PREPARING THE LIST OF SYSTEMS AND APPLICATIONS HOSTED IN DISASTER RECOVERY INFRASTRUCTURE: CASE STUDY IN THE BANKING SECTOR

Gjergji Mulla

University of Tirana, "Mother Teresa" Square 4, 1001, Tirana, Albania

Abstract

In this study, the analysis of business processes is done in a second level bank in Albania. The paper shows how to identify the systems and applications that are used by the retail banks, and how to specify the recovery time objective (RTO) for each of these systems and applications. A questionnaire has been prepared with a dedicated session for the applications and systems used during the business processes.

The interviews have been conducted with the business line responsive employee in charge for the business continuity management plan. These employees are also responsible to update the questionnaire in case something changes in their day-to-day processes and to notify the business continuity manager for these changes. For each process the respondent employee has indicated all the systems and applications used by their business line during each business process. After analyzing the gathered information from the interviews, a final table is prepared where all the systems and applications used by the business lines and the respective recovery time objectives are listed.

Keywords*: recovery time objectives, business continuity management, disaster recovery*

INTRODUCTION

Crisis management is the organization and coordination of activities in preparation for, and response to, events that prevent or impede normal organizational operations (thereby threatening its most important goals). These events may be characterized by low probability, high consequence, ambiguity and little time to respond (Mitroff, Pauchant, & Shrivastava, 1988; Pearson & Clair, 1998; Weick, 1988).

Destruction can refer to a critical system's data and/or programs, including the operating system, server and the communication devices. A critical system's back-up, referred to as a constitute of a synchronous replication of updates (mirroring) in the case of the database server: the data stored in the primary database and its "mirror" database are destroyed. With regard to a critical system's programs, the back-up involves replicated programs between high-availability servers or load-sharing servers. Logical destruction means that the critical system's equipment is physically intact. To begin with, the critical systems addressed are those that are under the responsibility of the institution (S.A & C. A., 2010).

The events that can lead to the logical destruction of a critical system and its back-up have many causes:

- Human cause: malicious intent, manipulation error.
- Technical cause: a bug that appears after an operational mode set-up or after a virus attack.

The back-up solutions to be implemented in response to these causes are based on three components:

- Recovery of the critical system's data and/or programs.
- Solutions to recover lost data from the backup saved.
- Alternative solutions.

BACKGROUND

A quick review of the key topics in business continuity management (BCM) literature is presented in this section.

The restoration of application server or technical server programs is based on procedures which already exist within the framework of the standard operation of critical systems. We assume that the critical system is equipped with warning functions capable of notifying the business lines of any destruction or corruption of data occurring the evening before, at the earliest. Otherwise, the system cannot be considered as critical.

We therefore assume that the last valid save to be restored is:

- either the one from the day before, if the warning was sent during the day, on a working day
- or the one from two days before, if the warning was sent after the last save (e.g. during the evening or on a non-working day).

Data integrity controls must be defined and put in place within critical information technology (IT) applications, along with an automated alert report system, in order to detect any destruction or corruption of data as quickly as possible. These controls and warnings must be defined in compliance with the business line requirements in terms of availability, integrity, confidentiality and proof (AICP) indicators (S.A.& C. A., 2013).

For some critical systems, data recovery can involve recycling old data, if this is technically and functionally possible. The recovery procedures implemented can be either technical or business procedures. It is recommended that technical procedures to be implemented rather than business procedures. In reality, the latter have proven to be very difficult, or even virtually impossible to be defined in most cases (CAG, 2007).

A re-engineering of the information system can be an opportunity to make provision for and implement data recovery technical procedures, if they are not already operational.

The alternative solutions enable continuity of business activities during the data restoration process and during the recovery of data that have been lost since the last valid backup restoration.

In most cases, alternative solutions and procedures designed to handle the “prolonged unavailability of an IT site” cases can also be deployed in response to the “logical destruction of a critical information system and its backup” cases.

The implementation of BCM solutions in response to this case can lead to the set-up of a variant of the IT contingency project used for the “unavailability of an IT site” case.

BCM and Disaster Recovery Plan (DRP)

We need to understand the difference between a business continuity management plan and disaster recovery plan. A simple way to understand the difference is that BCM comes first, and if BCM's efforts fail, DRP is engaged to fill the gap. For example, let’s consider the case of a data center that is built near a river. The task of the BCM is to verify if the local authorities are performing the tasks of river maintenance as foreseen. Also, the task of BCP is to take measures to protect the building from the water. Regardless of the efforts made in the framework of the measures explained above, it is possible that in specific cases the building will be affected by a flood. The pressure on the flood can be increased to the point where the flood cannot be handled. The destructive level of this flood can be higher than measures taken by the building where the data center is located, causing flooding of the building. At this point, the continuity plan activates the disaster recovery plan to take over. The goal of this plan is to restore business operations to the main datacenter as soon as possible (S.A.& C. A., 2012).

