International Journal of Economics, Commerce and Management
United Kingdom ISSN 2348 0386 Vol. X, Issue 8, Aug 2022

http://ijecm.co.uk/

THE IMPORTANCE OF BUSINESS CONTINUITY MANAGEMENT IN THE BANKING SECTOR

Kreshnik Vukatana
Department of Statistics and Applied Informatics, Faculty of Economy,
University of Tirana, "Mother Teresa" Square 4, 1001, Tirana, Albania
kreshnik.vukatana@unitir.edu.al

Gjergji Mulla
Department of Statistics and Applied Informatics, Faculty of Economy,
University of Tirana, "Mother Teresa" Square 4, 1001, Tirana, Albania
gjergji.mulla@unitir.edu.al

Abstract

To establish resilience and the capacity for an effective reaction, business continuity is a management strategy that analyzes possible threats to a company. Research and development on business continuity management (BCM) are ongoing. In literature exist standards and studies that define principles, challenges and approaches related to BCM. This study was conducted in the context of banking sector in Albania, to evidence the most important processes for each bank department, with focus on the criticality of these processes. For this reason, 28 semi-structured interviews with questions within a predetermined thematic framework on BCM, were asked to different senior managers including all departments. The results highlighted the main processes needed, with the various levels of criticality that must be considered to build a robust business continuity plan (BCP). The natural continuation of this work will be the design of a suitable infrastructure, by analyzing the costs of relative hardware and software components, needed to apply this BCP.

Keywords*: business continuity management, business continuity plan, banking sector*

INTRODUCTION

Business continuity management (BCM) is defined as the advanced planning and preparation of an organization to maintain business functions or quickly resume after a disaster has occurred. It specifies requirements to implement, maintain and improve a management system built to protect against, reduce the likelihood of the occurrence of, prepare for, respond to, and recover from disruptions when they arise. These risks include fire, flood, or cyber-attacks (ISO, 2019).

Other than those potential risks, laws and business specifics have been recognized as the primary drivers behind the BCM policies development in the finance sector. As a result, business continuity planning is crucial for banks as the sector grows, to protect customers and adhere to global regulatory standards. Furthermore, the banking sector differs from other industries in the fact that BC planning is crucial for some additional reasons, as outlined by the Bank of Japan in 2003:

- Preventing widespread payment and settlement disorder or preventing systemic risks by limiting the inability of financial institutions in a disaster area to execute payment transactions.
- Reducing managerial risks, for example, by limiting the challenges for banks to continue providing financial services during and after disasters (Arduini & Morabito, 2010).

The remaining part of this paper is structured as follows: Firstly, an overview of BCM principles and current challenges is presented in the background section. Next, it is introduced the methodology section, describing the steps performed to create the data collection. Then, in the next section are described the results with the related discussion. At the end, in the conclusion and future work section are shown the findings and upcoming work, needed to implement a reliable infrastructure for the considered unit.

BACKGROUND

A quick review of the key topics in BCM literature is presented in this section.

BCM Principles

The goal of BCM is to sustain the company's critical services, as well as the anticipated restart of operations, if required temporarily and in a degraded manner. It thereby improves organizational resilience (Bhamra et al., 2011; Engemann & Henderson, 2012). The BCM attempts to maintain continuous availability of crucial organizational resources and activities to guarantee the accomplishment of crucial goals and missions (Bajgoric, 2014). According to

most of the pertinent literature, BCM is a decision-making process that considers ideas like company resilience, long-term performance, and value preservation. It is claimed that the Business Continuity Plan (BCP), which is a collection of policies and documents outlining a series of actions and the people in charge of carrying them out, is the main output from the BCM life cycle and will help businesses resume operations as soon as possible after a disruption (Haggège & Vernay, 2019; Jain et al., 2020; Rezaei Soufi et al., 2018).

