Open University Cyprus **Hellenic *Open University***

Master's join degree/post graduate Programme
Enterprise Risk Management (ERM)

MASTER THESIS

How do organisations such as Electronic Money and Payment Institutions in Cyprus turn threats and crisis situations into strategic opportunities in times of crisis management?

Anastasis Spyrides

Supervisor
Dr. Anastasis Petrou

May 2021

Open University Cyprus **Hellenic *Open University***

Master's join degree/post graduate Programme
Enterprise Risk Management (ERM)

MASTER THESIS

How do organisations such as Electronic Money and Payment Institutions in Cyprus turn threats and crisis situations into strategic opportunities in times of crisis management?

Anastasis Spyrides

Supervisor
Dr. Anastasis Petrou

This thesis submitted for partial fulfilment of the requirements of the
Master's join degree/post graduate programme
«Enterprise Risk Management (ERM)»
Faculty of Economics and Management

Open University of Cyprus **Hellenic Open University**

May 2021

BLANK PAGE

SUMMARY

This research study reflects the results of a research designed to examine how organisations operating in the Electronic Money and Payment Institutions of Cyprus turn threats and crisis situations into strategic opportunities in times of crisis management. Data was collected using mix a methods approach of qualitative and quantitative elements in four organisations. The study includes fifty completed data collection surveys and four interview questions of qualified individuals. The results are used to critically evaluate how such institutions react in cases of crisis even occur.

Findings show modest existence of a suitable crisis management level of readiness in the surveyed institutions. Furthermore, any additional risk management and / or preparedness efforts are indicated where relevant. Real scenarios describe how the institutions created prospects while continue operating without any crisis disruption. The effects of the results are critically examined and recommendations of future research are suggested.

ACKNOWLEDGEMENT

To start with I would like to express my thankfulness to my supervisor Dr. Anastasis Petrou for his constant supervision, support and tutelage during the course of my MSc degree. My gratitude extends to the Faculty of Economics for the opportunity to undertake my studies at the Department of Enterprise Risk Management, Open University of Cyprus.

I would also like to express my thanks and appreciation to the representatives and the companies themselves for participating to my search study and making this research worth doing. Findings of my research will be given to the companies as a gesture of my respect and gratitude.

Finally, I would like to thank my family and my wife for been part of this process through their constant support and encouragement.

"Great things don't come from comfort zones." Roy T. Bennett

Table of Contents

CHAPTER 1 5

INTRODUCTION 5

1.1 Problem Statement 5

1.2 Research Aim, Objectives and Questions 6

1.3 Limitations and Benefits of the Research 7

1.4 Structure 8

CHAPTER 2 10

LITERATURE REVIEW 10

2.1 Electronic Money and Payment Institution 10

2.2 Why to set up an EMI or PI Organization in Cyprus 11

2.3 Enterprise Risk Management (ERM) 11

2.4 Crisis Management (CM) 12

2.5 ERM Framework 13

2.5.1 ISO 31000 – Guidelines 13

2.5.2 ISO 31000 – Principles 14

2.5.3 ISO 31000 – Framework 16

2.6.4 ISO 31000 – Process 23

2.7 Types of Risks 26

2.7.1. Strategic Risk 26

2.7.2. Regulatory Risk 27

2.7.3. Operational Risk 28

2.7.4. Technology Risk 29

2.7.5. Financial Risk 29

2.7.6. Fraud Risk 30

2.7.7. Reputational Risk 31

2.8 Risk and Opportunities (COVID-19) 31

2.8.1 Low Exposure Risk 31

2.8.2 Medium Exposure Risk 32

2.8.3 High Exposure Risk 32

CHAPTER 3 33

METHODOLOGY APPROACH AND METHODS 33

3.1 Pragmatism 33

3.2 Mixed Methods 34

3.3 Data Collections Methods 34
3.4 Constructing and Analyzing the Data Collection Survey 36
3.5 Constructing and Analyzing the Interviews Questions 41
CHAPTER 4 45
DATA PRESENTATION & ANALYSIS 45
4.1 Demographics and Participant Characteristics Analysis 45
4.2 Data Collection Survey Analysis 61
4.3 Interview Questions Analysis 77
CHAPTER 5 91
DISCUSSION 91
Recommendations, Future Research and Conclusion 91
5.1 Answers to the main research questions 91
5.1.1 Which are the most material risks an EMI organization faces during specific crises? 91
5.1.2 How to manage, reduce or eliminate a possible manifestation of material risks with potential negative impacts? 92
5.1.3 What are risk management prevention measures in use and in relation to the identified risks? 94
5.1.4 How to utilize a crisis and adapt it into organizational opportunity (e.g., covid-19 vs electronic banking) 95
5.2 Summarize 96
5.3 Limitations 96
5.4 Recommendations on Future Research and Conclusion 97
REFERENCES 99
APPENDIX 1 105
PART A: Demographics 106
PART B: Data Collection Survey 108
PART C: Interview Questions 111
APPENDIX 2 112
PART A: Demographics 112
PART B: Data Collection Surveys 115
PART C: Interview Questions #1 124
PART C: Interview Questions #2 128
PART C: Interview Questions #3 133
PART C: Interview Questions #4 137

CHAPTER 1
INTRODUCTION

1.1 Problem Statement

The European Parliament and of the Council has replaced Directive 2000/46/EC and amending Directives 2005/60/EC & 2006/48/EC with Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of Electronic Money Institution (EMI) and Payment (PI) based on the Electronic Money Law 81(I)/2012 and Payment institutions Law 31(I)/2018 of the Republic of Cyprus's Constitution (Central Bank of Cyprus, 2020). The Regulatory body for the licensing and supervision of EMI's and PIs in Cyprus is the Central Bank of Cyprus (Official Journal of the European Union, October 2009 and December 2015).

As stated by Borge (2001: 4) "Risk management means taking deliberate action to shift the odds in your favor increasing the odds of good outcomes and reducing the odds of a bad outcome."

In business large or small private or public, every department of a company should have a crisis management plan without any exceptions. Crisis management is an organizational process of dealing with a disruptive, sudden, unanticipated and unexpected event that threatens to harm the organization and its stakeholders (Fink, 2002: 54). This process must include actions linked to threat detection with strategic implementation: prevention, assessment, treatment, monitoring and continuously review the crisis.

Yet, we do not know enough about crisis management in EMIs and PIs. This lack of knowledge is exposing organisations to disruptions, such as those caused by COVID-19 including losses in revenue, missed strategic opportunities and impacts their reputation.

Therefore, it is imperative to address this lack of research with purposive research that focuses on this crisis management predicament faced by EMIs and PIs in Cyprus.

Benefits of such research will include the most material risks of EMIs organisations faces during specific crises the purpose is to analyze how to manage, reduce or eliminate a possible manifestation of material risks with potential negative impacts and what are the risk management prevention measures in use and in relation to the identified risks. We will utilize the crisis of covid-19 and adapt it into EMI and PI organizational opportunity.

This research study reflects the results of a research designed to examine how organisations operating in the Electronic Money and Payment Institutions of Cyprus turn threats and crisis situations into strategic opportunities in times of crisis management.

Part of the research includes an examination of how EMIs and PIs ensure compliance with legislative requirements set by CBC related to risk management by referring to major areas and particularly: How do they identify, manage and monitor the risks relating to the company activities, process and systems while turn threats into strategic opportunities in time of crisis management?

To enable the detection of the risks to which an EMI might be exposed and to facilitate the implementation of corrective measures to mitigate those risks using the quarterly review of effectiveness method to analyze the most material risks: strategic risk, regulatory risk, operational risk, technology risk, financial risk, fraud risk and reputational risk that might be faced by a company as well as manage these risks.

1.2 Research Aim, Objectives and Questions

Research Aim:

To understand how Electronic Money Institutions (EMI) and Payment Institutions (PI) entities ensure compliance with legislative requirements set by CBC related to risk management, while examine a review of effectiveness to analyze the most material risks of an such organization: strategic risk, regulatory risk, operational risk, technology risk, financial risk, fraud risk and reputational risk that might be faced by a company as well as how to manage, reduce or eliminate these risks.

Research Objectives:

1. To understand which are the most material risks an EMI organization faces during specific crises.

2. To comprehend how to manage, reduce or eliminate a possible manifestation of material risks with potential negative impacts.
3. To understand what are the risk management prevention measures in use and in relation to the identified risks.
4. To recognize how to utilize a crisis and adapt it into organizational opportunity (e.g., covid-19 vs electronic banking)

Research Questions:

1. Which are the most material risks an EMI organization faces during specific crises?
2. How to manage, reduce or eliminate a possible manifestation of material risks with potential negative impacts?
3. What are risk management prevention measures in use and in relation to the identified risks?
4. How to utilize a crisis and adapt it into organizational opportunity (e.g., covid-19 vs electronic banking)?

1.3 Limitations and Benefits of the Research

"The more that you read, the more things you will know. The more that you learn, the more places you will go." (Seuss, 1978)

Limitations Research results of the thesis seems satisfactory even though in every research the researcher will face limitations that may restrict the research.

Our target was to approach all the EMIs and PIs in Cyprus to get the maximum results, overall are 12 operating institutions. The researcher manages to collect data from 4 institutions due to confidentiality policy, reporting obligations, deadlines given by the regulator and restrictions of Covid-19. The total number of the employees in the 4 EMI and PI organizations are 95. From those, the target of the researcher was to achieve 60 data collection surveys and 4 interviews questions of qualified individuals. Due to timing of the pandemic virus COVID-19 and restrictions measures announced by Cyprus government we have not received full responses from 10 questionnaire that seems to be incomplete. Even though we manage to do the 4 interviews to qualified individuals following the researchers target with key positions to an EMI and PI institutions and with over 5 to 10 years of experience within the business: Compliance Manager & AMLCO, Head of Compliance & AMLCO, Executive Director, Compliance Manager.

Even though we can say that the response rate of the sample collected from the questionnaires is 83% and from the interviews 100%. A sample with this dimension of 83% response rate may bring significant and reliable outcome. The lack of previous research studies on the topic did not affect the researcher from being accurate and the performing results was satisfactory.

Benefits of the research is for the reader to understand how Electronic Money Institutions (EMI) and Payment Institutions (PI) entities ensure compliance with legislative requirements set by Central Bank of Cyprus (CBC) related to risk management while understanding how to manage, reduce or eliminate material risks of such organization. To achieve this goal, the thesis is organized into the following sections.

1.4 Structure

Chapter 1, The first chapter of the thesis is related to the introduction. The researcher is describing the problem statement, research aim, limitation, benefits and structure of the thesis. The aim of the thesis is to provide a more in-depth look of how do organisations such as Electronic Money (EMI) and Payment Institutions (PI) turn threats and crisis situations into strategic opportunities in times of crisis management? The basic goal of the research is that we do not know enough and about crisis management in EMIs and PIs and this lack of knowledge is exposing organisations to disruptions, such as those caused by COVID-19 including losses in revenue, missed strategic opportunities and impacts their reputation. Therefore, it is imperative to address this lack of research with purposive research that focuses on this crisis management predicament faced by EMIs and PIs in Cyprus. Part of the research includes an analysis of how EMIs and PIs ensure compliance with legislative requirements set by Central Bank of Cyprus (CBC) related to risk management while understanding how to manage, reduce or eliminate material risks of such organization.

Chapter 2, The Second chapter of the research study is the Literature review: The purpose is to familiarize the reader with the topic and provide an explanation of licensing and supervisory authorities of Electronic Money (EMI) and Payment Institutions (PI) in Cyprus, a brief description and an explanation of why to set up an EMI and PI in Cyprus, the overall idea or definition of Enterprise Risk Management and Risk Management. An overview of ISO 3100 - Risk management: Guidelines of the principles, a framework and

a process for managing risks, the researcher will analyze and compare them according to the risk management framework of Electronic money and payment institutions in Cyprus. We will briefly describe and analyze the most material types of risks that might be faced by an Electronic Money (EMI) and Payment Institutions (PI) in Cyprus faces during specific crises: strategic risk, regulatory risk, operational risk, technology risk, financial risk, fraud risk and reputational risk that might be faced by a company as well as how to manage those risks. The purpose is to analyze how to manage, reduce or eliminate a possible manifestation of material risks with potential negative impacts and what are the risk management prevention measures in use and in relation to the identified risks. We will analyze the risk and opportunities of COVID-19 with low, medium and high exposure risks.

Chapter 3, The third chapter of the thesis presents the methodology. The employed Pragmatist Philosophy / Methodological Approach used Mixed Methods of qualitative and quantitative elements in data collections such as 50 closed-ended type surveys and 4 interviews questions to qualified individuals of open-ended type questions from 4 Electronic Money and Payment Institution. Finally, we defined the limitation of the research methodology and how may the outcome be influenced by those limitations.

Chapter 4, The fourth chapter of the research study is relating to data presentation and analysis. The researcher will conduct, analyze and implement the findings of demographics and participants characteristics, data collection surveys and interview questions.

Chapter 5, The fifth chapter of the thesis is the conclusion, findings and interpretation of the research entitled: How do organisations such as Electronic Money and Payment Institutions in Cyprus turn threats and crisis situations into strategic opportunities in times of crisis management? We are interested to identify gaps between the literature review and collected data.

CHAPTER 2
LITERATURE REVIEW

2.1 Electronic Money and Payment Institution

Republic of Cyprus has harmonized its legislation with the relevant European Parliament and of the Council directives and practices governing the operations of Electronic Money Institutions ("EMI") and Payment Institution ("PI") (PricewaterhouseCoopers, 2020).

For the provision of electronic money services in the Republic of Cyprus a permission must be granted by the Central Bank of Cyprus (the ''CBC'') to pursuant the right of establishment and the freedom to provide services, in accordance with the provisions set out in the Law (Central Bank of Cyprus, 2021).

As already mentioned in the introduction section, the initiation and ordinance of EMIs and PIs in Cyprus are regulated by the Law 81(I)/2012 (the "Electronic Money Law") and Law 31(I)/2018 (the "Payment Institutions Law") correspondingly, as modified. Electronic Money and Payment Institutions regulations are in harmony with the latest EU legislative directives (Official Journal of the European Union, October 2009 and December 2015).

The transposed provisions of the 2nd Payment Services Directive among the individual Cyprus legislation broadens the scope of payment services regulation among the EU. It additionally introduces changes to conduct of business needs aimed toward rising shopper protection and competition and changes to security and transparency needs.

Electronic money and payment institution when established and fully licensed in Cyprus are able to offer their services freely within the EU on a cross-border basis or by launching offices through the so-called "EU passporting process", without any additional authorization from the Central Bank of Cyprus ("CBC") as they benefit from EU regulations on freedom of services provision (Central Bank of Cyprus, 2021).

2.2 Why to set up an EMI or PI Organization in Cyprus

The EU member state is compliance with EU laws and regulations. Republic of Cyprus is a eurozone member thus this is making an easier penetration to the EU markets and a cost effective setting up to an ongoing operational service. Opportunities in the local corporate and institutional market since English is the business language and a more convenient time zone for conducting 24 hour a day business. A favorable tax system with no withholding tax on dividend distributions to foreign shareholders. That includes 12.5% corporation tax with possibility to drop up to 2.5% due to Notional Interest Deduction (NID), tax incentives for non-domiciled tax residents. Republic of Cyprus is known for the provision of highly qualified professional service such as accounting firms, legal firms and consultancy firms. An efficient regulator the Central Bank of Cyprus (CBC), which provides simplified procedures, reduced bureaucracy and lower regulatory fees (PricewaterhouseCoopers, 2020).

2.3 Enterprise Risk Management (ERM)

Enterprise Risk Management (ERM) definition as stated by Segal (2011: 24) is "the procedure by which businesses detect, assess, manage, and disclose all important risks to improve value to stakeholders". Crises are deliberate actions to reduce exposure to the event or its negative consequences. Risk management and decision making are closely related, but not identical. Decision making techniques are integral to risk management and vice versa.

The Risk Management function of a Company is performed independently to identify, manage and monitor the risks relating to the Company's activities, processes, systems and reports directly to the Board of Directors. The role of the Risk Manager is such to enable the detection of the risks to which the company might be exposed and to facilitate the implementation of corrective measures to mitigate those risks. (Vasile and Croitoru, 2012)

Risk management refers to the process of identifying risks and taking actions to reduce the potential of a negative outcome in favor of more favorable ones.

As such risk management is defined by three key questions:

- How are the results measured, given a choice?

- What is the starting point for measuring?
- What is the ending point?

Figure 1. Basic Stepwise Process

2.4 Crisis Management (CM)

According to Pearson and Clair (1998: 59-61) Organizational crisis management is a systematic effort by organizational representatives with external stakeholders to deter crises or to effectively manage the existing one that already occurs. Organizational crisis management effectiveness is evidenced when potential crises are avoided or when major stakeholders believe that the success results of short and long-range effects of crises outmatch the malfunction results. (Faghfouri, 2012)

Crisis management is an organization's method of handling a tumultuous and surprising event that threatens to hurt the organization and its stakeholders. A situation unfolding due to an unforeseen trigger event. This process must include actions linked to threat detection, strategic implementation, prevention, assessment and evaluation, handling, and/or termination of the crisis.

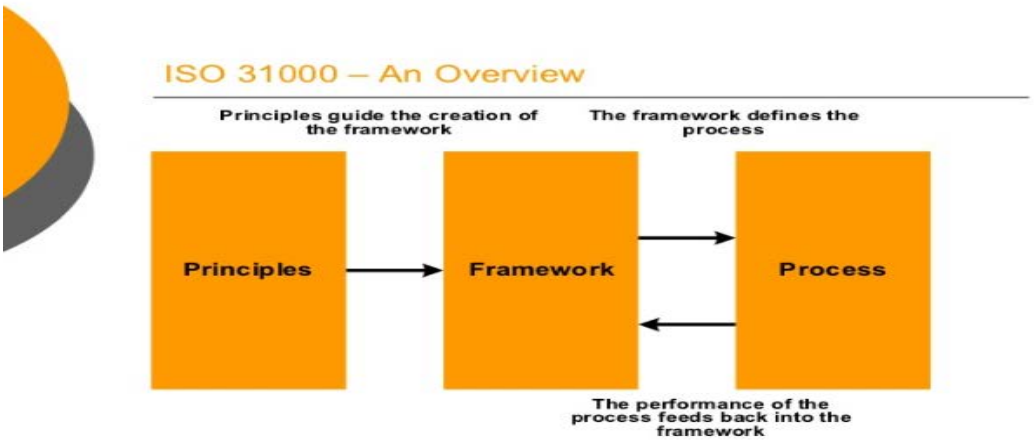
Crises rare measure events that disrupt the conventional operations of a company, with knocks on the implications for its assets, its future relationships with a company's stakeholders and that threaten the terribly survival of the organization (Carroll, 2009).

2.5 ERM Framework

The global financial crisis in 2008 demonstrated the importance of adequate risk management. Since that time, new risk management standards have been published, including the international standard, ISO 31000 "Risk management – Principles and guidelines". This guide draws together these developments to provide a structured approach to implementing enterprise risk management (ERM) (International Organization for Standardization, 2009).