Emergencies versus incidents

We must also distinguish emergencies from incidents and the corresponding response procedures. Emergency procedures and response actions against them are generally for risks with a high degree of impact on business processes, compared to incident response procedures. They may include incident response plans, but they usually deal with broad impact factors. To illustrate the difference, an incident response plan addresses situations such as an attack against the organization's network attempting to gain access to a customer database. For this we must have a response plan which must be activated as a response to the attack, and the people who will implement this plan by performing the relevant actions.

The emergency response plans are to handle risks with a high degree of impact such as interruptions of electricity in the entire facility, which has caused a massive interruption of work processes.

At the beginning, we must remind that, according to the regulatory office demand, each facility must protect itself against risks of major disasters (Mulla & Ademi, 2015).

Concerning buildings, we can classify the main risks as follows:

- Natural environment
    - Flooding, mudslide, earthquake, lightening, weather conditions (wind, thunderstorm, cyclone, tornado, etc.)
- External reasons
    - External enterprises in neighbourhood (industrial risks as SEVESO, etc.)
    - Criminality and malicious acts
- Transport traffic
    - Proximity of important traffic roads
    - Train rails
- Pipe-lines, gas-lines
- Falling of planes, etc.

Exposition to risks and risks evaluation depend strongly on characteristics of the area where the enterprise's primary site is settled and where the enterprise considers building its back-up site. In both cases, risks analysis is necessary for the primary site and the back-up one. Detail level of this analysis will be different, in function of this area nature: industrial, agricultural or urban. Until these days, regulator bodies in Albania has not defined any recommendation concerning the distance and the perception is that recommendations of this type will never be proposed. But in case on wrong choice, regulator bodies would not be in support of this choice and the "moral responsibility" would be engaged (Mulla & Ademi, 2015).

It is probable that the regulator body will check if back-up sites are exposed to the same type of risks as primary site (for instance, both of them settled next to a flooding area). In this case, the regulator bodies can ask to justify the enterprise's choice and can compare this choice to solutions chosen by other entities, having similar activities.

METHODOLOGY

In this study, the analysis of business processes is done in a second level bank in Albania. The research question related to this paper was: How to identify the systems and application that are used by these types of institutions and how to deters their recovery time objective? In order to find the answer for the question raised, we have prepared a questionnaire where beside the other information gathered for the business processes of the bank, there is a dedicated session where the interviewed employees will fill regarding the applications and systems used during their work. This information is part of table 1.

Table 1. Application list for each process.

Application	RTO	MPDL	Critical time	Primary Site	T+4	D	D+1	D+N

The interviews have been conducted with the business line responsive employee in charge for the BCM plan. These employees are also responsible to update the questionnaire in case something changes in their day-to-day processes, and they are also responsible to notify the business continuity manager for these changes.

For each process the business line responsible employee has indicated all the systems and applications used by their business line during each business process. In Table 2 are listed all departments and positions of the employees interviewed in the bank, and the respective dates.

Table 2. Plan of the interviews with departments and employee position.

Unit	Department	Date of interview	Position
Compliance	Compliance	09/05	SM
Human Resources Office (HRO)	HR	10/05	CHRO
Legal Office	Legal	11/05	CLO
Risk Management Office	Risk and Permanent Control	12/05	CRO
Marketing & Bank Products Office	Products section	13/05	CPO
Operational Office	Head Operational Office	02/06	COO
	Finance	16-18/05	CFO
	Head IT Office	17/06	CTO
	IT Office / Systems	15/06	SM
	IT Office / Applications	16/06	SM
	Payments and Correspondent Banks	19/05	SM
	Treasury / Intermediary Office	20/05	CHO
	Credit Administration	23/05	SM
	Problem Loans and Legal Litigation	24/05	SM
	Administrative Support	25/05	SM
	Director of Recovered Assets Management	26/05	SM
	Treasury	27/05	SM
	Debt Recovery and Negotiations Sector	31/05	SM
	Cards & ATM	01/06	SM
	VAULT	02/06	CHO
Retail Office	Direct and Alternative Sales	03/06	CRtO
	The region of Tirana	06/06	SM
	Business Center Office	09/06	SM
Enterprise Office	Division of Enterprises	10/06	SM
	Enterprises Sector Alpha	13/06	SM
	Enterprises Sector Beta	14/06	SM
	Enterprises Sales	15/06	SM
	Investments	17/06	SM

Source: Vukatana & Mulla, (2022)

During the interviews, has been gathered a lot of information that must be linked with each other like relations between business activities, processes, software applications, user sites, applications, servers, networks and IT sites. For better management and use of this information, organizing those data within a structured database, will give to the institution a considerable advantage. The organization could generate vital information in form of reports to discover what happens in case a service, application or system will fail and which are the critical processes that will be affected by this failure.