Based on these considerations, the following are the key principles to consider when applying BCM to the banking sector:

1) The board of directors and top management are accountable for making sure the bank develops and keeps an excellent BCM.
2) The risks resulting from significant disruptions, the concentration of essential business functions, and outsourcing agreements must be carefully identified, evaluated, and mitigated and be part of the bank's BCM.
3) The recovery goals and plans must consider the seriousness of the potential hazards to the bank's crucial business operations.
4) To reassure key internal and external stakeholders about the bank's readiness in the case of a significant interruption, the IT department is required as part of BCM for critical business functions and related technical infrastructure.
5) To guarantee the bank's BCM's applicability and efficacy, a constant organizational awareness and testing for business continuity and resuming strategies is necessary.
6) To address the reputational risks, the BCM should include a strong communication strategy for internal and external stakeholders in the case of a significant operational disruption.
7) To reflect the operational environment and business circumstances of the bank, the methodologies and the plans for business continuity must be periodically reviewed and maintained.

BCM Challenges

Despite the potential advantages of using BCM, there are still very few organizations using it properly compared to the sheer number of businesses and institutions, especially in developing nations (Asgary et al., 2012; Frikha et al., 2021; Hamed & Alenezi, 2016; Kato & Charoenrat, 2018). With the recent experience from COVID 19, the disruption of services is more frequent and implementing effective triggers for businesses to adopt a BCP, the challenges are plentiful.

In ("8 Most Common Obstacles to Business Continuity Programs", 2022) are listed the most common challenges to take in consideration when creating BCP:

Lack of Resources. When you don't have the money, staff, or resources you need to get the job done right, managing a BCP can be difficult. Making a comprehensive budget outlining the precise expenditures of the program is one of the greatest ways to make sure you are getting all you require. Then calculate the financial losses the company would suffer if the plan were not in place.

Lack of Executive Support. Business involves a lot of risk-taking, and management is typically more willing to accept the chance that nothing serious will go wrong than to invest money preparing for business disruption. It might be quite difficult to shift that thinking and get management's support.

Lack of Organizational Engagement. Every employee must be aware of what has to be done and committed to the program in order for it to be effective. Lack of organizational engagement was cited by 61% of businesses as one of the biggest difficulties in business continuity (Assurance Software, 2022).

Insufficient Tools and Technology. A significant portion of a BCP will deal with technical issues like data loss, technological malfunctions, and communications system outages. A specific instrument or piece of technology, such as incident management software, satellite systems, or 4G LTE connectivity, may be required by the BCP to address these problems.

Lack of Routine Testing. Testing is needed to identify weaknesses either in BCP, or in the enactment of it. Creating different scenarios can be challenging because it is needed to predict all the possible cases.

Inability to Monitor the Program. It can be difficult to keep track of the critical employees as well as the preparedness of all the systems. The indicators to use to assess a plan's performance are unclear, and time may be very limited.

High Complexity. Keeping track of all the threats that are always appearing is a difficult undertaking. There are more complicated threats like cyberattacks in addition to the more obvious ones, like extreme weather, or other natural disasters. COVID 19 is an illustration.

Constant Training. For all employees to understand their duties and responsibilities, they must receive thorough training. The BCP is not likely to stay the same, which is the problem. The personnel of the organization will need to be retrained to include these modifications as new threats are discovered or enhancements to the strategy are implemented. Workers that leave and are replaced take their knowledge with them, so new hires will need to undergo extensive training from scratch.

METHODOLOGY

In this study, the research is done in a second level bank in Albania. Our research question was: What impact has the existence of BCM policy in the bank sector? A questionnaire was built for the interviews which was used to collect data about the impact that risks may have on the business and its processes. The core of it is shown in Table 1 and 2.

Table 1. Processes based on their critical period.

Name of the process	Sensitivity depending on the normal or critical periods of the processes	
	Normal period	C/I/NC
	Critical period	C/I/NC

Each senior manager is asked to fill the table with name of the process ran in the department and to note if it has a critical period or is sensitive during all the year, and to define its criticality (C=critical, I=important, NC=not critical).