2.5.1 ISO 31000 – Guidelines

Figure 2. ISO 31000-An Overview



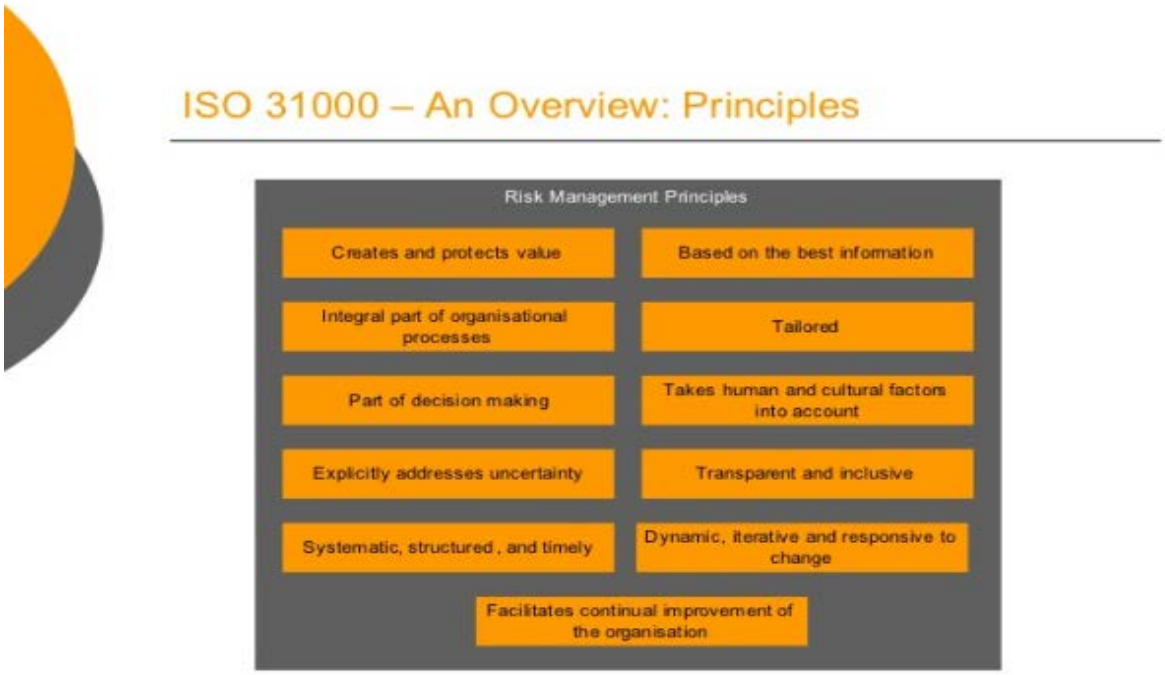
ISO 31000:2009

- An international standard providing principles and guidelines on effective risk management.
- Industry agnostic can be applied to any type of risk and in any type of organization.
- Intended to be tailored by organizations to meet organizational needs.
- A set of definitions, terms and principles to help guide and inform effective risk management.
- An outline for creating a risk management framework and process.

The above figure shows as the three major elements of ISO31000:2009 which the researcher is going to analyze and compare them according to the risk management framework of Electronic money and payment institutions in Cyprus. (International Organization for Standardization, 2009)

2.5.2 ISO 31000 – Principles

Figure 3. ISO 31000-An Overview: Principles



The organization creates and protects value by helping to identify the internal and external factors that could give uncertainty. Risk should not be managed by its own but to create and achieve a better performance.

We have value that cannot easy be defined and at the same time tend to great performance, reputation and legal compliance. Individuals, social and economic factors can always be importance in regards of safety and compliance.

Uncertainty can come accords internal and external organizational activities, the framework for managing risks should always implement according to organization needs and decision making. The process for managing risk should be an integral part of the operation otherwise the company will understand that changes will need to implement.

Improvement of the framework, decision making and activities can make improvement to the framework and at the same time treat risk while understanding associated risks. Risk can solely be assessed or with success treated if the nature and supply of that uncertainty

are understood. When risk is being assessed, it is important to contemplate the uncertainty related to estimating the ratings for probability and consequence.

A consistent approach to managing risk at the time choices are created can produce efficiencies in a company and may offer results that build confidence and success. This needs structure practices that think about the risks related to all choices and also the use of consistent risk criteria that relate to the organization's objectives and also the scope of its activities.

It is important to use the most effectiveness information in order to understand the risk at this point we can include method of research. Information may be limited and at this point we can use statistical predictions. Different areas of risk may require different tailored processes should take into account any legislative or other external obligations to which the organization is committed. Risk management takes human factors into account error can be occurred due to lack of knowledge, late to respond on warnings and actions.

Implementation of risk management ought to be transparent and inclusive we want to think about problems with confidentiality, security and privacy.

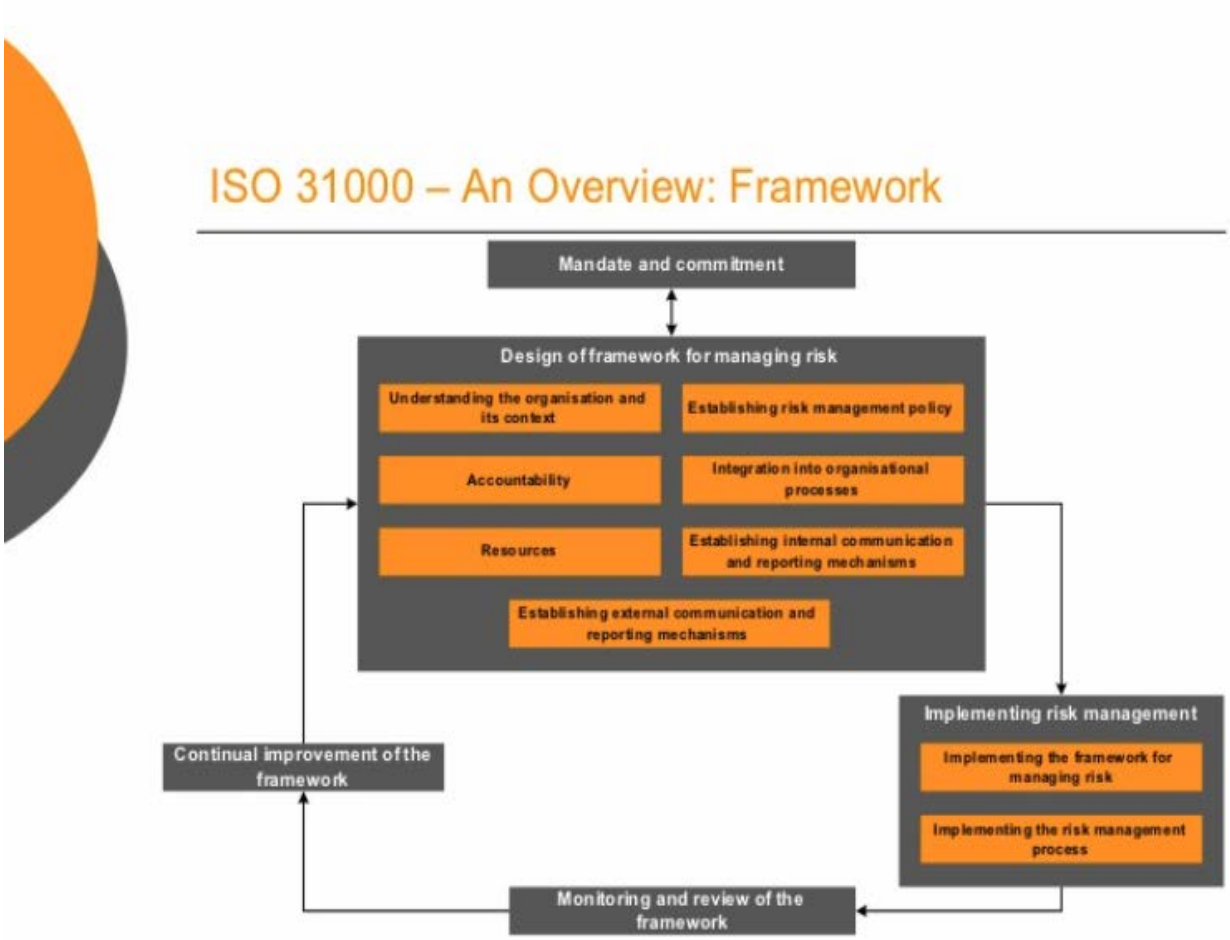
Risk management should be dynamic, monitoring and review should be incorporated into each of the core steps of the risk management process.

Continual improvement should be into consideration in order to be able to achieve the best sufficient outcome according to decision making and reducing uncertainty.

(International Organization for Standardization, 2009) and (Federation of European Risk Management Associations, 2011).

2.5.3 ISO 31000 – Framework

Figure 4. ISO 31000-An Overview: Framework



Enterprise risk management (ERM) is equivalent to the ISO definition of Risk Management Framework (Fraser and Simkins, 2010: 100). British Standard BS 31100 defines ERM Framework and thus "Risk management framework is a set of components that provide the foundations and organizational arrangements for designing, implementing, monitor, reviewing and continually improving risk management throughout the organization (protocols)" (BSI, 2008).

Risk Management begins with the mandate and commitment of the management and governance bodies of the electronic money (EMI) & payment institution (PI) and is followed by design of a framework implementing risk management, monitoring and review of framework and lastly continuously improving of the framework. Establishing

an effective risk framework an essential aspect of good corporate for all companies and should be a key priority for boards of directors and senior managements (International Organization for Standardization, 2009).

The implementation of risk management framework requires the appropriate risk department for the size of and complexity of the organization. Almost all monetary establishments are required to possess a head of risk management and/or a risk committee, with officers or departments accountable for completely different areas of risk.

All businesses are equivalent to a variety of risks, some of them are expected but many of them are unexpected or not successfully managed (Koblanck, 2016). Implementing a proper risk management framework can support institutions in more successful development. It will also recognize why things have gone left instead of right and ideally to act prior to losses occurrence. The aim of having an effective risk management framework is to be pro-active instead of reactive in managing the risks where exist in an extraordinarily business model (Koblanck, 2016).

Risk management framework is an inclusive set of policies targeting the decreasing of impact related to risks within an EMI and PI organization (Koblanck, 2016). The framework is a result of preparation and evaluation processes. Risk register is the major aspect of maintaining an essential working document.

For electronic money and payment institutions, the area that is generally least developed is operational risk and this required the greatest attention. The groups engaged in managing the electronic money institutions operations have the biggest understanding of what can go negative and should be embraced the soonest possible in the development process of risk strategy. This offers a great stability to the business development teams who often neglect to foresee the risks in the strategies that they are promoting or realize risk evaluation as an obstacle to improvement (Koblanck, 2016).

Mandate and Commitment

Mandate and Commitment of management at all organizational levels and activities.

The company is introducing risk management and ensuring its ongoing effectiveness. The top management should consider risk management to be one of its core competencies. It covers on a risk-based approach all operations that require strong sustained commitment by management, as well as strategic and rigorous planning to achieve commitment at all levels. The company risk management framework covers all operations (Bachtiar, 2013).

Key elements are:

- Promotion of a strong risk management culture
- Protect the capital base and support effective capital management.
- Integrations of risk considerations and capital needs.

The management risk committee is also acting as the governance and control committee of the company. The board has the overall responsibility for ensuring an effective risk management. The company needs to have data for risk management and as we have seen resources are not included to the framework and the risk management process. Strong communication skills lead to the benefits of risk management to all stakeholders, including the board and employees. The annual strategic dialogue takes place mid-year and agrees the key strategic objectives for the business. The planning dialogue takes place every quarter. The agreed plan is recommended to the Board for approval. (Proença, et al., 2017)

Design of Framework for Managing Risk

Understand the organization and its context

The purpose is to help and to understand the organization and all the elements that could affect its context.

> ***External context:*** The company should take more elements into consideration to fully understand the organization e.g., regulatory, legal, technological, economic, and financial. Monitoring and performance could be the key drivers that the

company needs to analyze more. External stakeholders do care about the organization so it could have been one major factor, the company need to approach, discuss make questionnaires and surveys for a better relationship.

Internal context: For a risk manager is always hard to make everyone understand the importance of risk evaluation. The company and the board need to help. Effective governance, in opposition, considerably assists the organization. The structure is good to be review periodically. Roles and accountability need to have the knowledge and experience. According to strategy the company needs to create a plan of actions to eliminate the habits and manage time correctly. Every business needs to have an objective like the need to increase profit margin and efficiency. Internal stakeholders need to be involved, company needs be professional and keep it word, have an open mind. Values have solid impact on the individuals in the corporation and dictate how they get dressed, behave, and perform their work (Bachtiar, 2013)

Establishing risk management policy

The overall stance and means to dealing with risk. It should clearly state organizations objectives for and commitment to and addresses.

The company adds value thought four primary components.

- Risk strategy and risk appetite
- Risk underwriting and identification
- Risk reporting and monitoring
- Communication and transparency

All responsibilities are being categorized according to the position of each employee and in a proper manner by the board which it considers to be an active member. Risk management has been measured and report or updated while its response to an event or change annually according to the organization needs and circumstances (Bachtiar, 2013) and (International Organization for Standardization, 2009).

Accountability

Authority and proper competency for handling risk which is enabled by:

The company has developed, reviewed and approved by the board on an annual basis in line with the corporate planning process.
Each responsibility and employee role should be categorized correctly to bring into consideration an overall and appropriate planning with making sure the non-exposing company shall have in place the below documentation:

- Risk Management Manual
- Risk Management Policy and Procedures
- Program of Operation Manual
- Business Continuity and Disaster Recovery Plan
- Risk Register with categorization of material risks

Employees have the authority and the knowledge according to responsibilities.
(Allianz P.L.C., 2017)

Integration into organizational processes

Integration happens when internal and external factors successfully combined. External factors needs to be taken into consideration to fully understand the organization social factors and facilitating conditions. The company will need to analyze more the performance and monitoring of organization culture.
Internal factors are regarding the environment of the institution and how do they implement internally. Stakeholders shall be involved, the company needs to act professional and efficient to understand the importance of risk evaluation. Structure should be reviewed periodically to create plan and actions (Bachtiar, 2013).

Resources

The organization should allocate appropriate resources for risk management to have a successful risk management we need as more data as possible. Resources are expensive and needed for each step of the risk management process. The company needs to make sure that employees have all relevant skills and qualifications. At this point the risk

manager can speak to the board for the most important needs of the company will trying to implement a successful risk management, due to limited resources priorities is the most important in order to be able to achieve a successful risk management. From the top to the bottom management ideas needs to be heard, questionnaire while being involved to the main risk process and procedure. While having all relevant experience, knowledge, information and training (Bachtiar, 2013).

Establishing internal and external communications and reporting mechanism

The company should be committed to have an internal and external control system that fulfils its organizational obligations and all relevant requirements. The company's internal and external control system is based on a strong control culture which emphasizes and demonstrates to all employees the importance of internal and external controls in the company. As part of this, the institution seeks to avoid policies and practices that may provide incentives for inappropriate activities (Bachtiar, 2013).

Implementing Risk Management

Implementing the framework for managing risks

In implementing framework for managing risk the organization should:
The risk strategy is the main component of the Company's risk management framework it determines the strategy of handling the risks that the institution recognizes during the pursuance of broader enterprise strategy (Allianz Group, 2018). With the risk strategy, the Company seeks to:

- Safeguard the EMI and PI organization reputation.
- Remain solvent even during an incident of worst circumstances event.
- Maintain adequate financial resources to meet its operational liabilities and
- Provide resilient profitability.

(Allianz Group, 2018)

On a regular basis, the compliance function should identify, documents and assesses the compliance risk associated with EMI and PI business activities. This helps to obtain that the overall compliance framework reflects the risk exposure. The Compliance Function needs to support the Risk Management and vice versa.

Implementing the risk management process

Risk management should be implemented by ensuring that the risk management process is applied through a risk management plan at all relevant levels and functions of the organization as part of its practices and processes. The use of the internal model is subject to approval by the Board of Directors of the Company (Quantum Leben, 2018)

Monitoring and Review of the Framework

The management of strategic risks is implicitly embedded into the execution of the annual strategic dialogue process, including the establishment of strategic priorities and execution of the steps towards their fulfillment. As a key element of our risk management framework, the Company's approach to risk governance enables an integrated management of local and global risks and ensures the risk profile remains consistent with the Company's risk strategy and capacity to bear risks. The risk strategy and corresponding risk appetite are transferred into standardized limit management processes covering all quantified risks throughout the Company and taking into account the effects of risk diversification and risk concentration (International Organization for Standardization, 2009)

Continual Improvement

The Company should have an integrated structure or a business continuity plan in place to oversee the operation of the Risk Management Framework and in turn the Risk Management Function operating within the Company. The Board has overall responsibility for ensuring an effective risk management system is in place

(International Organization for Standardization, 2009) and (Federation of European Risk Management Associations, 2011).

2.6.4 ISO 31000 – Process

Figure 5. ISO 31000-An Overview: Process

Risk management prevention measures are in use and in relation to identified risks. The development of a risk management framework involves conducting a risk assessment process of communication and consultation, establishing the context, risk assessment (risk identification, risk analysis, risk evaluation) risk treatment, monitoring and review with purpose to manage, reduce or eliminate a possible manifestation of material risks with potential negative impacts (International Organization for Standardization, 2009) and (Federation of European Risk Management Associations, 2011).

Communication and Consultation

The company needs to learn from customers what risk means outside of the organization. Stakeholders need to be informed. A system of communication and information needs to be performed into the environment of the organization regarding risk and management.

Establish the Context

The Company works within the CBC regulatory framework. The use of an internal model is subject to approval by the Board of Directors of the Company. The organizations internal model encompasses the regulatory rules and principles to ensure the initial and ongoing appropriateness of the internal model.

The framework should cover the whole life cycle of the internal model from model development to model implementation and use.

Risk Assessment

Risk identification and analysis

No list of risks can be excluded due to rapid changes of the information technology. However, a categorization of risks could help the organization in systematically identifying risks in the electronic banking organization. Most important risks categories of electronic money activities may be operational risk, reputational risk and regulatory risk and these are discussed further. EMI and PI organization should be focusing on the identification, assessment, mitigation and monitoring of the above-mentioned risks with potential to significantly threaten the achievement of company objectives. These are discussed, challenged and finalized with the responsible risk experts and/or risk owners throughout the company with actions to mitigate any risks where the risk is above target level. Risk identification may involve historical information, theoretical analysis, informed and expert opinions and stakeholders desires (Federation of European Risk Management Associations, 2011) (International Organization for Standardization, 2018).

Risk evaluation

The Risk and Control Self-Assessment (RCSA) is a risk management process by which the Company must ensure, through performance of a qualitative based analysis that effective controls or other risk mitigation activities are in place for all potentially large impact operational risks. Business experts are required to consider results from previous RCSA activities, and operational risk events, when carrying out the scenario analysis. (Ramar, 2014).

The management of legal and compliance and the outsourcing risk is covered as part of the broader operational risk management framework. In general, liquidity risk in the Company is a secondary risk following external events, such as natural disasters, that are generally reflected in the internal risk capital model (Kumar, 2008)

Risk Treatment – a cyclical process

The management of strategic risks is implicitly embedded into the execution of the annual Strategic Dialogue process, including the establishment of strategic priorities and execution of the steps towards their fulfillment. The Company performs an Own Risk and Solvency Assessment (ORSA) on at least an annual basis known as a regular ORSA, as well as following any internal or external events with potential to materially alter the Company's risk profile. The Management Risk Committee discusses the findings of the ORSA while challenging the outcomes were essential. The management comes to a decision if they proceed will recommending approval of the ORSA findings and report to the Board Risk Committee for review, challenge and/or recommendation to the Board for approval (Ministry of Finance Cyprus, 2017) and (Federation of European Risk Management Associations, 2011).

The Board has overall accountability for evaluating the ORSA findings report and challenging, either directly or through representatives, as applicable, the entirety of the evaluation and its assumptions and its ultimate acceptance. (Ministry of Finance Cyprus, 2017) and (Federation of European Risk Management Associations, 2011).

Monitoring and Review

The Company is committed to have an Internal Control System (ICS) that fulfils its organizational needs and all relevant regulatory requirements. The Company's Internal Control System is based on a strong control culture which emphasizes and demonstrates to all employees the importance of internal controls in the Company. As part of this, the Company seeks to avoid policies and practices that may provide incentives for inappropriate activities (Bachtiar, 2013).