If the information gathered from the interviews will be saved in separated documents, then the process of tracking the effects of a failure (service, system or application) will be very difficult to be managed and will lead to errors. Also, the process of keeping the plan up to date will be much more difficult. Creating the proposed databases generally require a lot of developing time.

RESULTS AND DISCUSSION

Table 3 shows part of the list of applications and systems that are used from each business line. In the table it is also specified the number of users that should have access to those systems and application from each business line after the disaster has affected the organization. Table 3 does not have all the identified applications and processes. The reason for not showing all the information gathered from the interviews is to protect the confidentiality of the enterprise data.

Table 3. Partial example of systems and applications

Business Line	Application	RTO	MPDL	Critical time	Prim.	T+4	D	D+1	D+N
Legal	FC	3D	0D		x	0	0	0	1
Legal	Email	3D	1D		5	0	0	0	1
Legal	File Server	3D	1D		5	0	0	0	1
Legal	Legal Software	3D			5	0	0	0	1
Audit	FC	1 d			3	1	1	1	1
Audit	Email	1 d	0		3	1	1	1	1
Audit	File Server	1 d	0		3	1	1	1	1
Audit	Manits	1 d			3	1	1	1	1
HR	FC	1D	1d		7	3	3	3	3
HR	File Server	1D	1d		7	3	3	3	3
Marketing and Communications	Departments Doc	2W			6				
Finance Division	FC	2H	0		13	4	4	4	
Finance Division	Reporting system	4H	0		13	5	5	5	

Table 4 presents in a summary of the number of processes that are evidenced from the data collection. The total number of applications and systems used by the bank is 54. The departments with more processes are Retail (8) and IT (19).

Table 4. Final list of systems and application with the respective RTO and other information

Name	RTO	MPDL	Critical time	Prim.	T+4	D	D+1	D+N
FC	4H	0		13	4	4	4	
Reporting system	4H	0		13	5	5	5	
SWIFT	4H	1D		14	5	5	5	
AECH	4H	1D		14	5	5	5	
AIPS	4H	1D		14	5	5	5	
Reuter (Internet)	4H	1D		14	5	5	5	
Kondor +	1D			3	2	2	2	
Fixed Assets	4H	1d		3	3	3	3	

CONCLUSION AND FUTURE WORK

By creating the right questionnaire, and by conducting the interviews with all the business lines of the bank, it was possible to identify the systems and application that are used by an institution and to deters their recovery time objective. The results show the number of applications and systems used by the bank that consist in 54 in total. For each of them we have specify the recovery time objective. For example, if for the Swift system, the RTO from the Treasury department has been set on 1 working day and from the Payments and Correspondent Banks department has been set to 4 hours, then the final result for this system to be up and running in case an incident effect this system will be the lower time frame that in our case is 4H.

The future work related to this paper will be the research on how to create a disaster recovery site, in order to host not only the processes that are critical for the organization but also the applications and systems that are used to support these critical systems.

REFERENCES

1. Mitroff, I.I., Pauchant, T.C., & Shrivastava, P., 1988. The structure of manmade organizational crises. Conceptual and empirical issues in the development of a general theory of crisis management. Technological Forecasting and Social Change, 33, 83– 107.
2. CAG-Crédit Agricole Group, 2007. BCP Methodology. Crédit Agricole Group. November 2007
3. Mulla,Gj., Ademi, A., 2015. Assessing business risk as key part of the BCP project. Tirana: Information systems and Technology Innovation: including Modern Business solutions.
4. Mulla,Gj., Ademi, A., 2015. Implementation of the Crisis Management System.
5. S.A, C. A., 2010. Security Committe Policy. Security Committe Policy. Credit Agricole S.A.
6. S.A., C. A., 2012. CISI committee presentation, BCP project.
7. S.A., C. A., 2013. Crisis management system operating manual.
8. Vukatana, K., & Mulla, G., 2022. The importance of business continuity management in the banking sector. International Journal Of Economics, Commerce And Management, X(8).