Table 2. Types of risks related to the process.

Type of risk	Yes/No
Penalties	
Loss of earnings	
Legal consequences	
Damage of bank image	
Others	

Then for each process he/she must name the risks (penalties, loss of earnings, legal, image damage or other) if they happen (yes/no) when the process is stopped.

Table 3 show the plan prepared for the interviews and the position of the employ interviewed (SM=Senior Manager, CHR=Chief Human Resources Officer, CLO=Chief Legal Officer, CRO=Chief Risk Officer, CPO=Chief Products Officer, COO=Chief Operational Officer, CFO=Chief Finance Officer, CTO=Chief Technical Officer, CHO=Chief Head Officer, CRtO=Chief Retail Officer).

Table 3. 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

The duration of the plan was about 40 days, interviewing 28 employees where 10 of them where directors and 18 senior managers. Their selection is not random but inclusive and is based on the definition of Bank Security Committee that is responsible for BCM (ISO, 2019).

The information collected from the forms is numerous, manual processing of this data can normally lead to not fully accurate results. To solve this problem, a model was designed to make it possible to process the above information in an automated way. The questionnaires were previously converted into an Excel document, using several keywords, indexed information collected from different parts of the forms. For this purpose, a VBA (Visual Basic for Applications) program was built, which processes the collected information by creating the results tables shown in the following section.

RESULTS AND DISCUSSION

Table 4 shows some partial data from the process of collection. There are displayed only some general processes as examples, to better illustrate the results, because most of processes evidenced constitute confidential information. These are general processes that do not violate the principles of confidentiality.

Table 4. Partial example of processes with their respective criticality and risks.

Dept.	Name of process	Sensitivity	Penalties	Loss of earnings	Legal conseq.	Image
Legal	Archiving of Credit Files/ Contacts with third parties / Bank original documents	A	Yes	Yes	Yes	Yes
Legal	Maintaining Relations, communication & coordination of External Advisors/third parties	C	No	Yes	Yes	Yes
Audit	Preparation of Audit Plan (definition of auditable objects, risk map, pluri-annual audit cycle	B	No	No	No	No
Audit	Performance of audit mission as per yearly audit plan	A	No	No	No	No
Audit	Quarterly / yearly reporting of planned and unplanned audit missions and related results	C	No	No	No	No
HR	HR MANAGEMENT / Recruitment and Adaptation	B	No	No	No	No
HR	Remuneration - Motivation - Labor Relations and Legislation	A	No	No	Yes	No

Table 5 shows a summary of the number of processes that are evidenced from the data collection. The total number is 106. Regarding the level of sensitivity, they are divided in 84 (critical), 17 (important) and 17 (not critical). The departments with more processes are Retail (17) and IT (17). The number of processes that have penalties if a disruption happens are 25, the ones with loss of earnings are 45, those with legal consequences 34, and those which bring a damage for the bank image are 59.

Table 5. Number of processes for each noted department, with the respective number of risks.

Department	No. of proc.	Penalties	Loss of earnings	Legal consequences	Damage of bank image
Legal Office	6	2	6	4	6
HR	5	-	-	1	-
Audit	6	1	1	1	1
Risk and Permanent Control	4	1	1	1	2
Compliance	4	4	-	4	4
Finance	7	3	-	3	3
Treasury	8	-	8	-	4
Administration	5	1	5	4	4
Payment Sector	6	6	6	6	6
Treasury / Intermediary Office	4	1	1	1	-
Retail	17	1	13	3	16
Credit Administration	6	1	5	4	4
IT Systems	17	-	-	1	2
Cards and ATMs	4	3	4	-	4
Main Vault	2	1	1	1	1
Enterprises	5	-	3	-	2

CONCLUSION AND FUTURE WORK

The research question posed in this work was: What impact has the existence of BCM policy in the banking sector? Results show that there are 108 services with different levels of sensitivity: critical, important, and not critical. The types of risks regarding the bank, related to those processes, such as penalties, loss of earnings, legal consequences and image damage are present in most of the processes. This fact shows that the impact of these risks from service interruption is very high and the need of a BCM in the banking sector is necessary. Given the high number of processes evidenced from the data collection, it is suggested that only the processes with critical sensitivity must be included in the BCP.