On a regular basis, the compliance and risk management function identify, documents and assesses the compliance risk associated with EMI business activities. This helps to make

sure that the overall compliance framework reflects the risk exposure. The Company need to have an internal audit policy in place.

The Internal Audit policy constitutes a local adaption of the EMI and PI organization audit policy taking into consideration the specific circumstances and requirements of the company.

(Federation of European Risk Management Associations, 2011).

2.7 Types of Risks

According to Chernobai, Rachev and Fabozzi (2007:15) In finance, risk is the fundamental elements that affects financial behavior. Risk is a measure of uncertainty about the future outcomes and to capture the potential of sustaining a loss. Risk manager responsibility is to enable the detection of risks to which the organization might be exposed and to facilitate the implementation of corrective measures to mitigate those risks (Vasile and Croitoru, 2012).

The most material risks that might be faced by an EMI and PI organization are briefly described below.

2.7.1. Strategic Risk

Strategic risk is the risk that might cause to a corporation by unsuccessful business choices or lack therefrom. Strategic risk is usually a major factor in determining company's value, notably noticeable if the corporate experiences a pointy decline in a very short amount of your time (Clarke, 1999).

Impact High: Likelihood Low

Risk Mitigation

Quarterly meetings with the Board of Directors of the electronic money & payment institution and discuss issues relating to the competitive advantage of organization competition and opportunities the company can seek.

Clients' retention is an essential element of the company's business in order to prevent any material losses.

Risk Mitigations

1. Diversify client base and explore new markets and industry sectors.
2. Develop and maintain close client relations, to better adjust and fit their needs.
3. Offer clients a dedicated risk, sales and compliance account management team.
4. Expand to new and complementary services and lines of business.

The company workforce directly corelates to the company's results, thus finding the best talent in the industry and experienced management is key to building a leader in the online payments industry.

Risk Mitigations

Prioritize the recruitment of highly skilled workers and provide staff with the needed training to transform them into field specialists .

Emphasize team building and career development is an integral part of the company's infrastructure.

2.7.2. Regulatory Risk

Regulatory risk is the risk that a variation in laws and regulations will significantly influence the business of the company (PWC, 2021).

Impact High: Likelihood Medium to Low

Risk Mitigations

The complaint unit has procedures for monitoring European and National legislation, it also identifies changes and informs affected parties to implement the new requirements. In addition, the complaint unit should maintain a register with the new legislation in force. Where it is deemed necessary legal consultation is seeking.

2.7.3. Operational Risk

As stated by Central bank of Kenya, operational risk is the threat of failure resulting from insufficient or failed internal processes, individuals and systems or from exterior incidents.

Impact High: Likelihood Medium to Low

The key goal of an EMI organization is the Operational Risk Management Framework (ORMF) is to detect, evaluate, observe and report the risks to which the organization might be exposed to. To be efficient, it is mandatory that the framework to be consistent with business processes and will bring benefits the institution in financial and non-financial terms. To prove the value of operational risk a robust basis should be provided. (The Institute of Operational Risk, 2020)

Risk Mitigations

With the application of this six-stage process, EMI and PI organizations obtain the implementation of a robust risk management framework. The framework allows the institution to manage risk more efficiently, it also improves the dynamic intensity among risk and prospect (Kluwer, 2011).

The manageable framework for operational risk management is to comply with the multitude of regulatory requirements:

1. Risk detection
2. Basic risk management procedure
3. Reporting
4. Crucial risks, scenarios and wealth calculation
5. Risk appetite
6. Operational & audit contribution and reconsideration

(Kluwer, 2011)

Where practical, companies may employ three lines of defense as part of their operational risk governance and risk management structure. A robust risk culture with a well defined

communication and comprehension and a solid sense of risk consciousness can deliver comfort when used in combination with this approach (The Financial Service Authority, 2011).

The three lines to consist of the following:

1. The first line is provided by the business units – comprising the business units, support functions and embedded risk staff.
2. The second line is provided by the risk management function – comprising the operational risk management function and the compliance functions.
3. The third line is the Governance and oversight provided by the internal and external auditors.

(The Financial Service Authority, 2011)

2.7.4. Technology Risk

Technology risk is the likelihood of technology catastrophe with intent to disrupt the organization such as data protection cases or service outages. (Central Bank of Kenya, 2013).

Impact High: Likelihood Medium to Low

Risk Mitigations

The chief technology officer should participate in an IT think tank team of the organization that monitors technological advancements, trends opportunities and threats while close monitoring any technological upgrades. Implement a cyber risk insurance policy available from insurance agencies.

2.7.5. Financial Risk

Risk Relating to fraud and other types of financial crime.

- Jointly with settlement risk, this is the highest area of concern having both financial and reputation risks associated with it. The policy objective should maintain the maximum resource to mitigate this risk to the fullest extent.
- Avoid markets and products prone to high levels of risk.

Impact High: Likelihood medium but with risk mitigation likelihood can be reduced to low.

Risk Mitigations

Policies and procedures will involve:

1. AML Policy including
    a. Compliance policy
    b. Criminal activity reporting
    c. Customer selection
2. PEP Sanctions policy
3. Anti bribery policy
4. Fraud monitoring systems
5. Staff recruitment and ongoing training
6. Documented policies and procedures
7. Market and product review
8. Working with regulators/partners to ensure all policies are up to date with current requirements.

2.7.6. Fraud Risk

Internal fraud arise when a present or ex-worker take the opportunity to thieve, amend or destroys organizational information (such as customer data) or assets (such as computer software or physical assets) for private benefit. It may involve unethical activities concerning blackmail it may involve conspiracy with other individuals or it may include misrepresentation of financial or other business documents. (Deloitte, 2016).

Impact High: Likelihood Medium to Low

Risk Mitigations

1. Security Awareness Program
2. Physical Access Management
3. Two-factor authentication (external)
4. Advanced Email Solution (Microsoft)

5. Backup of all important information

2.7.7. Reputational Risk

Reputational risk is the threat of exposure possibility to the good name or standing of the company.

Impact High: Likelihood Low

Risk Mitigations

Reputational risk is part of the organization strategy and planning. The control processes of technology should allow to reduce the likelihood and security of event that could cause reputational damage. A certificate of Good Standing of the company is considered essential.

2.8 Risk and Opportunities (COVID-19)

Employers should have a guide based on resources, guides and directives published by the World Health Organization (WHO), Cyprus Government, employers and other business practices. Employers and managers, in consultation with employees, ought to do and often update the risk assessment for work related exposure to COVID-19, ideally with the support of activity health services.

The employer has a duty to ensure the safety and health of the staff and others in the workplace. This includes providing and maintaining a work environment that is without risk to health and safety and adequate facilities for staff in carrying out their work, as is reasonably practicable (World health organization, 2020).

2.8.1 Low Exposure Risk

Organizations who fall under the category of low exposure risk are the jobs or work without frequent or close contact with the overall public or others. Workplace staff of this group have minimal or no activity contact with the people and different co-workers due to the ability of providing remote services. EMIs and PI organizations might embrace and be more familiarized with this category due to capacity of remote staff i.e., functioning from home or divided into two separated teams who would either work at the office following guidelines of the world health organization of 1 person per 8 square meters ratio or work from home (World health organization, 2020).

2.8.2 Medium Exposure Risk

Organizations who fall under the category of medium exposure risk are the jobs or work with frequent or close contact with the overall public or others. Workplace staff of this group have regular and activity contact with the people in high-population or mass work environments. EMI and PI organization do not fall under the category of medium exposure risk level. Organizations who fall under this risk level are industries of frontlines workers e.g., coffee shops or food marketplaces and public transportation where physical distancing of a minimum 1 metre may be difficult to observe (World health organization, 2020).

2.8.3 High Exposure Risk

Organizations who fall under the category of high exposure risk are the jobs or work who most likely have contacted people infected or suspected to have contacted people of having the virus of COVID-19 and where objects and surfaces possibly contaminated with the virus. EMI and PI organization do not fall under the category of high exposure risk level. Organizations who fall under this risk level are domestic services, delivery providers, home repair technicians who were known or suspected of having COVID-19 and provide services to either homes or home care where physical distancing of a minimum 1 metre is very difficult to observe (World health organization, 2020).

CHAPTER 3

METHODOLOGY APPROACH AND METHODS

3.1 Pragmatism

The research methods of this study were based on a pragmatic philosophy and methodology utilized by mixed methods approach of qualitative and quantitative elements. Pragmatism as a research paradigm denies getting involved in theories such as reality apart from human practice. However, it recognizes that there can be one or numerous realities that are unclose to empirical research (Creswell and Clark 2011). Pragmatist researchers have presented their special opinion that there is an independent reality that exists apart from human adeptness. Nevertheless, the reality is there and it can only be meet through human adeptness (Goles and Hirschheim 2000; Morgan 2014a; Tashakkori and Teddlie 2008). The crucial foundation of pragmatist philosophy is that knowledge and reality are built on certainty and behaviors that are socially constructed (Yefimov 2004). Pragmatists agree that the knowledge worldwide is socially built, even though some of them match individuals experiences more than others (Morgan 2014a). Realists disbelieve that reality is decided once and for everyone (Pansiri 2005). Furthermore, as long as it helps individuals to build acceptable relation with other elements reality is true according to pragmatists (James 2000). The pragmatist would not identify an object according to what it looks like or what it is being used for, but instead based on how it would assist them to accomplish their aim (Goles and Hirschheim 2000, p. 261) and (Kaushik, and Walsh, 2019).

3.2 Mixed Methods

Mixed methods research as described by Creswell & Clark (2011, pp. 7–11) is to understand the research objective through multiple research phases because one data source may be insufficient to answer the question. Qualitative methods will be executed from 4 interviews of qualified individuals with open-ended questions. Quantitative methods will be executed from the questionnaire of 50 individuals with closed ended questions. Finally, we defined the limitation of the research methodology and how may the outcome be influenced by those limitations (American Psychological Association. 2020).

The basic notion of a mixed methods approach is that the joint qualitative outcome and quantitative results produce additional information not collected only from the qualitative or quantitative results but thought the combination of them (Creswell, 2015; Greene, 2007; Tashakkori & Teddlie, 2010).

The most common and well-known approach to mixing methods is the Triangulation Design (Creswell, Clark, et al., 2003). The purpose of this design is to achieve different but paired data on the same topic (Morse, 1991, p. 122) with aim to greatly understand the research dilemma. The intention in utilizing this design is to merge the different strengths and nonoverlapping weaknesses of quantitative methods with those of qualitative methods (Patton, 1990). This design and its fundamental aim of uniting different methods has been discussed broadly in the literature (e.g., Jick, 1979; Brewer & Hunter, 1989; Greene et al., 1989; Morse, 1991). The Triangulation design is mainly utilized when a researcher wish to compare quantitative outcomes with qualitative results or simply to justify or outstretch quantitative outcomes with qualitative elements. Involves enhanced resources. After all, mixed methods research are labor strenuous, need vital and essential amount of resources plus time rather than those conducting a single method research (American Psychological Association. 2020) and (Brown, 2018).

3.3 Data Collections Methods

The data collection method was accomplished through 50 data collection surveys and 4 interviews questions from 4 EMI and PI organizations in Cyprus. The interview questions and the surveys have been sent via email to the representative of each organization and

upon participation acceptance, an email and/or a hard copy followed to the central offices of the institutions and more specifically: During the 1st approach, 4 data collection surveys to the 1st company via hand, 3 data collection surveys to the 2nd company via email, 3 data collection survey to the 3rd company via email. During the 2nd approach, 14 data collection surveys to the 1st company via hand, 10 data collection surveys to the 2nd company via hand, 11 data collection surveys to the 3rd company via hand and 5 data collection survey to the 4th company via email. EMI and PI institutions where are all located at Nicosia, Cyprus. Interviews questions have been sent via email to the four representative managers of each organization in the areas of: Compliance Manager & AMLCO, Head of Compliance & AMLCO, Executive Director, Compliance Manager.

Table 1. Data Collection Method

Code Name	EMI Representatives	1st approach (Surveys)	2nd approach (Surveys)	Total Surveys	1st approach (Interview Questions)	2nd approach (Interview Questions)	Total Interview Questions
#1	Compliance Manager & AMLCO	4 via hand	14 via hand	18	1 via email	1 via email	1
#2	Head of Compliance & AMLCO	3 via email	10 via hand	13	1 via email	1 via email	1
#3	Executive Director	3 via email	11 via hand	14	1 via email	1 via email	1
#4	HR Officer	0 via email	5 via email	5	0 via email	1 via email	1
				Total: 50			Total: 4

Our target was to approach all the EMIs and PIs in Cyprus to get the maximum results, overall are 12 operating institutions. The researcher manages to collect data from 4 institutions due to confidentiality policy, reporting obligations, deadlines given by the regulator and restrictions of Covid-19 pandemic. The total number of the employees in the 4 EMI and PI organizations are 95. From those, 50 of them have finally responded to the questionnaires, that is considered as the final sample. Our target was to approach 60 of them we have not received full responses from 10 questionnaires that seems to be incomplete due to COVID-19 pandemic and restrictions measures announced by Cyprus

government, less people in the offices. Even though the researcher can positively reveal that the response rate of the sample collected from the questionnaires is 83% and from the interviews 100%.

The data collection from the questionnaires was not the ultimate. The period that the questionnaires were available in the EMI and PI institutions was during the second lockdown period in Cyprus which a significant amount of personnel were working from home or was on obligatory leave. However, the sample from the questionnaires with this dimension of 83% response rate may bring significant and reliable outcome. The lack of previous research studies on the topic did not affect the researcher from being accurate and the performing results was satisfactory.

3.4 Constructing and Analyzing the Data Collection Survey

1. Do you consider risk management an important function for your organization?

Purpose of first question:

Target was to understand if the employees considered risk management as an important function of the company. With this question we were able to get the general idea from each employee and how do they approach risk management.

Answer was:

Strongly Disagree☐

Disagree☐

Neutral☐

Agree☐

Strongly Agree☐

2. Does risk management improve business performance?

Purpose of second question:

Target was to understand if the employees have a general knowledge about risk management and if risk management may improve business performance according to their believes.

Answer was:

Strongly Disagree☐

Disagree☐

Neutral☐

Agree☐

Strongly Agree☐

3. **Is top management involved in risk management processes?**

Purpose of third question:

Target was to understand if top management is involved in risk management process and if employees have the knowledge of that and the general approach.

Answer was: Yes or No.

4. **Does your organization have a procedure manual and policies of risk management?**

Purpose of fourth question:

The target was to understand if the organization maintain a risk manual and policies of risk management in place available and readable for all employees independent of their position in the company.

Answer was: Yes or No.

5. **Does your organization maintain a risk register scoring the likelihood, impact and severity of potential risks that may affect business performance or obligations?**

Purpose of fifth question:

Target was to understand if a risk register is available and if there was a categorization and monitoring of potential risks that might affect the organization as an entity.

Answer was: Yes or No.

6. **Have you ever been informed what kind of risks your organization might be exposure to?**

Purpose of sixth question:

Target was to understand if the employees of the organization are familiar and informed about organizational risks that might affect their organization.

Answer was: Yes or No.

7. What type of risks it could have the highest impact in your company?

Purpose of seventh question:

Target was to understand if the employees where sufficiently informed about the highest risk that their company might be exposed to.

Answer was: Choose the highest impact risk.

Strategic Risk☐

Regulatory Risk☐

Operational Risk☐

Technology Risk☐

Financial Risk☐

Fraud Risk☐

Reputational Risk☐

8. What type of risk it could have the lowest impact in your company?

Purpose of eighth question:

Target was to understand if the employees where sufficiently informed about the lowest risk that their company might be exposed to.

Answer was: Choose the lowest impact risk.

Strategic Risk☐

Regulatory Risk☐

Operational Risk☐

Technology Risk☐

Financial Risk☐

Fraud Risk☐

Reputational Risk☐

9. How often do you take trainings internal or external regarding issues of risk management?

Purpose of ninth question:

Target was to understand if employees take trainings internal or external regarding risk management and on the other hand to identify if they were sufficiently informed about risk management issues.

Answer was: Choose how often.

Never☐

1-2 per year☐

3-4 per year☐

5-6 per year☐

More than 7☐

10. Are you aware if your organization has a BCP in place at the current time?

Purpose of tenth question:

Target was to understand if the employees of the organization are aware if their organization maintain a business continuity plan (BCP) since it helps to avoid and mitigate risks associated to any disruption of the company.

Answer was: Yes or No.

11. How often do you believe a business continuity plan should be revaluated?

Purpose of eleventh question:

Target was to understand if the employees believe that a business continuity plan should or should not be revaluated.

Answer was: Choose of the below.

Never☐

Daily☐

Monthly☐

Quarterly☐

Yearly☐

12. Did you participate in an exercise of the business continuity plan with or without any cause?

Purpose of twelfth question:

Target was to understand if the employees of the organization have participated in an exercise of the business continuity plan with or without any cause. The strategy of business continuity plan needs to be tested regularly.

Answer was: Yes or No.

13. Are you familiar with guidelines against COVID -19 pandemic in Cyprus Government?

Purpose of fourteenth question:

Target was to understand if the employees are familiar and continuously informed with the guidelines against COVID -19 pandemic in Cyprus Government.

Answer was: Yes or No.

14. Does your company maintain a handbook of COVID-19 pandemic available for employees?

Purpose of fifteenth question:

Target was to understand if the employer offered to the employees the option of being familiar and informed regarding COVID-19 pandemic.

Answer was: Yes or No.

15. During the crisis of COVID -19 pandemic was you company able to continue working?

Purpose of sixteenth question:

Target was to understand if the company was able to continue working during the crisis of COVID-19 and if they have any disruptions.

Answer was: Yes or No.

16. Did you have any meetings or trainings against the COVID-19 virus?

Purpose of seventeenth question:

Target was to understand if the company offered to the employees the option for meetings or trainings against the COVID -19 virus.

Answer was: Yes or No.

17. **Are you satisfied with what your company did to protect the employees from the COVID-19 virus?**

Purpose of eighteenth question:

Target was to understand if the employees are feeling satisfied and secure with what the company did to protect them from COVID-19 virus.

Answer was: Choose of the below.

Strongly Disagree☐

Disagree☐

Neutral☐

Agree☐

Strongly Agree☐

18. **Did risk management helped your organization to overcome a crisis event like Covid-19 pandemic?**

Purpose of nineteenth question:

Target was to understand if the employees are feeling satisfied and comfortable with risk management and if it may help their organization to overcome from a crisis like COVID-19 pandemic.

Answer was: Yes or No.

3.5 Constructing and Analyzing the Interviews Questions

1. **Does your organization have a procedure manual and policies of risk management?**

The purpose of risk management manual is to provide an overview of the risk management processes and framework within the organization. The aim is to give a practical guidance for the management of risk within departments and teams, to decrease the frequency of incidents and to reduce impact of incidents if they occur.

The purpose of the risk management policy is to provide guidance regarding the management of risk, to support the accomplishment of business objectives, safeguard employees and business assets while ensure financial sustainability.

2. **Which are the most material risks an EMI organization faces during specific crises?**

The purpose of the questions is to understand which are the most material risks of an EMI and PI organization in Cyprus. The aim is to enable the detection of risks to which the organization might be exposed and to facilitate the implementation of corrective measures to mitigate those risks.

3. **How to manage, reduce or eliminate a possible manifestation of material risks with potential negative impacts?**

The purpose of the question is to understand how to manage, reduce or eliminate a possible manifestation of material risks with potential negative impact.

The aim is to monitor the material risk with potential negative impact:

a) Identify the risk itself and on time.
b) Avoid or eliminate the risk itself.
c) Use the transfer approach, transfer the risk to a third party.
d) Mitigate, with mitigation we reduce the likelihood of risk incidence or it reduce the impact of the risk within acceptable limits.

