requirements to which the organization subscribes are taken into account in the establishment, implementation and maintenance of the integrated management system.

REFERENCES

Doughty, K. (2001). *Business Continuity Planning: Protecting Your Organization's Life*. Retrieved April 13, 2018, from https://books.google.ro/books?hl=en&lr=&id=vG2qvt7I6eYC&oi=fnd&pg=PP1&dq=the+organization+continuity+plan+implementation&ots=mgKAVtjNux&sig=1G37Gs-2gaicgQa52zMnm-YxwP4&redir_esc=y#v=onepage&q=the%20organization%20continuity%20plan%20implementation&f=false.

Elliot, D., Swartz, E., Herbane, B. (1999). Just waiting for the next big bang: business continuity planning in the UK finance sector. *Journal of Applied Management Studies*,(8), pp. 43–60. Here: p. 48.

EN ISO 27031:2014 Information technology – Societal Security - Business continuity management systems-Requirements.

EN ISO 9001:2015 Quality management systems Requirements.

Engemann, K. (Ed.). (2018). The Routledge Companion to Risk, Crisis and Security in Business. London: Routledge.

Ferguson, C. (2018). Business continuity and disaster management within the public service in relation to a national development plan, *Journal of Business Continuity & Emergency Planning*,*11*(3) / Spring 2018, pp. 243-255(13), Publisher: Henry Stewart Publications.

Intrieri, C. (2013). "*Business Continuity Planning*". Flevy, Retrieved September 29, 2013.

ISO CEI 27001:2013 Information Technology. Security techniques. Information security management systems. Requirements.

Kirvan, P., Miller, J.A. (2017). Free business continuity policy template. Retrieved from http://searchdisasterrecovery.techtarget.com/feature/Free-business-continuity-policy-template-for-SMBs

Law no. 677/2001 November 21, 2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data.

Soufi, H. R., Ali Torabi, S., Sahebjamnia, N. (2018). Developing a novel quantitative framework for business continuity planning, *International Journal of Production Research*, DOI: 10.1080/00207543.2018.1483586.

Zeng, Z , Ziao, E. (2017). An integrated modeling framework for quantitative business continuity assessment, Process Safety and Environmental Protection, 106, February 2017, Pages 76-88.