The use of semi-structured interviews in this research can bring limitations related to some data loss regarding the little understanding or inadequate response about what a process is, and how its level of criticality is defined. For this reason, to each interviewee is explained in advance what a process should be and a list of examples with a different level of criticality (critical, important, and not critical) is shown to them, to better understand the topic.

As future work, based on the findings of this work, the right infrastructure should be proposed and built including human resources, hardware, and software. This infrastructure

should be accompanied by a BCP having in mind measures to be taken to protect critical or sensitive processes and information; the steps for the recovery of processes and information in case of disaster; how to keep the BCP functional; including testing of the BCP periodically to ensure that it is functional and to correct any possible deviations from it.

REFERENCES

8 Most Common Obstacles to Business Continuity Programs. (2022). [Blog]. Retrieved 2 August 2022, from https://www.agilityrecovery.com/article/8-most-common-obstacles-business-continuity-programs.

Arduini, F., & Morabito, V. (2010). Business continuity and the banking industry. Communications Of The ACM, 53(3), 121-125. https://doi.org/10.1145/1666420.1666452

Asgary, A., Anjum, M., & Azimi, N. (2012). Disaster recovery and business continuity after the 2010 flood in Pakistan: Case of small businesses. International Journal of Disaster Risk Reduction, 2, 46-56. https://doi.org/10.1016/j.ijdrr.2012.08.001

Assurance Software. (2022). *Business Continuity Benchmark Study* (p. 13). Assurance Software, Inc. Retrieved from https://cdn2.hubspot.net/hubfs/2224760/Final_BCBenchmarkStudy-121119.pdf

Bajgoric, N. (2014). Business continuity management: a systemic framework for implementation. *Kybernetes*, *43*(2), 156-177. https://doi.org/10.1108/k-11-2013-0252

Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: the concept, a literature review and future directions. International Journal of Production Research, 49(18), 5375-5393. https://doi.org/10.1080/00207543.2011.563826

Engemann, K., & Henderson, D. (2012). Business continuity and risk management (1st ed., pp. 59-71). Rothstein Associates Inc., Publisher.

Frikha, G., Lamine, E., Kamissoko, D., Benaben, F., & Pingaud, H. (2021). Toward a modeling Tool for Business Continuity Management. IFAC-Papersonline, 54(1), 1156-1161. https://doi.org/10.1016/j.ifacol.2021.08.136

Haggège, M., & Vernay, A. (2019). Story-making as a method for business modelling. Business Process Management Journal, 26(1), 59-79. https://doi.org/10.1108/bpmj-12-2017-0363

Hamed, T., & Alenezi, M. (2016). Business Continuity Management & Disaster Recovery Capabilities in Saudi Arabia ICT Businesses. International Journal of Hybrid Information Technology, 9(11), 99-126. https://doi.org/10.14257/ijhit.2016.9.11.10

ISO (2019). 22301:2019 Security and resilience — Business continuity management systems — Requirements.

Jain, P., Pasman, H., & Mannan, M. (2020). Process system resilience: from risk management to business continuity and sustainability. International Journal of Business Continuity and Risk Management, 10(1), 47. https://doi.org/10.1504/ijbcrm.2020.105615

Kato, M., & Charoenrat, T. (2018). Business continuity management of small and medium sized enterprises: Evidence from Thailand. *International Journal of Disaster Risk Reduction*, *27*, 577-587. https://doi.org/10.1016/j.ijdrr.2017.10.002

Rezaei Soufi, H., Torabi, S., & Sahebjamnia, N. (2018). Developing a novel quantitative framework for business continuity planning. International Journal of Production Research, 57(3), 779-800. https://doi.org/10.1080/00207543.2018.1483586