4. **What are risk management prevention measures in use and in relation to the identified risks?**

The purpose of the question is to understand what the risk management prevention measures in use are and in relation to the identified risks.

The aim is to be able to identify and manage potential risks that may affect the workplace. Risk management prevention measures are actions taken in response to the identified risk factors that may potentially cause an insistent or harm the organization activities. The management measures should either be designed to minimize the risks or eliminate them fully, with the latter clearly being most popular.

5. **Does your organization maintain a risk register scoring the likelihood, impact and severity of potential risks that may affect business performance or obligations?**

The purpose of the question is to recognize if the organization maintain a risk register with scoring the likelihood, impact and severity of potential risks that may affect the organization performance or the business obligations. Therefore, every EMI organization should maintain a risk register since it is a tool used to manage risks and to comply with regulatory acts as repository of all identified risks.

6. **Did you participate in an exercise of the business continuity plan with or without any cause? Does your company have any contingency or disaster recovery plan in place? How often do the employees take trainings internal or external regarding issues of risk management?**

The purpose of the questions is to recognize if the organization exercise the business continuity plan along with the disaster recovery plan and if the employees take trainings regarding risk management. Business continuity and disaster recovery plan should be test regularly in order be verified how efficiently is in real time scenarios. Risk management training can benefit the organization since it helps the employees to understand how important is to be able to recognize and manage the organizational risks while exercising their dally duties. Trainings will improve employee's performance and the broader enterprise.

7. **Does your company maintain a handbook of COVID-19 pandemic available for employees? During the pandemic was you company able to continue working? Did you have any meetings or trainings against the virus?**

The purpose of the question is to recognize if the organization maintain a handbook of COVID-19 pandemic available for employees, if the company was able to continue working during the pandemic and if they had any meetings and trainings against the virus. A handbook of COVID-19 could be considered as progressive for an organization since the virus came to our lives without any warnings. Business was mainly struggling to safeguard their continues performance and to avoid any discontinuation of their business obligations. Employees are part of the organization and the employer should consider

them as a true asset since they contribute to success of an organization therefore meeting and trainings are significant against the virus combating.

8. How to utilize a crisis and adapt it into organizational opportunity (e.g., COVID-19 vs electronic banking)

The purpose of the question is to recognize if the organization utilize the crisis and adapt it into organizational opportunity. Opportunity is where the chance is.

Lockdown and restrictions announced by the government on in-individual services, have obliged the banks to immediately arrange an enhanced number of virtual services. EMI companies where already into that part of services and they were positively benefit from it, if you are expanding digital services you reduce time and cost.

With COVID-19 pandemic the EMI and PI organizations were able to increase customer relationships, data protection and cyber security. Upgrading their software development apps, use contactless cards and apple pay payments since the pandemic has dramatically accelerated the rate of digital adoption in financial services.

9. Did risk management helped your organization to overcome a crisis event like the COVID-19 pandemic?

The purpose of the question is to recognize if risk management function was able to help the company to overcome a crisis event like the COVID-19 pandemic.

Within the latest risk assessment results COVID -19 pandemic has been categorized as a high-risk level worldwide. A risk interconnectivity analysis should be assessed to understand other major business risks triggered by the virus. The current internal audit testing plans should be re-examined to ensure that they sufficiently cover pandemic risk aspects. Have risks been emerged such as enhanced cyber risks due to a remote workforce that need to be addressed. Policies and procedures should be in place to report, gather and analyze evolving risks as this situation progresses. COVID-19 may impact your controls reporting to stakeholders and the service organization's controls reporting. Risk is the main cause of uncertainty in any organization. Therefore, companies should be focusing on identifying and managing risks that may or may not cause disruption or discontinuation of daily obligations and business performance.

CHAPTER 4

DATA PRESENTATION & ANALYSIS

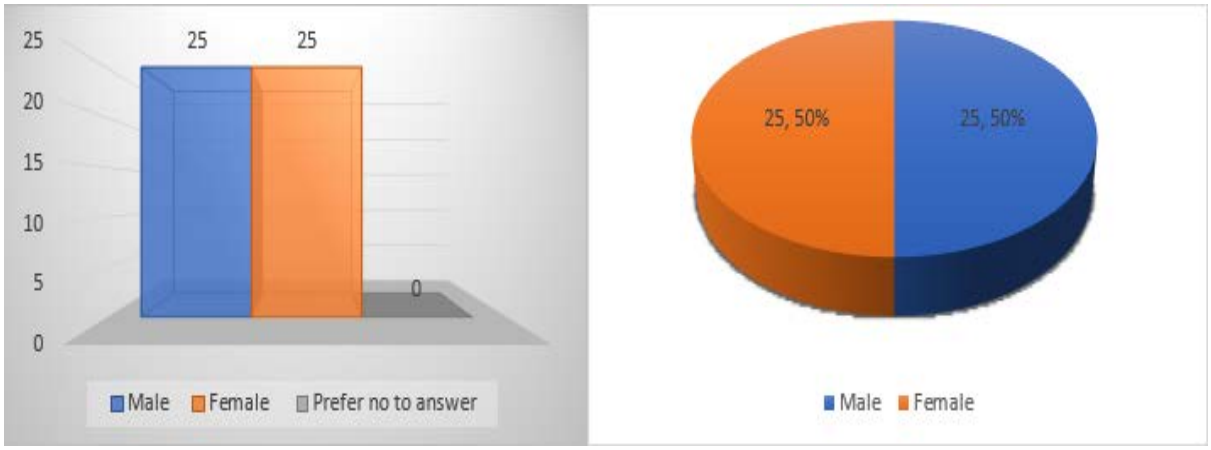
This section will present the results relating to data presentation and analysis. The researcher will analyze and implement the findings of demographics and participants characteristics, data collection surveys and interview questions. All of the above have been collected and edited in Microsoft Excel program. Results are presented for each Electronic Money and Payments institution separately and graphs demonstrates the overall surveys results from 50 employees and 4 Electronic Money and Payments institutions.

4.1 Demographics and Participant Characteristics Analysis

Table 2. Total Surveys in Each Organization

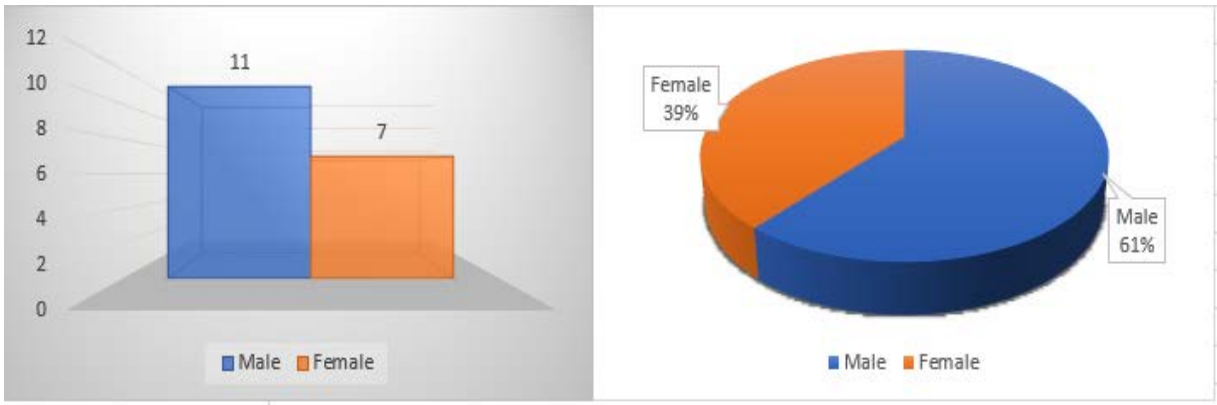
Electronic Money and Payment Institutions	Total Surveys
Institution #1	18
Institution #2	13
Institution #3	14
Institution #4	5

Figure 6. Gender

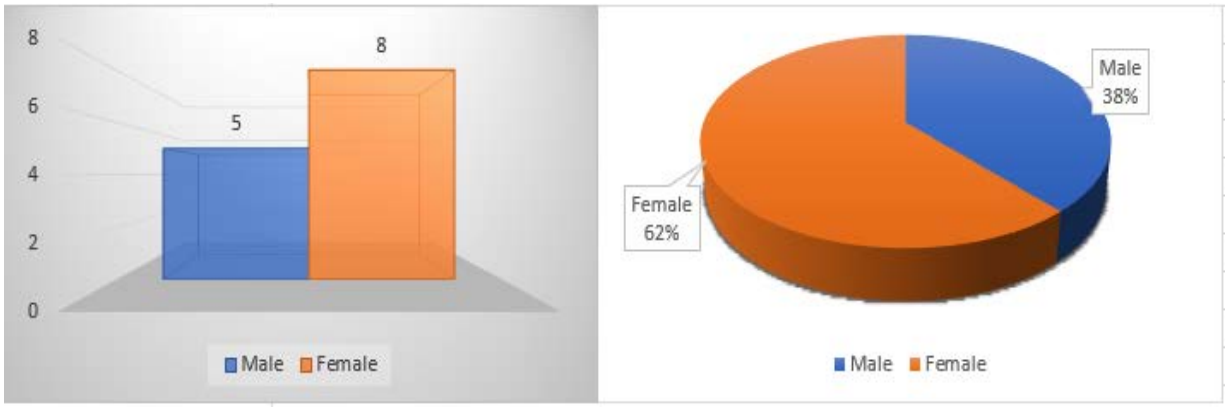


The above graph and chart demonstrates the genders of total surveys it involves 25 males with a rate of 50% and 25 females with a rate of 50%.The total number of employees are 50 from 4 EMI and PI institutions in Cyprus.

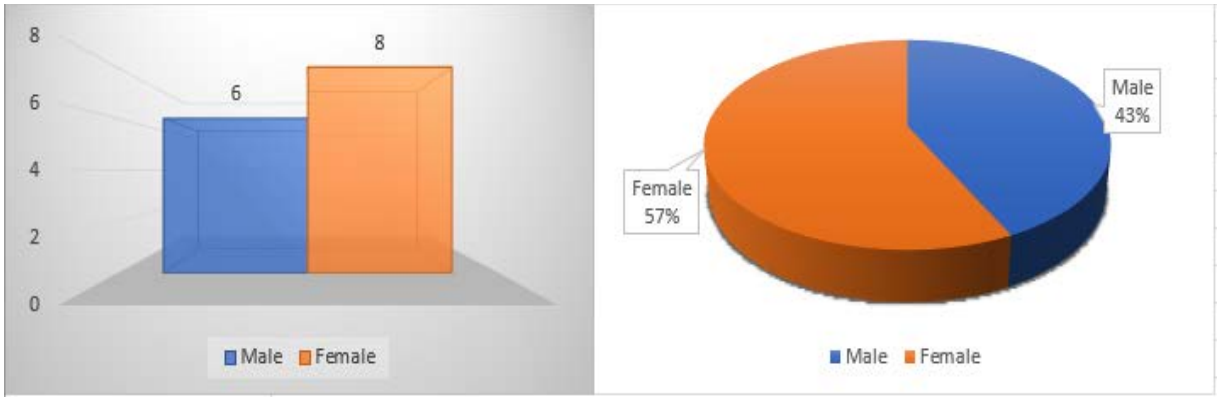
Company #1, the survey involved 11 males with a rate of 61% and 7 females with a rate of 39%. The total number of employees are 18 from EMI and PI institutions #1.



Company #2, the survey involved 5 males with a rate of 38% and 8 females with a rate of 62%. The total number of employees are 13 from EMI and PI institutions #2.



Company #3, the survey involved 6 males with a rate of 43% and 8 females with a rate of 57%. The total number of employees are 14 from EMI and PI institutions #3.



Company #4, the survey involved 3 males with a rate of 60% and 2 females with a rate of 40%. The total number of employees are 5 from EMI and PI institutions #4.

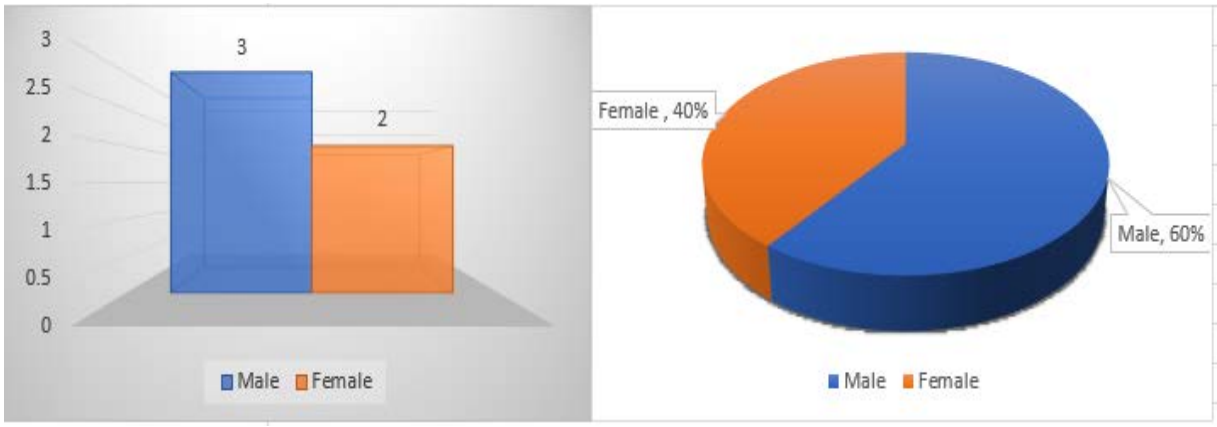
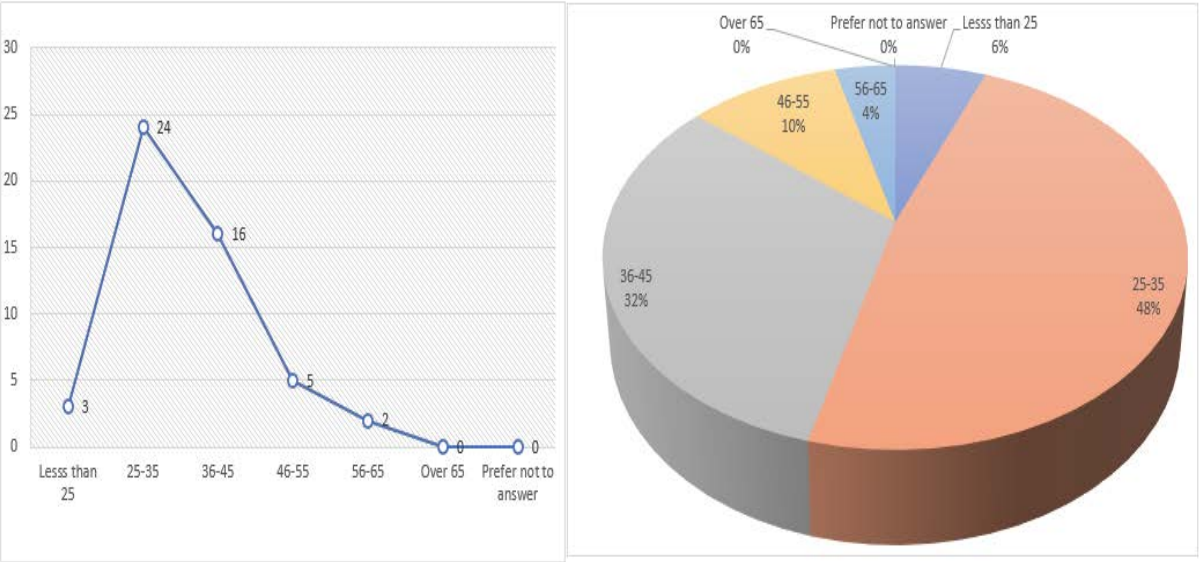
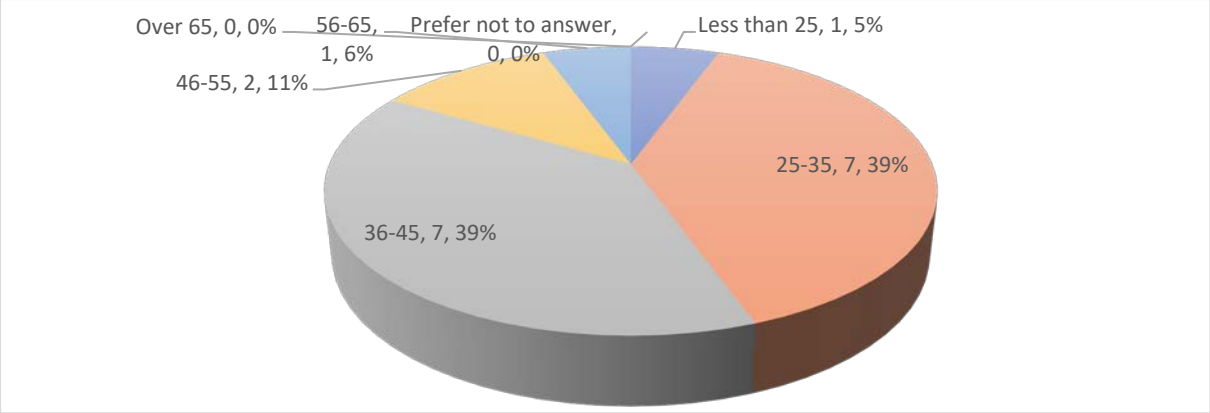


Figure 7. Age

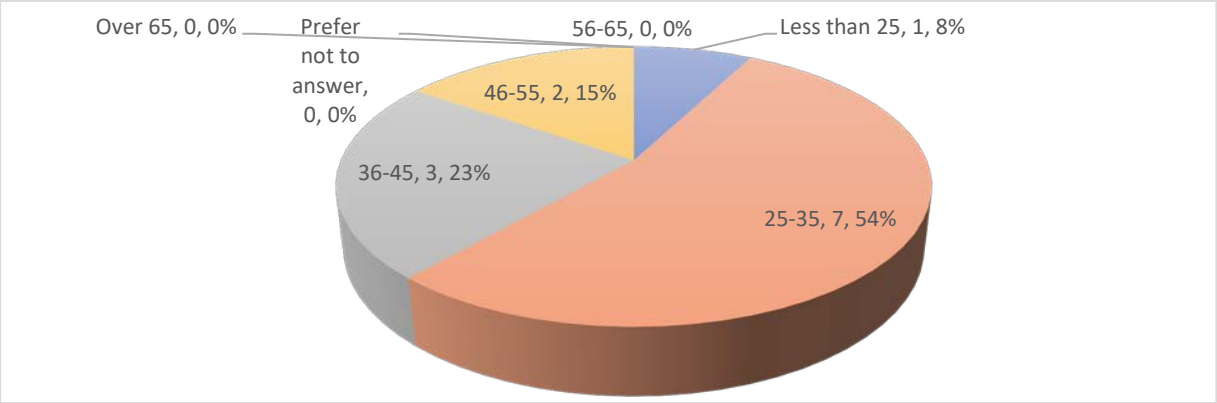


Following the graph and chart above demonstrates the age of employees of total surveys it involves 1 individual with age of less than 25 and a rate of 6%, 24 individuals with age of 25-35 and a rate of 48%, 16 individuals with age 36-45 and a rate of 32%, 5 individuals with age 46-55 and a rate of 10%, 2 individuals with age of 56-65 and a rate of 4%, 0 individuals with age over 65 and a rate of 0% and 0 individuals prefer not to answer with a rate of 0%. The total number of employees are 50 from 4 EMI and PI institutions in Cyprus. The researcher can observe that the majority of employees with the highest rate is concerning firstly 24 employees with ages from 25-35 and secondly 16 employees with ages between 36-45. The lowest employees are 2 with ages from 56-65. There are not at all employees with age over 65.

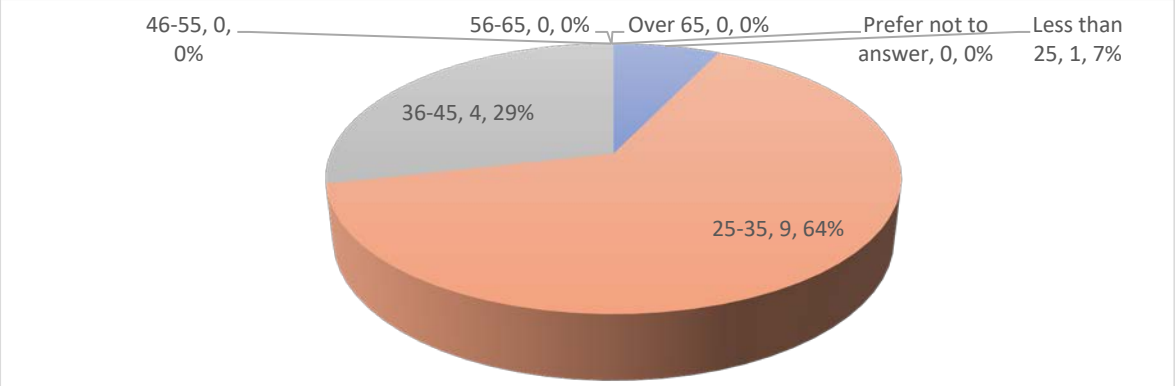
Company #1, the survey involved 1 individual with age of less than 25 and a rate of 5%, 7 individuals with age of 25-35 and a rate of 39%, 7 individuals with age of 36-45 and a rate of 39%, 2 individuals with age of 46-55 and a rate of 11%, 1 individual with age of 56-65 and a rate of 6%, 0 individuals with age over 65 and a rate of 0% and 0 individuals prefer not to answer with a rate of 0%. The total number of employees are 18 from EMI and PI Institution #1. We can observe that ages between 25-35 and 36-45 have the same number of 7 employees and a rate of 39%. The lowest employees are 1 from less than 25 and ages between 56-65. There are not at all employees with age over 65.



Company #2, the survey involved 1 individual with age of less than 25 and a rate of 8%, 7 individuals with age of 25-35 and a rate of 54%, 3 individuals with age of 36-45 and a rate of 23%, 2 individuals with age of 46-55 and a rate of 15%, 0 individuals with age of 56-65 and over 65 with a rate of 0%, 0 individuals prefer not to answer with a rate of 0%. The total number of employees are 13 from EMI and PI Institution #2. We can observe that ages between 25-35 have the highest number of 7 employees and a rate of 54%. The lowest employees are 1 with age less than 25.



Company #3, the survey involved 1 individual with age of less than 25 and a rate of 7%, 9 individuals with age of 25-35 and a rate of 64%, 4 individuals with age of 36-45 and a rate of 29%, 0 individuals with age of 46-55, 56-65 and over 65 with a rate of 0% and 0 individuals prefer not to answer with a rate of 0%. The total number of employees are 14 from EMI and PI Institution #3. We can observe that ages between 25-35 have the highest number of 9 employees and a rate of 64%. The lowest employees are 1 with age less than 25 and rate of 7%. There are not at all employees between 46-55, 56-65 and over 65.



Company #4, the survey involved 1 individual per age of 25-35, 46-55 and 56-65 and a rate of 20%. 2 individuals with age of 36-45 and a rate of 40% and 0 individuals with age of less than 25, over 60 and prefer not to answer with a rate of 0%. We can observe that ages between 36-45 have the highest number of 2 employees and a rate of 40%. The lowest employees are 1 between ages 25-35, 46-55 and 56-65 with rate of 20%. There are not at all employees between less than 25, over 65.

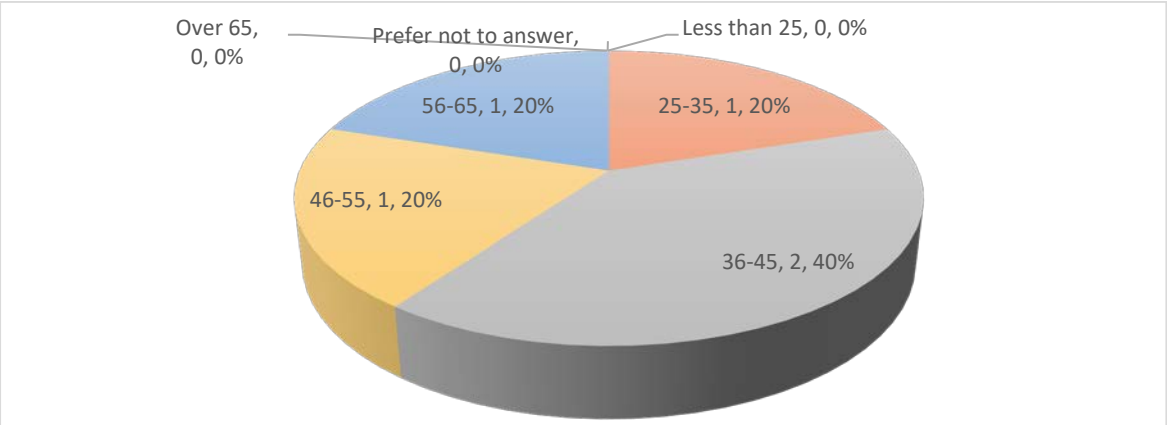
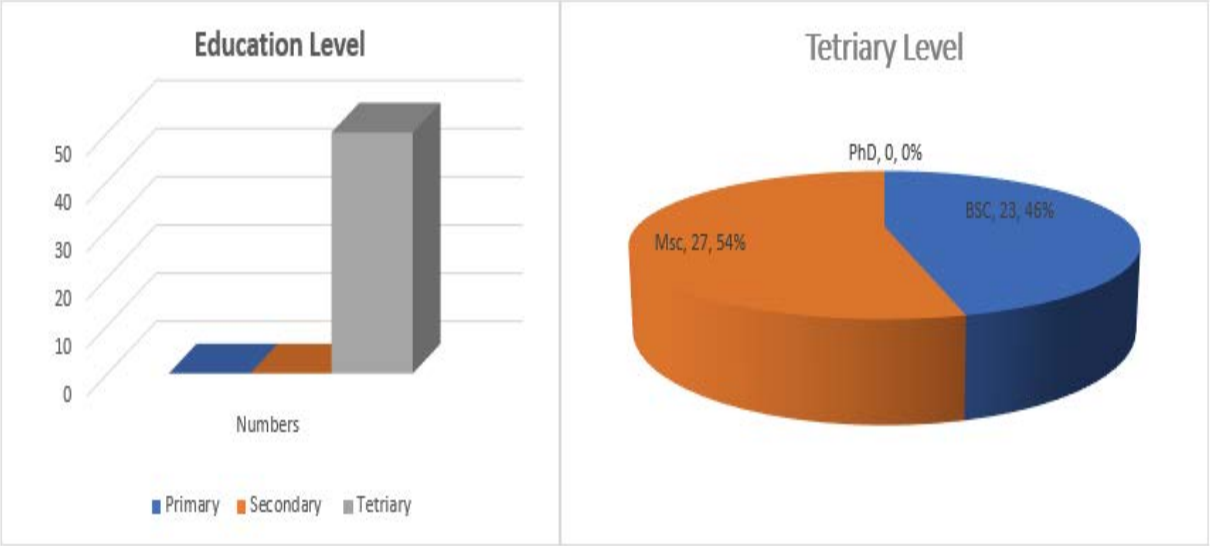
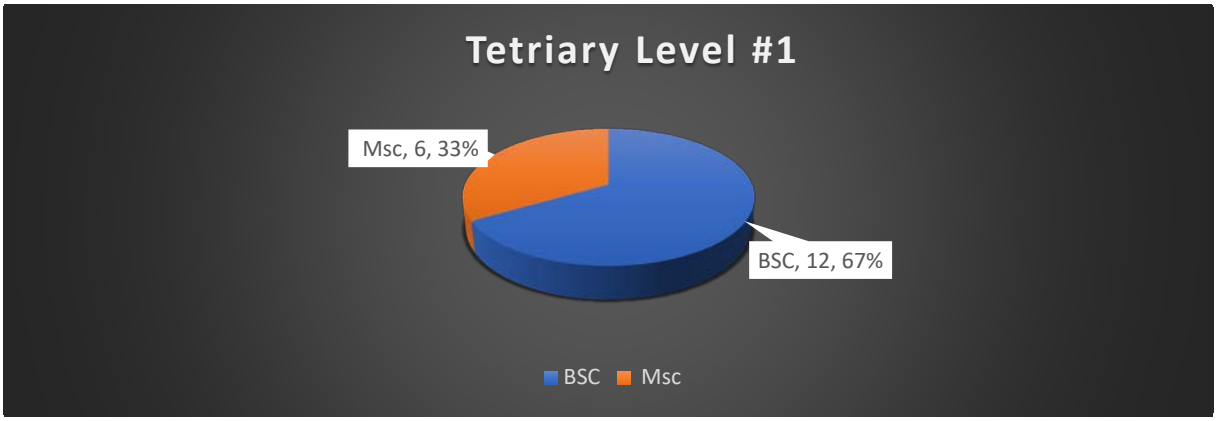


Figure 8. Educational Level

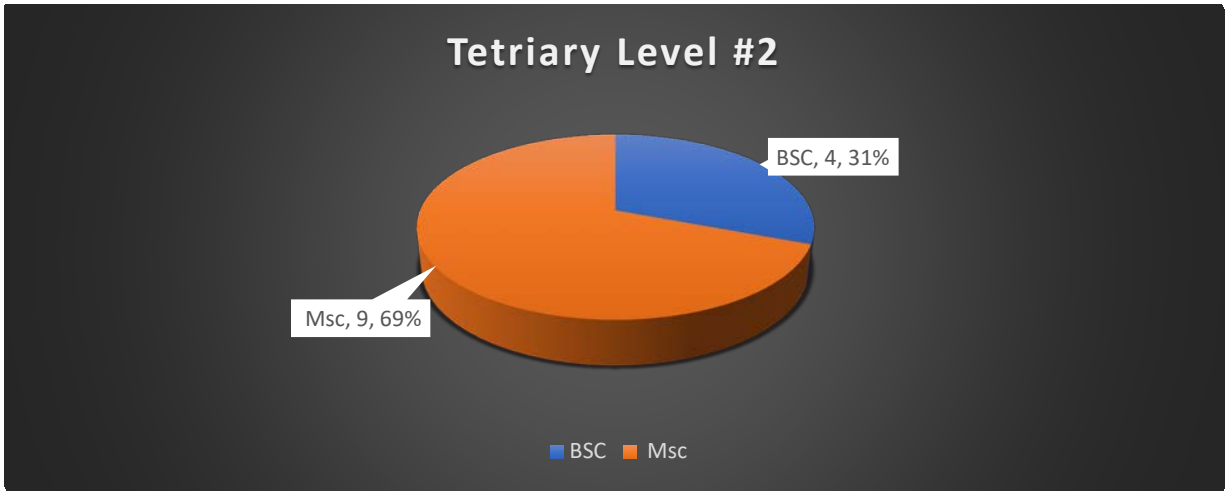


The above graph and chart demonstrate the education level of total surveys it involves 50 employees with tertiary level of education and 0 employees with primary and secondary level of education. Regarding tertiary level of education, we examine that 23 employees are holders of Bachelor of Science degree with a rate of 46% and 27 employees are holders of a Master of Science degree with a rate of 54%. No one over 50 employees hold Doctor of Philosophy degree. The researcher can observe that EMIs and PIs Institutions prefer employees with tertiary level of education and most preferably Master of Science. According to Demb, "Master's thesis plays a key role in three dimensions of graduate education: quality evaluations of programs, student mastery of a recognizably valuable set of learning outcomes, and as a facilitator in resolving certain developmental issues experienced by people in their twenties."

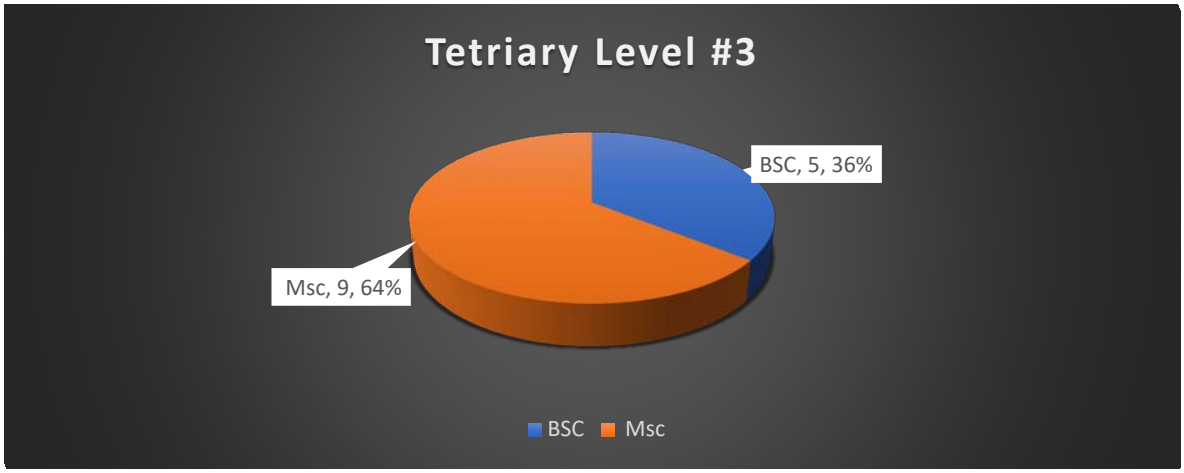
Company #1, the survey involved employees with tertiary level of education only and more specifically 12 individuals holding of BCs with a rate of 67% and 6 in individuals holding of MSc with a rate of 33%. The total number of employees are 18 from EMI and PI institution #1. We can observe that company #1 has much more bachelor's degree employees rather than master's degree employees. This should have been controlled more since education level is an important factor. Master's degree helps individuals to gain special knowledge and being more advance in the field of their expertise and it enhance professional network (Demb, 1999).



Company #2, the survey involved employees with tertiary level of education only and more specifically 9 individuals holding of MSc with a rate of 69% and 4 in individuals holding of BSc with a rate of 31%. The total number of employees are 13 from EMI and PI institution #2. We can observe that company #2 has much more master's degree employees rather than bachelor's degree employees.



Company #3, the survey involved employees with tertiary level of education only and more specifically 9 individuals holding of MSc with a rate of 64% and 5 in individuals holding of MSc with a rate of 36%. The total number of employees are 14 from EMI and PI institution #3. We can observe that company #3 has much more master's degree employees rather than bachelor's degree employees.



Company #4, the survey involved employees with tertiary level of education only and more specifically 3 individuals holding of MSc with a rate of 60% and 2 in individuals holding of MSc with a rate of 40%. The total number of employees are 5 from EMI and PI institution #4. We can observe that company #4 has again more master's degree employees rather than bachelor's degree employees.

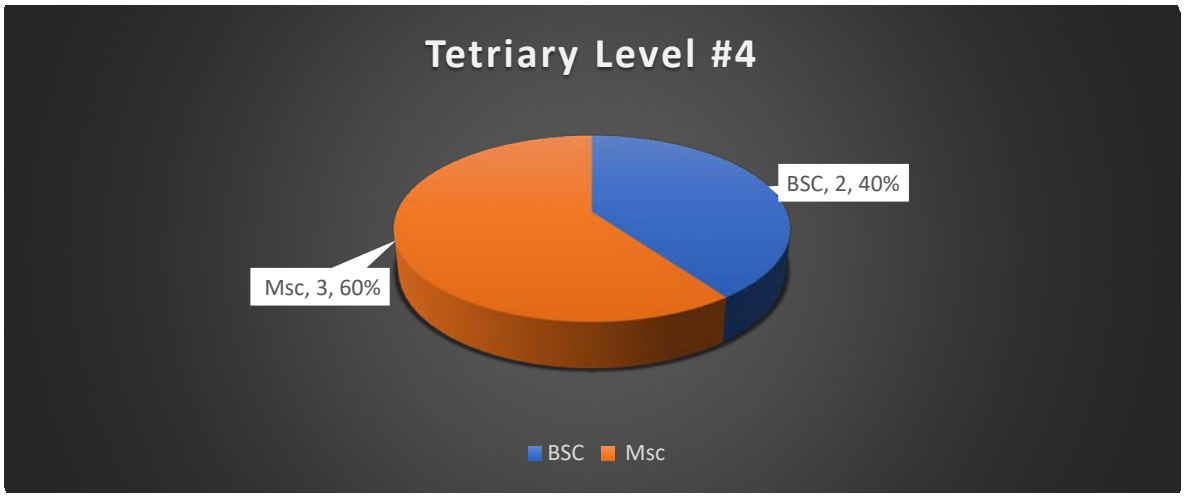
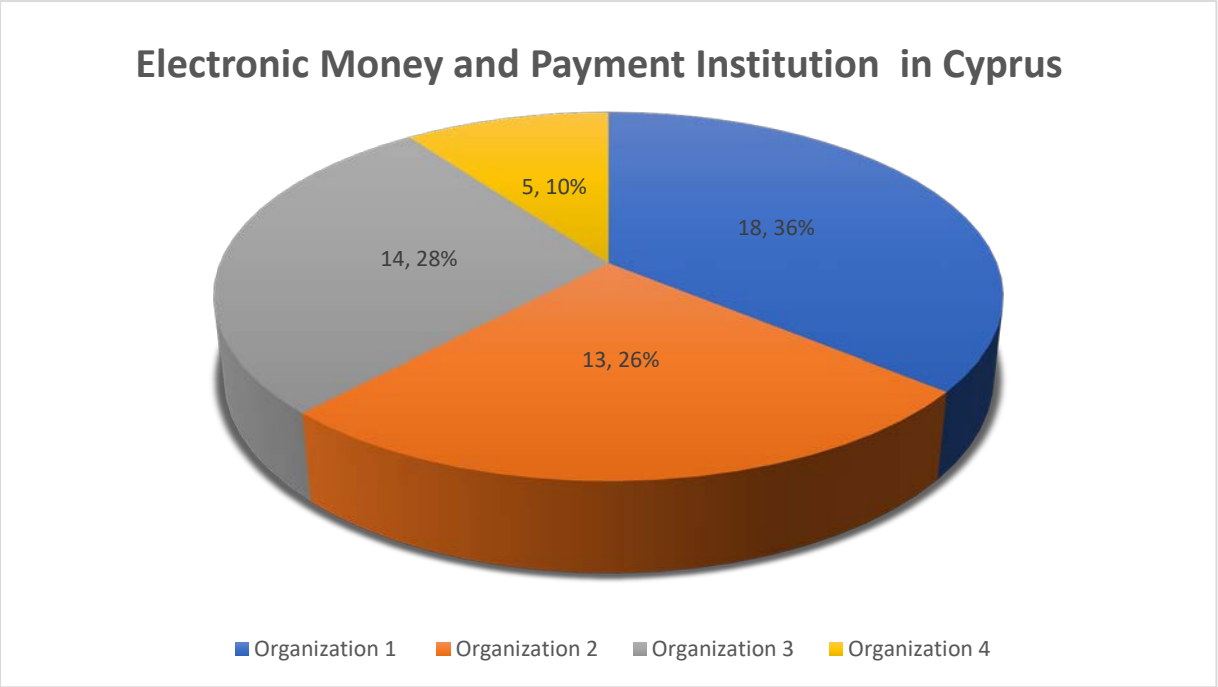
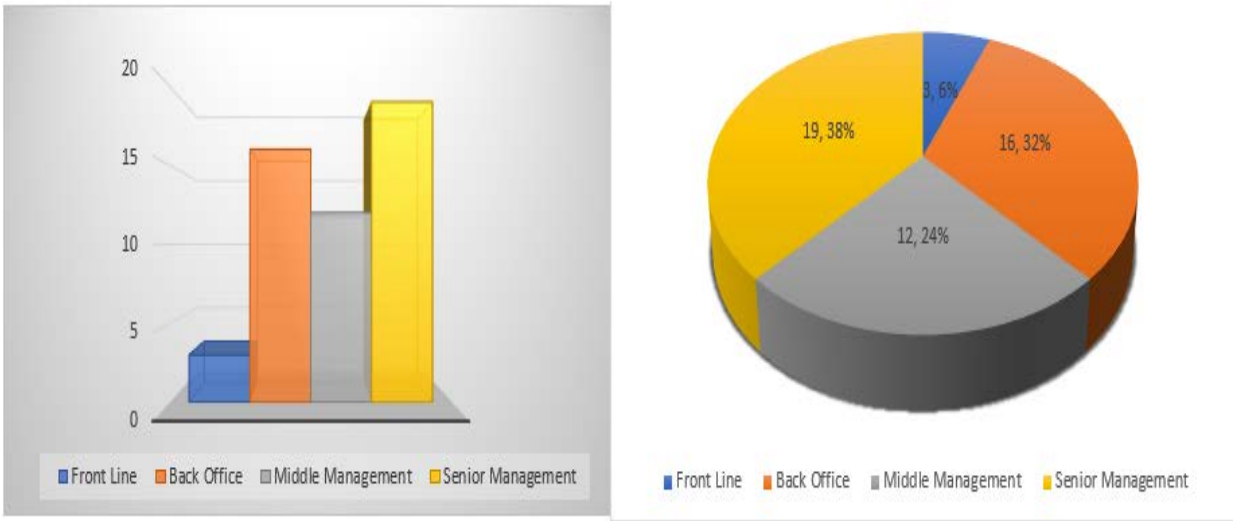


Figure 9. Type of Business you Work



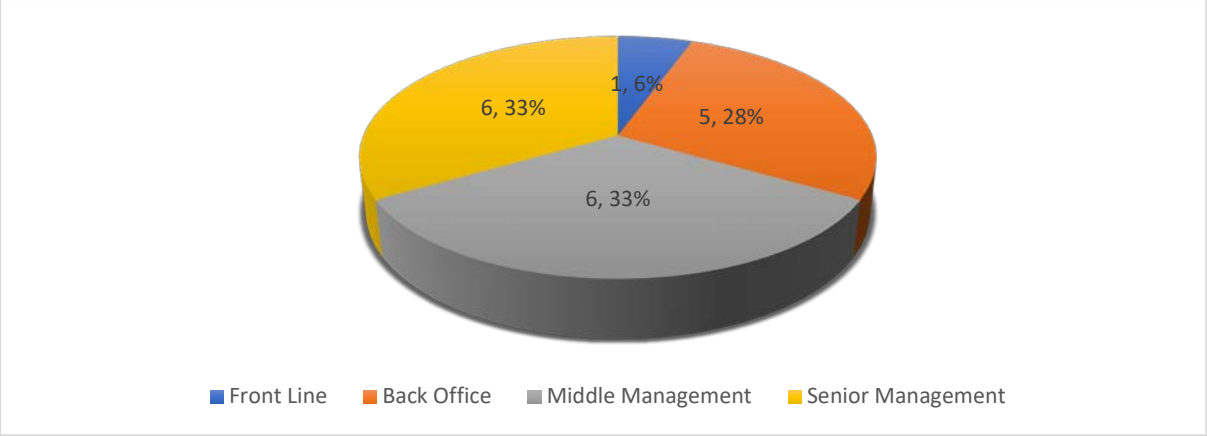
The above chart demonstrates the 4 Electronic Money and Payment institutions in Cyprus who positively accepted to participate to the research study. The authors have approach all of the EMIs and PIs institutions in Cyprus with a total of 12 operating organizations, 8 of them did not choose to participate due to confidentiality policy, reporting obligations, deadlines given by the regulator and restrictions of COVID-19 pandemic. Maybe in more normal times we would be able to have additional organizational participants. Regarding organization #4, I would like to mention that the researcher requested another 5 data collection surveys and the HR department of the company refused to give no more than already given 5 data collection surveys due to confidentiality policy of the institution. However, from organizations #1, #2 and #3 the author managed to collect full board of data collection surveys. The researcher observes from the chart above, the total number of participants are 50 employees from 4 organizations. From those, 18 employees are related to company #1 with a rate of 36% ,13 employees are related to company #2 with a rate of 26%, 14 employees are related to company #3 with a rate of 28% and 5 employees are related to company #4 with a rate of 10%.

Figure 10. Level of the Company's Hierarchy you Currently have

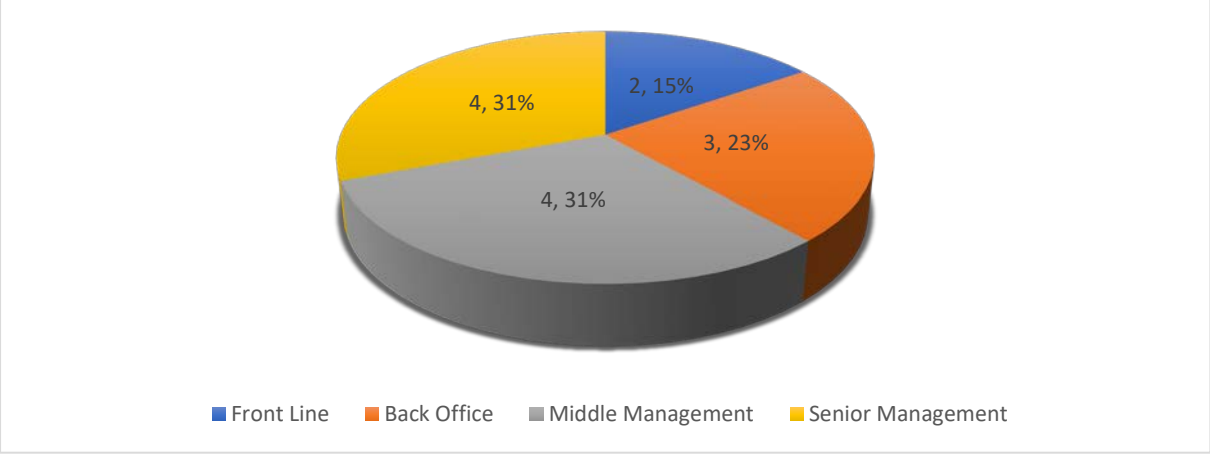


The above graph and chart demonstrate the level of the company's hierarchy employees currently have of total surveys it involves, 3 individuals from front line hierarchy and with a rate of 6%, 16 individuals from back-office hierarchy and with a rate of 32%, 12 individuals from middle management hierarchy and with a rate of 24%, 19 individuals from senior management hierarchy and with a rate of 38%. The total number of employees are 50 from 4 EMI and PI institutions in Cyprus. The researcher observes, the highest rate is concerning 19 employees with a rate of 38% from senior management level of hierarchy and the lowest employees is concerning 3 employees with a rate of 6% from front line level of hierarchy.

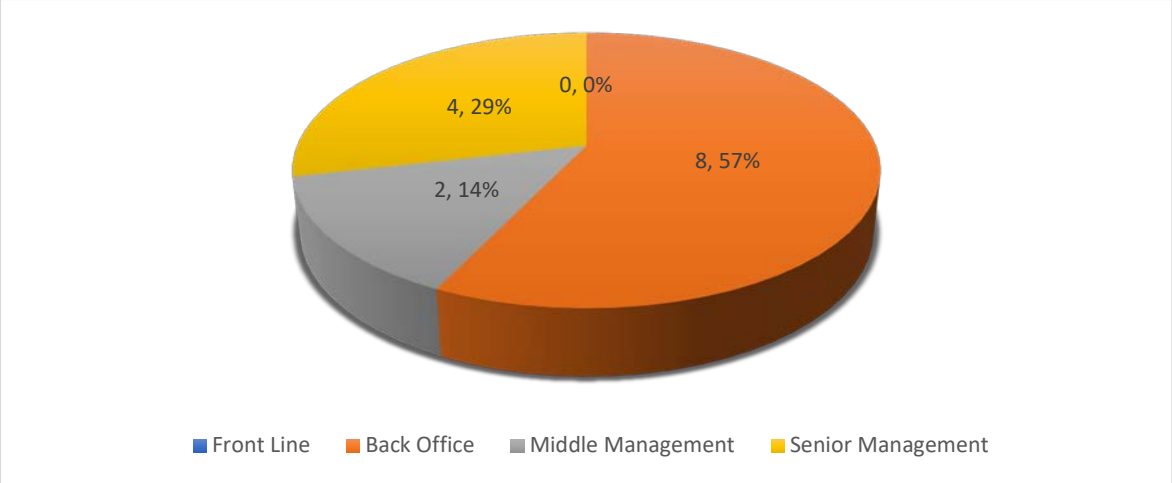
Company #1, the survey involved 1 employee from front line level of hierarchy and a rate of 6%, 5 employees from bank office level of hierarchy and a rate of 28%, 6 employees from middle management level of hierarchy and a rate of 33%, 6 employees from senior management level of hierarchy and a rate of 33%, The total number of employees are 18 from EMI and PI institution #1. We can observe that middle management and senior management have the same rate of 33% and the lowest level of hierarchy is front line with 6% rate.



Company #2, the survey involved 2 employees from front line level of hierarchy and a rate of 15%, 3 employees from bank office level of hierarchy and a rate of 23%, 4 employees from middle management level of hierarchy and a rate of 31%, 4 employees from senior management level of hierarchy and a rate of 31%, The total number of employees are 13 from EMI and PI institution #2. We can observe that middle management and senior management have the same rate of 31% and the lowest level of hierarchy is front line with 15% rate.



Company #3, the survey involved 0 employees from front line level of hierarchy and a rate of 0%, 8 employees from bank office level of hierarchy and a rate of 57%, 2 employees from middle management level of hierarchy and a rate of 14%, 4 employees from senior management level of hierarchy and a rate of 29%, The total number of employees are 14 from EMI and PI institution #3. We can observe that back office has the highest rate of 57% and the lowest level of hierarchy is front line with 0% rate.



Company #4, the survey involved 5 employees from senior management level of hierarchy only and a rate of 100%, The total number of employees are 5 from EMI and PI institution #4.

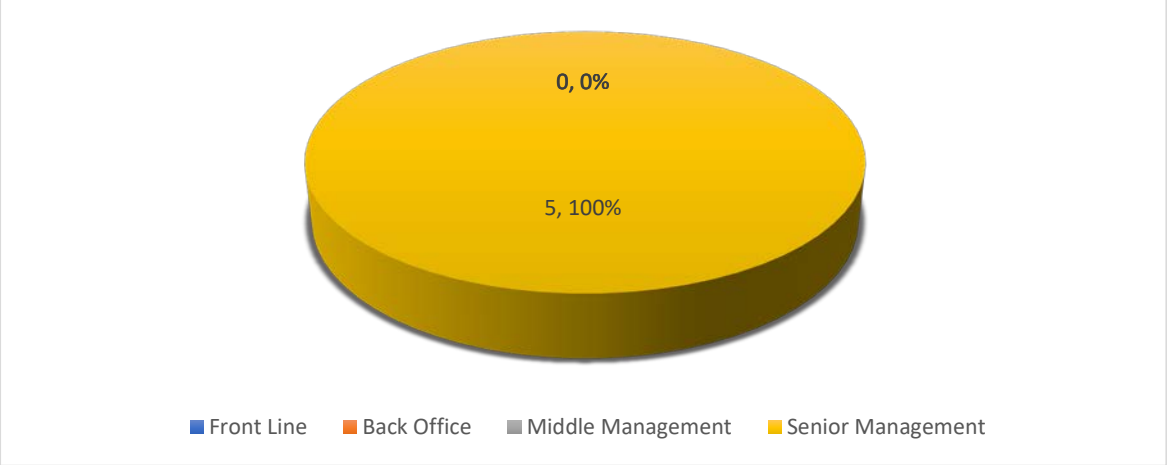
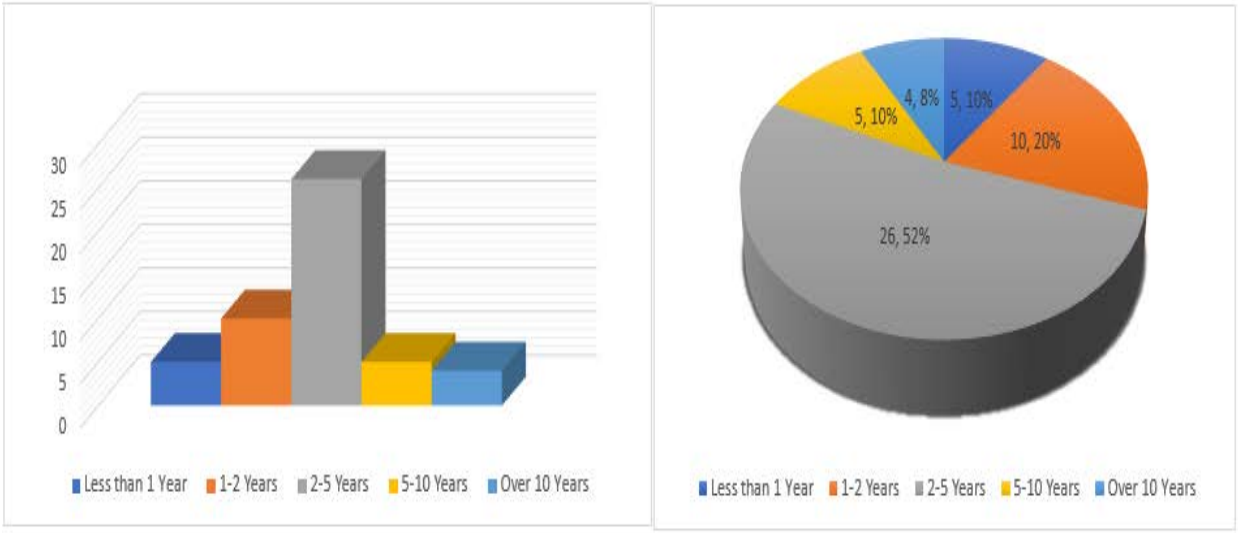
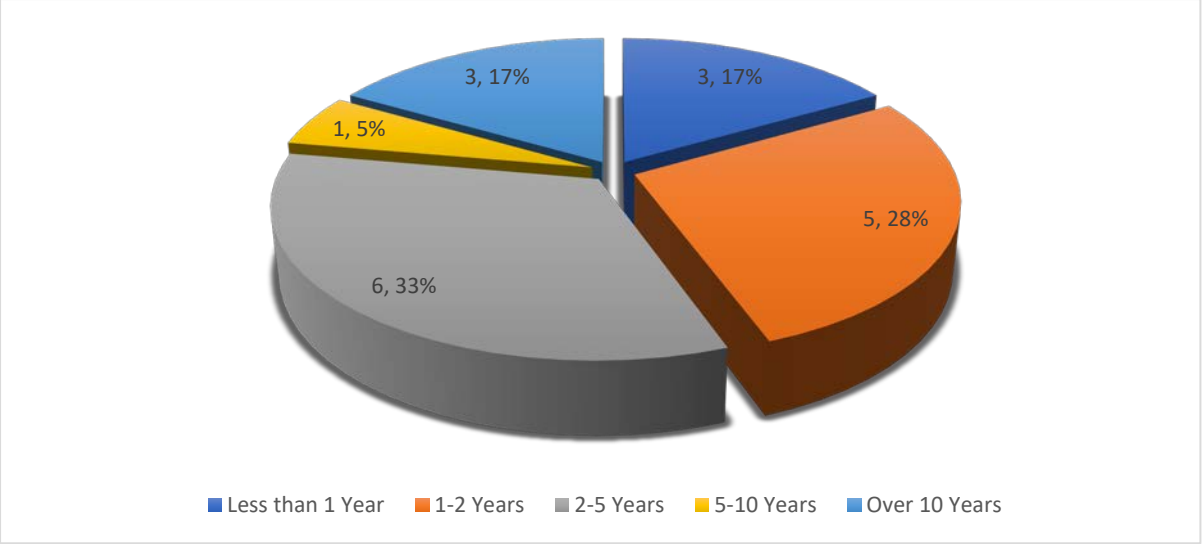


Figure 11. Work Experience in the Current Position

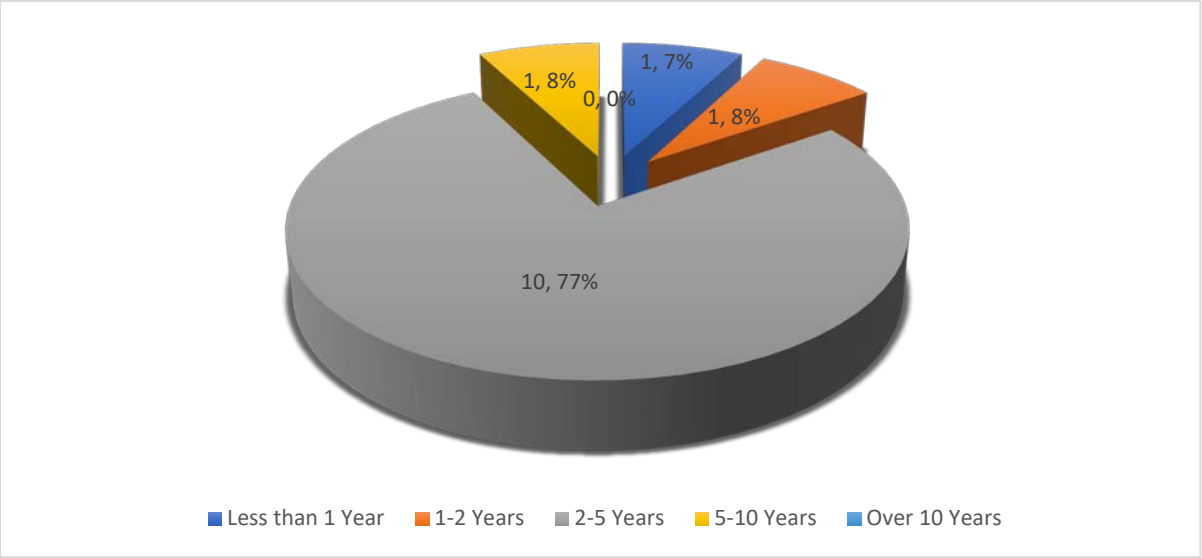


The above graph and chart demonstrate the level of the work experience in the current position of total surveys it involves, 5 individuals with less than 1 year of experience and with a rate of 10%, 10 individuals with 1-2 years of experience and with a rate of 20%, 26 individuals with 2-5 years of experience and with a rate of 52%, 5 individuals with 5-10 years of experience and with a rate of 10%, 4 individuals over 10 years of experience and with a rate of 8%. The total number of employees are 50 from 4 EMI and PI institutions in Cyprus. The researcher can observe that the highest rate is concerning years of experience between 2-5 years and with a rate of 52%. Electronic Money and Payments institutions are quite new in the financial institutions sector and more specifically in Cyprus. This companies started building their career within those years. However, we can clearly understand why we see this amount of amount of high response rate. (information retrieved from Central Bank of Cyprus)

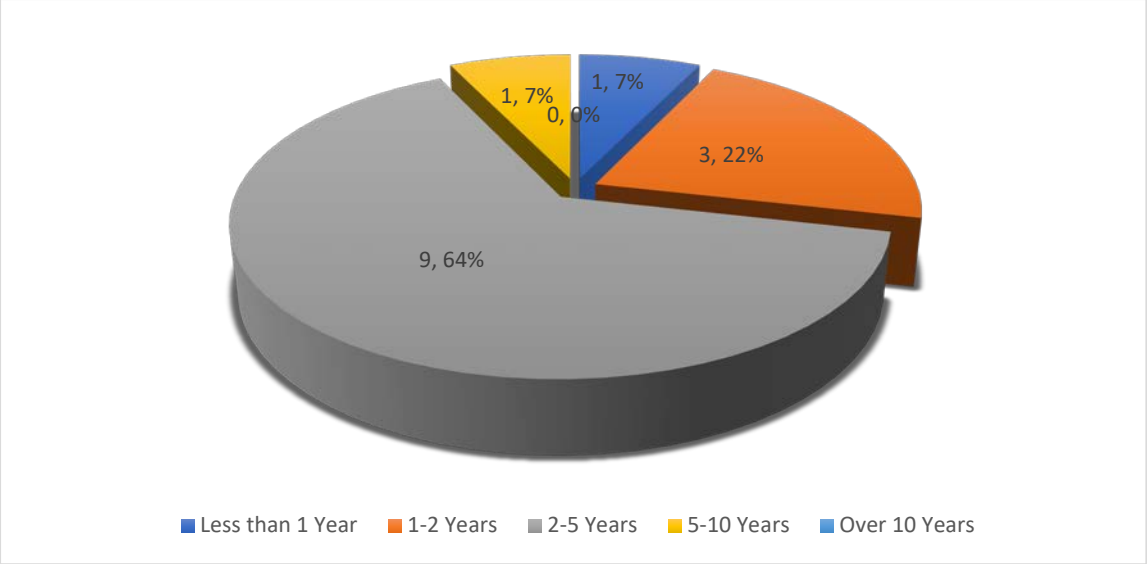
Company #1, the survey involved 3 individuals with less than 1 year of experience and with a rate of 17%, 5 individuals with 1-2 years of experience and with a rate of 28%, 6 individuals with 2-5 years of experience and with a rate of 33%, 1 individual with 5-10 years of experience and with a rate of 5%, 3 individuals with over 10 years of experience and with a rate of 17%. The total number of employees are 18 from institution #1.



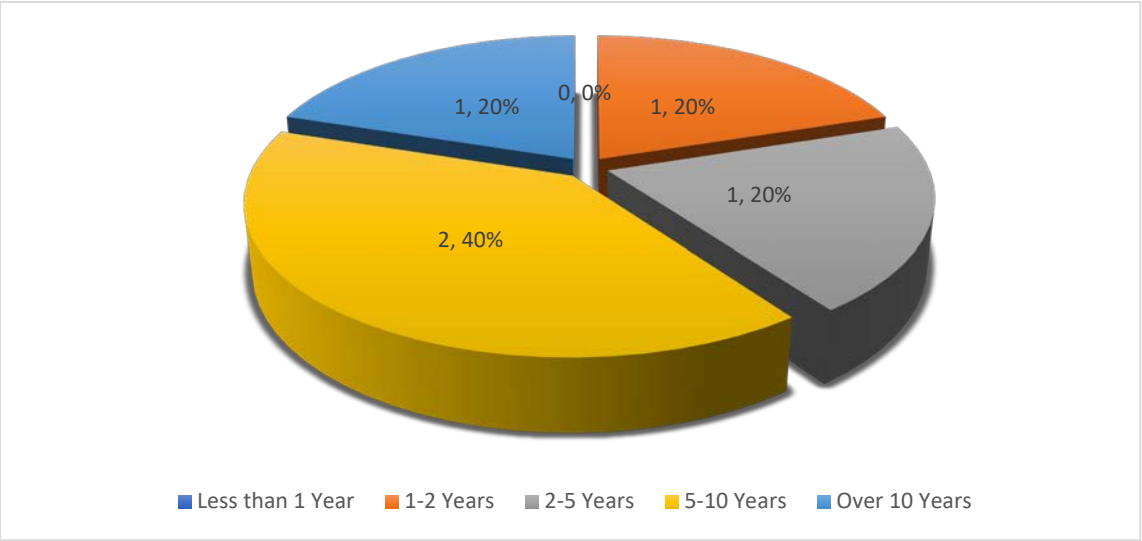
Company #2, the survey involved 1 individual with less than 1 year of experience and with a rate of 7%, 1 individual with 1-2 years of experience and with a rate of 8%, 10 individuals with 2-5 years of experience and with a rate of 77%, 1 individual with 5-10 years of experience and with a rate of 8%, 0 individuals with over 10 years of experience and with a rate of 0%. The total number of employees are 13 from institution #2.



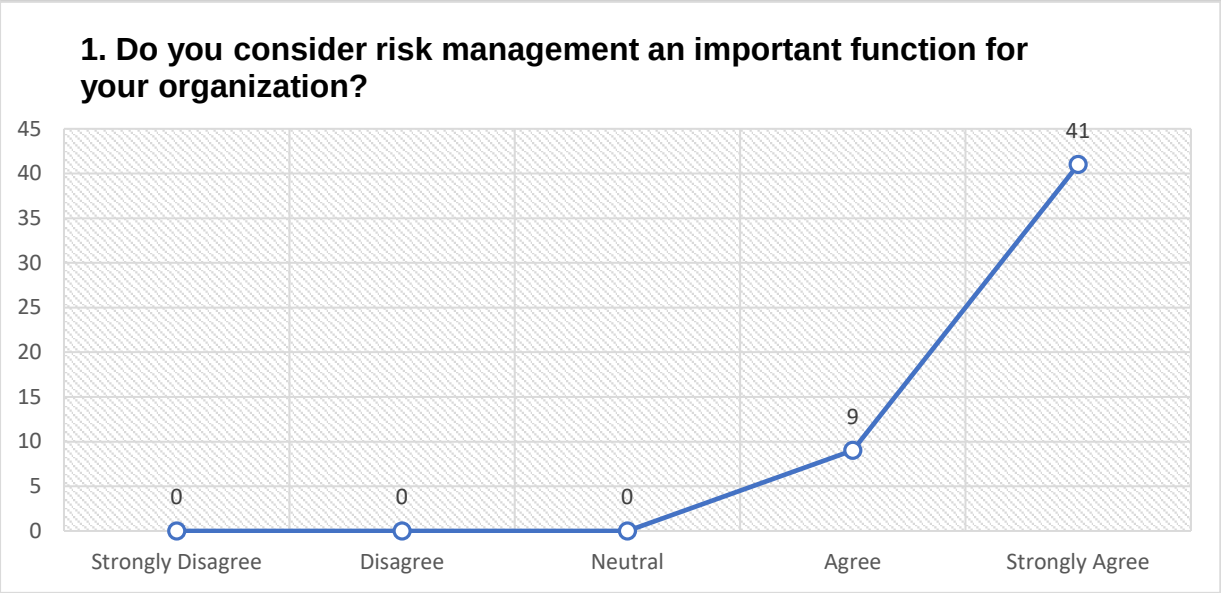
Company #3, the survey involved 1 individual with less than 1 year of experience and with a rate of 7%, 3 individuals with 1-2 years of experience and with a rate of 22%, 9 individuals with 2-5 years of experience and with a rate of 64%, 1 individual with 5-10 years of experience and with a rate of 7%, 0 individuals with over 10 years of experience and with a rate of 0%. The total number of employees are 14 from institution #3.

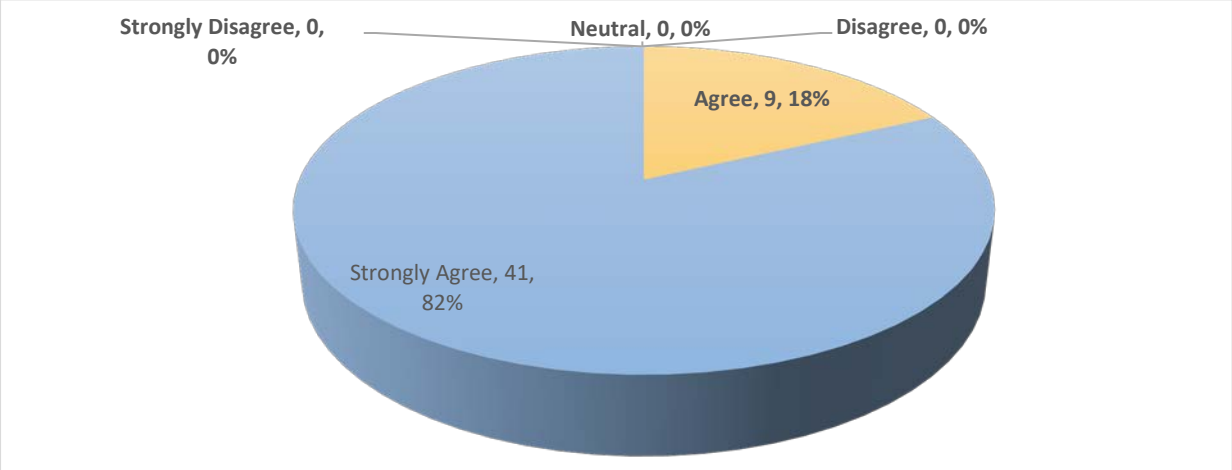


Company #4, the survey involved 0 individual with less than 1 year of experience and with a rate of 0%, 1 individual with 1-2 years of experience and with a rate of 20%, 1 individual with 2-5 years of experience and with a rate of 20%, 2 individuals with 5-10 years of experience and with a rate of 40%, 1 individual with over 10 years of experience and with a rate of 20%. The total number of employees are 5 from institution #4.



4.2 Data Collection Survey Analysis



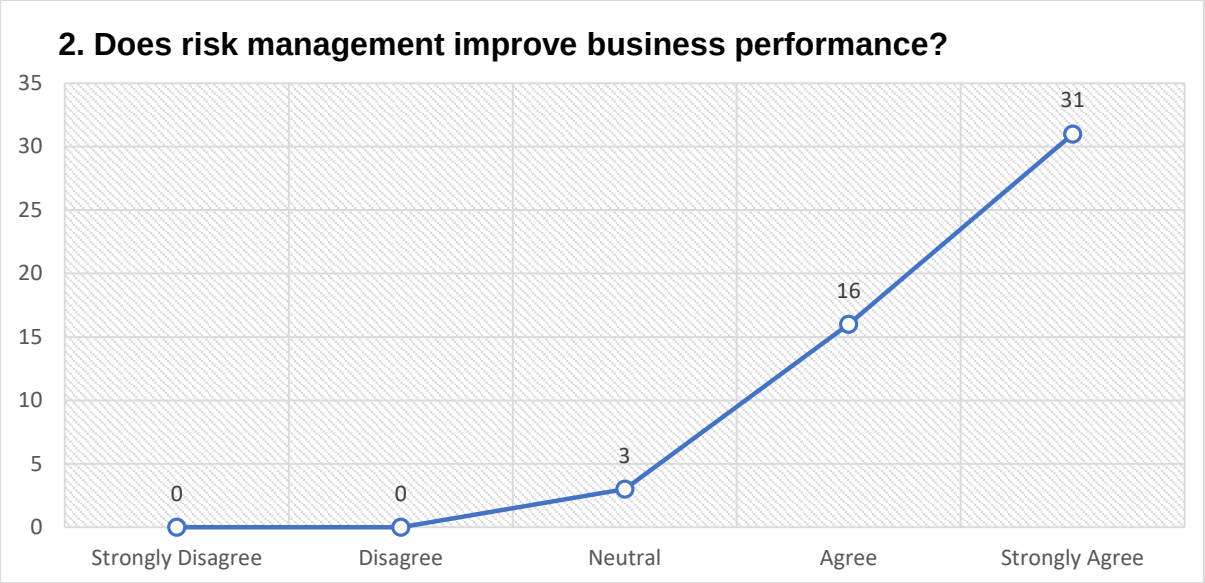


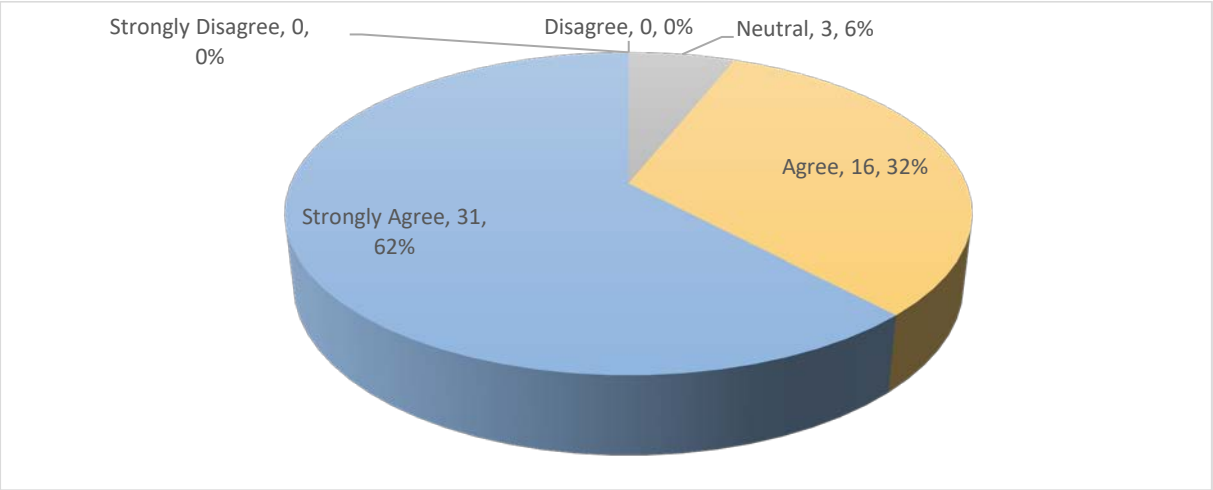
The above graph and chart demonstrate the question of total surveys: Do you consider risk management an important function for your organization? Agree: it involves 9 individuals with a rate of 18% and Strongly Agree: it involves 41 individuals with a rate of 82%. Strongly Disagree, Disagree and Neural: it involves 0 individuals with a rate of 0%. The total number of employees are 50 from 4 EMI and PI institutions in Cyprus.

According to the researcher findings we can observe that electronic money and payment institutions either agree or strongly agree to the question do you consider risk management an important function of your organization. The highest response was Strongly Agree with a rate of 82%. From this question the author was able to get the general idea from each employee and how do they approach risk management. Following the responses, the researcher obtain from interview question 9, and according to

interviewing individuals #1, and #3 the author observe that risk management in a crucial and important department within the institutions. According to interviewing individual #1 Yes, risk management played an important role since it helped to overcome the crisis while implementing a scenario on how to deal with the pandemic. According to interviewing individual #3, Risk management is crucial and an essential department with the organization but also the setup of the company helped to overcome the virus.

As stated by Aven (2010: 1) The purpose of risk management is to safeguard that satisfactory measures have been taken to safeguard the individuals and assets from potential and harmful consequences of the activities being undertaken, as well as to balance various anxieties, more specifically risks and costs. Risk management includes actions equally to prevent risk exposures and to decrease their potential harm to the institution itself.

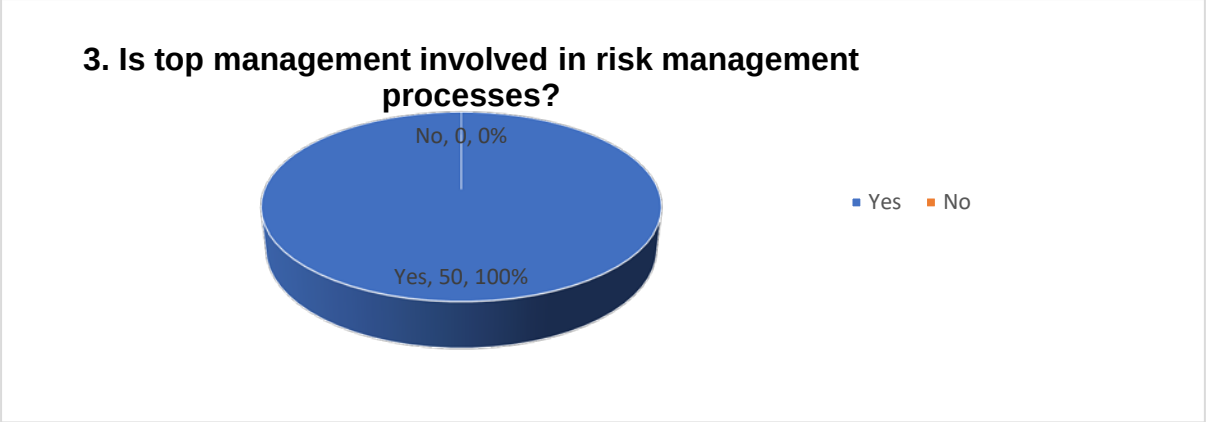




The above graph and chart demonstrate the question of total surveys: Does risk management improve business performance? Neutral: it involves 3 individuals with a rate of 6%, Agree: it involves 16 individuals with a rate of 32% and Strongly Agree: it involves 31 individuals with a rate of 62%. Strongly Disagree and Disagree it involves: 0 individuals with a rate of 0%. The total number of employees are 50 from 4 EMI and PI institutions in Cyprus.

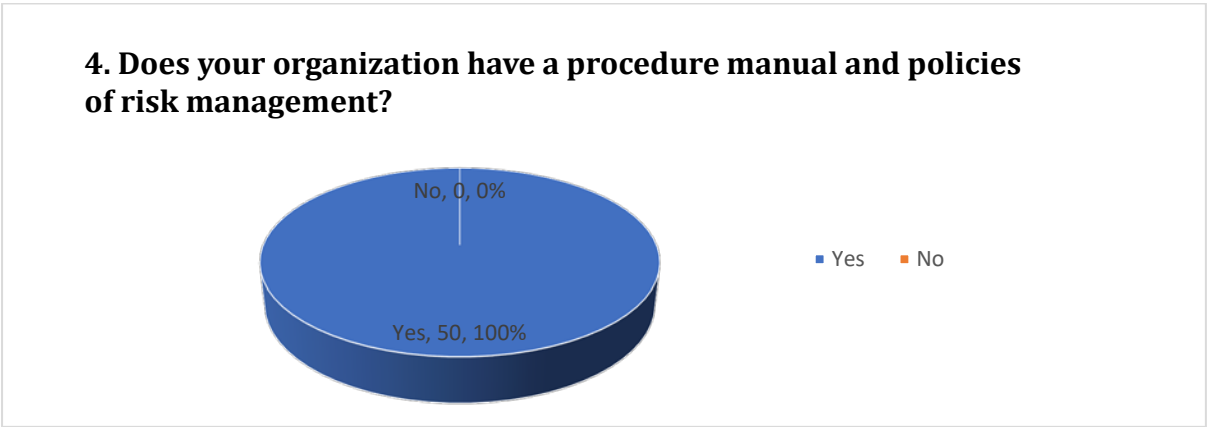
According to the researcher findings we can observe that electronic money and payment institutions either mostly strongly agree or either agree and a minority neutral to the question does risk management improve business performance. The highest response was Strongly Agree with a rate of 62%. From this question the author was able to obtain the approach by each employee and to understand if risk management improves business performance according to employee believes, awareness and expertise. Following the responses, the researcher obtain from interview question 9, and according to interviewing individuals #1, #2, #3 and #4 the author observe that they positively agree if risk management helped their organization to overcome the covid 19 pandemic event.

Risk management provides to the board and senior management a concise summary of potential risk that might be faced by the institution with the purpose of improving and/or preventing them. Risks are hypothetical obstacles. “For example, every time we cross the street, we run the risk of being hit by a car. The risk does not start until we make the commitment, until we step in the street. It ends when the problem occurs (the car hits us) or the possibility of risk is eliminated i.e., we safely step onto the sidewalk of the other side of the street” (Westfall, 2001).



The above chart demonstrates the question of total surveys: Is top management involved in risk management process? Yes, it involves 50 individuals with a rate of 100%, The total number of employees are 50 from 4 EMI and PI institutions in Cyprus. According to the researcher findings we can observe that electronic money and payment institutions top management is involved in risk management process.

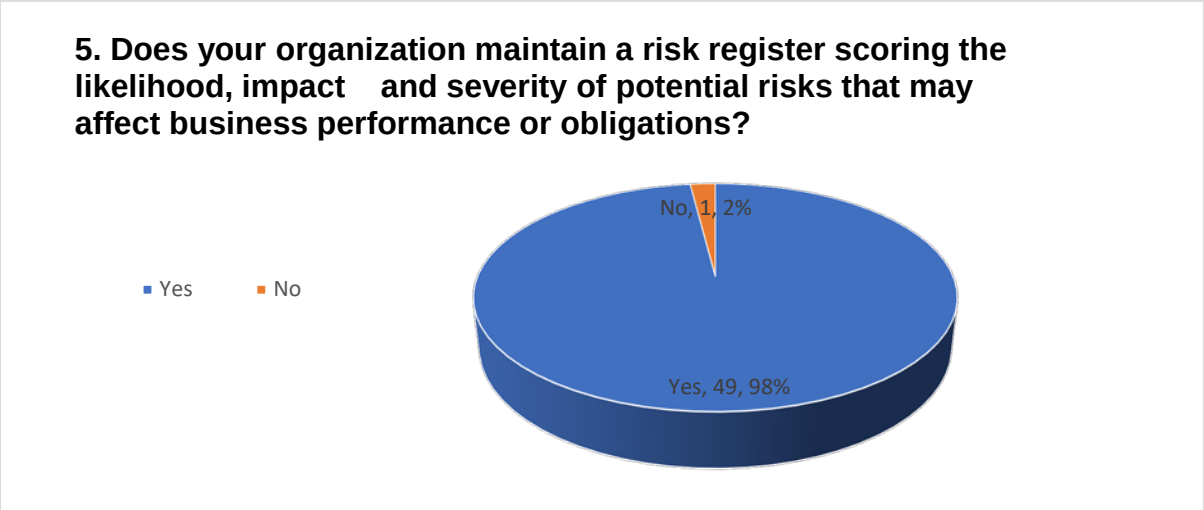
Following the responses, the researcher retrieves from interview question 3, and according to interviewing individuals #2 and #4 the author observe that the management risk committee is acting as the governance and control committee of the company. Risk Committee also ensures the appropriate and effective implementation of controls. In case of deficiencies the Risk Manager has the obligation to review, challenge and/or recommend on how to minimize or reduce those risks while reporting to the Board of Directors. The Board of Directors has the overall responsibility for ensuring an effective risk management.



The above chart demonstrates the question of total surveys: Does your organization have a procedure manual and policies of risk management? Yes, it involves 50 individuals with

a rate of 100%, The total number of employees are 50 from 4 EMI and PI institutions in Cyprus.

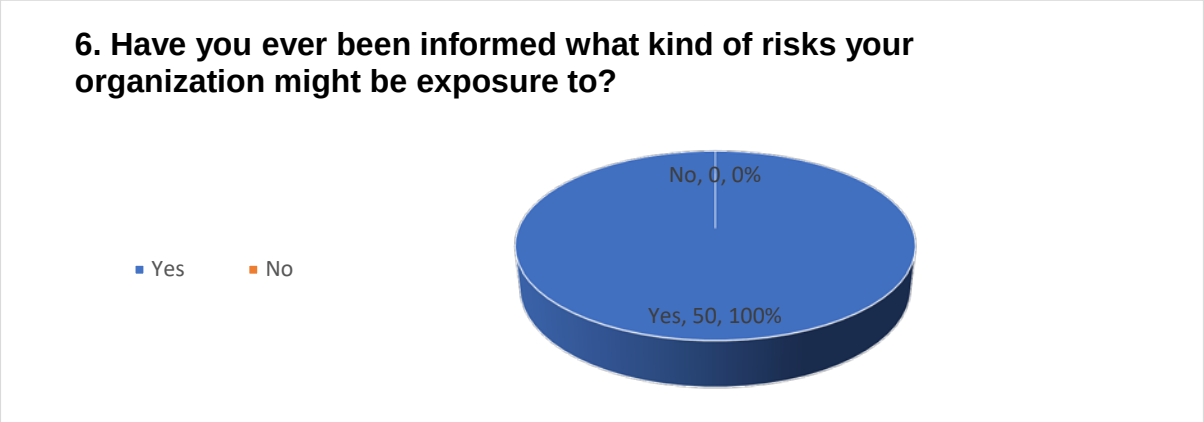
According to the researcher findings we can observe that electronic money and payment institutions have procedure manual and policies of risk management. Following the responses, the researcher retrieves from interview question 1, and according to interviewing individuals #1, #2, #3 and #4 the author can positively say that electronic money and payments institutions have procedure manual and policies of risk management since is a mandatory requirement set by the regulator Central Bank of Cyprus. The institutions are constantly working on enhancing risk procedures to reach the maximum level of safeguarding. Risk management manual provides an overview of the risk management process and a practical guidance for the supervision of risks within departments and teams, to decrease the frequency of incidents and to reduce impact of incidents if they occur. Risk management policy is to provide guidance regarding the management of risk, to support the accomplishment of business objectives, safeguard employees and business assets while ensure financial sustainability.



The above chart demonstrates the question of total surveys: Does your organization maintain a risk register scoring the likelihood, impact and severity of potential risks that may affect business performance or obligations? Yes, it involves 49 individuals with a rate of 98%. No, it involves 1 individual with a rate of 2%. The total number of employees are 50 from 4 EMI and PI institutions in Cyprus.

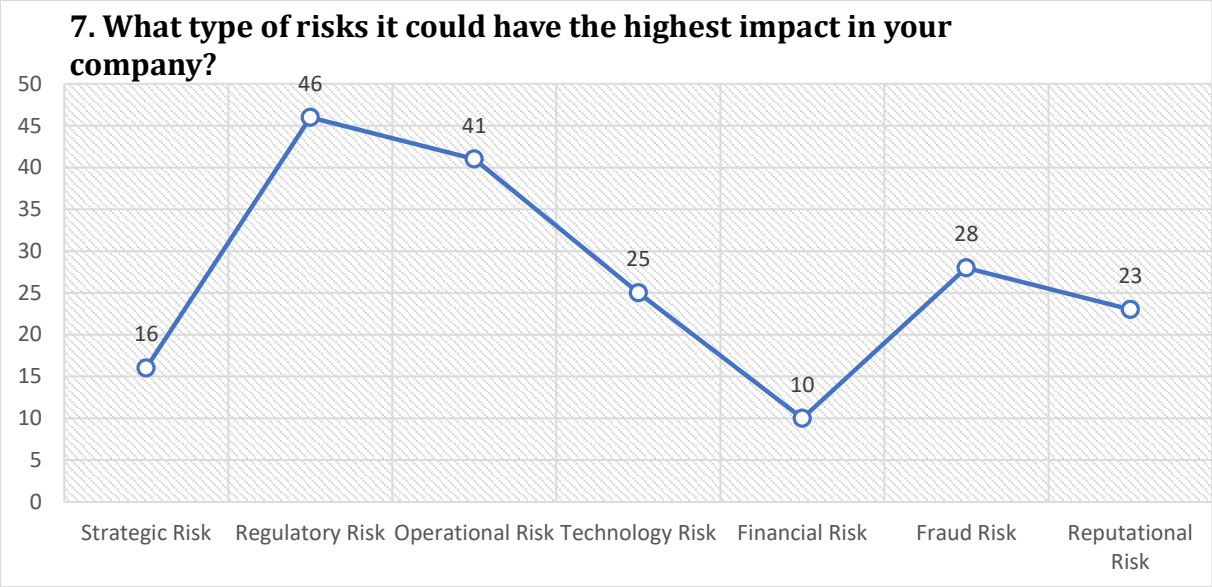
In line with the researcher findings, we can observe that electronic money and payment institutions maintain a risk register of risk management. Following the responses, the

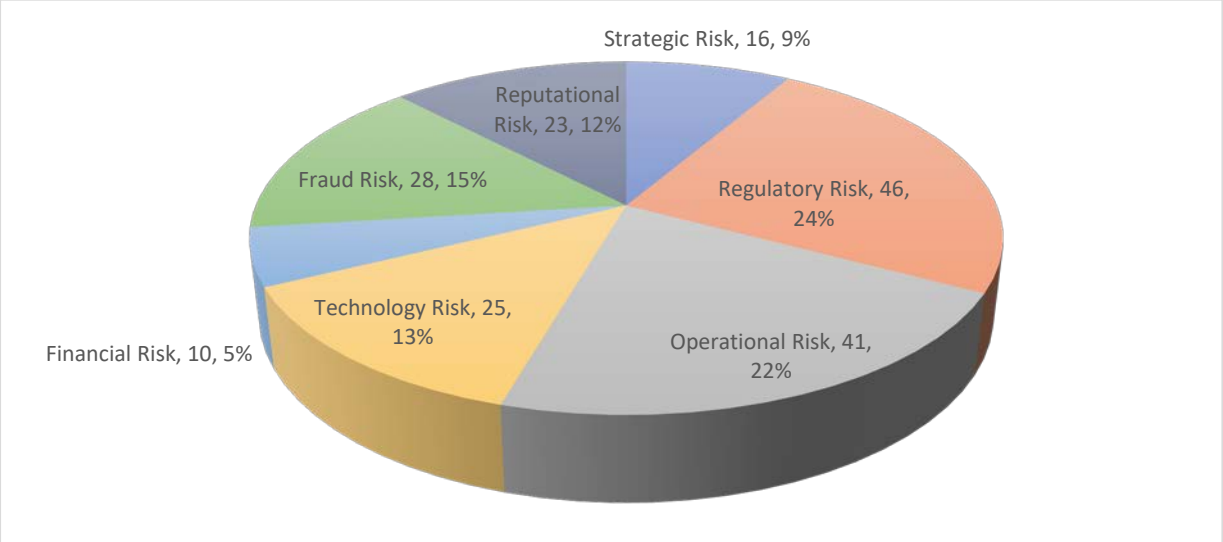
researcher retrieve from interview question 5 of all individuals #1, #2,#3 and #4 the institutions maintain a risk register. Risk registers as already explain at interview question 5, is a tool used to manage risks in order to comply with regulatory acts as repository of all identified risks based on the guidelines published by the "EBA" European Baking Authority or "CBC" Central Bank of Cyprus and obligations stemming out of PSD2. The researcher can estimate that negative response was added accidentally by 1 individual with a rate of 2%.



The above chart demonstrates the question of total surveys: Have you ever been informed what kind of risks your organization might be exposure to? Yes, it involves 50 individuals with a rate of 100%. No, it involves 0 individual with a rate of 0%. The total number of employees are 50 from 4 EMI and PI institutions in Cyprus.

Following the responses, the researcher retrieve from interview question 2 of all individuals #1, #2, #3 and #4 and according to the below survey Q.7 The researcher is able to obtain a result that will be performed and explained below. (survey Q.7)





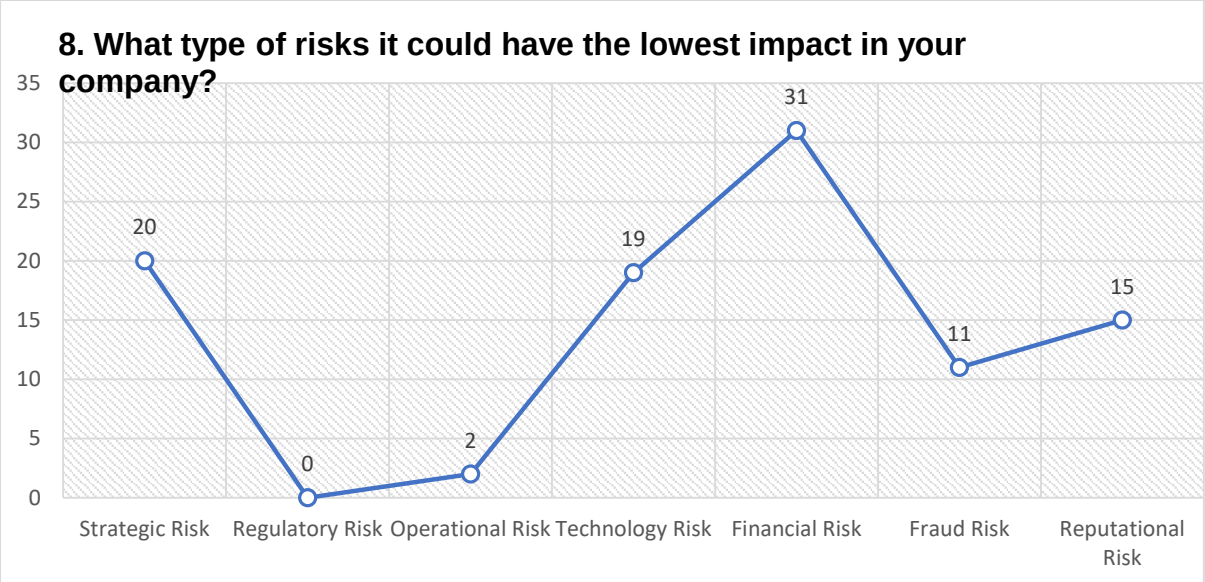
The above graph and chart demonstrate one of the authors main question of total surveys: What type of risks it could have the highest impact in your company? Strategic risk, it involves 16 individuals with a rate of 9%. Regulatory risk, it involves 46 individuals with a rate of 24%. Operational risk, it involves 41 individuals with a rate of 22%. Technology risk, it involves 25 individuals with a rate of 13%. Financial risk, it involves 10 individuals with a rate of 5%. Fraud risk, it involves 28 individuals with a rate of 15%. Reputational risk, it involves 23 individuals with a rate of 12%. The total number of employees are 50 from 4 EMI and PI institutions in Cyprus.

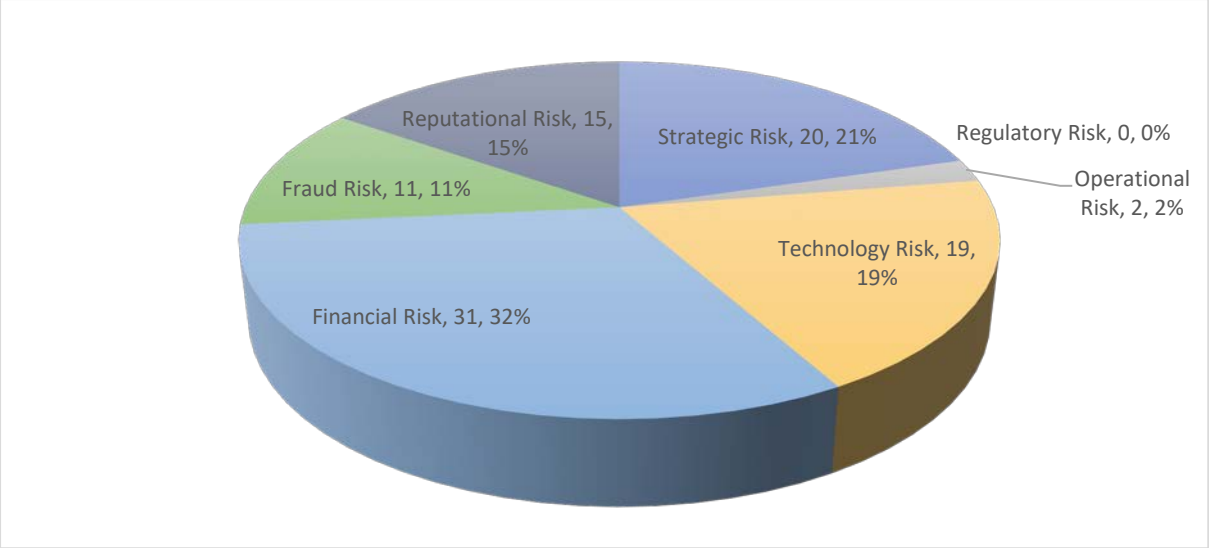
The researcher can observe that the highest risks of 4 EMI and PI institutions are Regulatory risk with a rate of 24%, Operational risk with a rate of 22%, Fraud risk with a

rate of 15% and Technology risk with a rate of 13%. The lowest according to the above graph is the financial risk with a rate of 5%.

Regulatory risk is the risk that a variation in laws and regulations will significantly influence the business of the company . The complaint unit has procedures for monitoring European and National legislation, it also identifies changes and informs affected parties to implement the new requirements. In addition, the complaint unit should maintain a register with the new legislation in force. Where it is deemed necessary legal consultation is seeking.

Operational risk, as stated by Central bank of Kenya, is the threat of failure resulting from insufficient or failed internal processes, individuals and systems or from exterior incidents. The key objective of an EMI organization is the Operational Risk Management Framework (ORMF) is to identify, assess, monitor and report the risks to which the organization may be exposed currently or potentially. To be efficient, it is essential for the framework to be solid, regularly applied and unified with business practices if it is to be defined as "embedded". The objective is to achieve a fully unified and embedded ORMF that will create advantages to the institution in economic and non-economic conditions. It must also offer a strong foundation for proving the importance of operational risk management activity (The institute of Operational Risk, 2020)





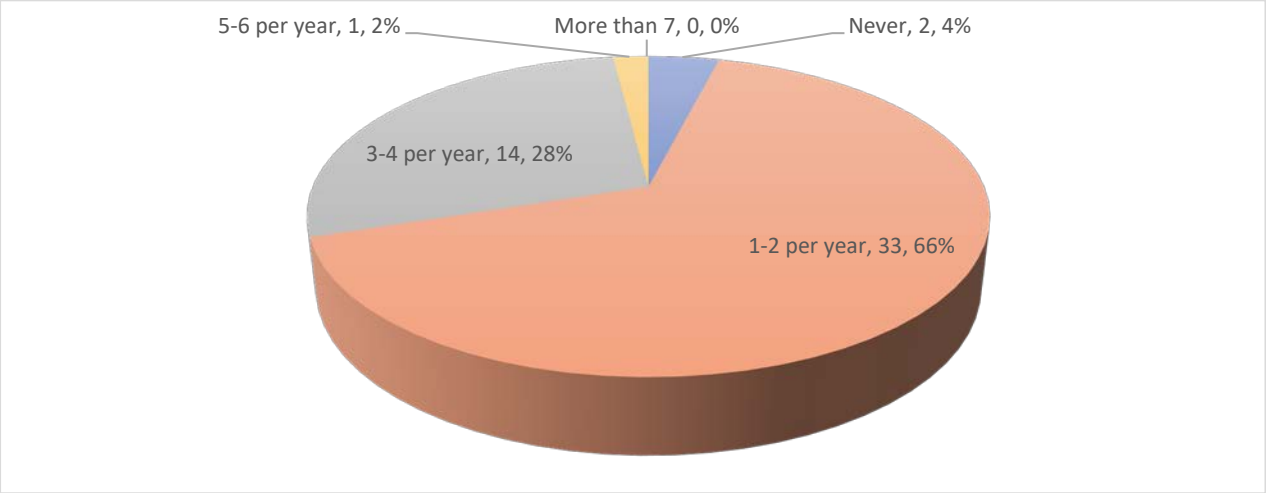
The above graph and chart demonstrate the question of total surveys: What type of risks it could have the lowest impact in your company? Strategic risk, it involves 20 individuals with a rate of 21%. Regulatory risk, it involves 0 individuals with a rate of 0%. Operational risk, it involves 2 individuals with a rate of 2%. Technology risk, it involves 19 individuals with a rate of 19%. Financial risk, it involves 31 individuals with a rate of 32%. Fraud risk, it involves 11 individuals with a rate of 11%. Reputational risk, it involves 15 individuals with a rate of 15%. The total number of employees are 50 from 4 EMI and PI institutions in Cyprus.

The researcher can observe that the lowest risks of 4 EMI and PI institutions are financial risk with a rate of 32% and strategic risk with a rate of 21%. The highest risks are regulatory with a rate of 0% and operational risk with a rate of 2%.

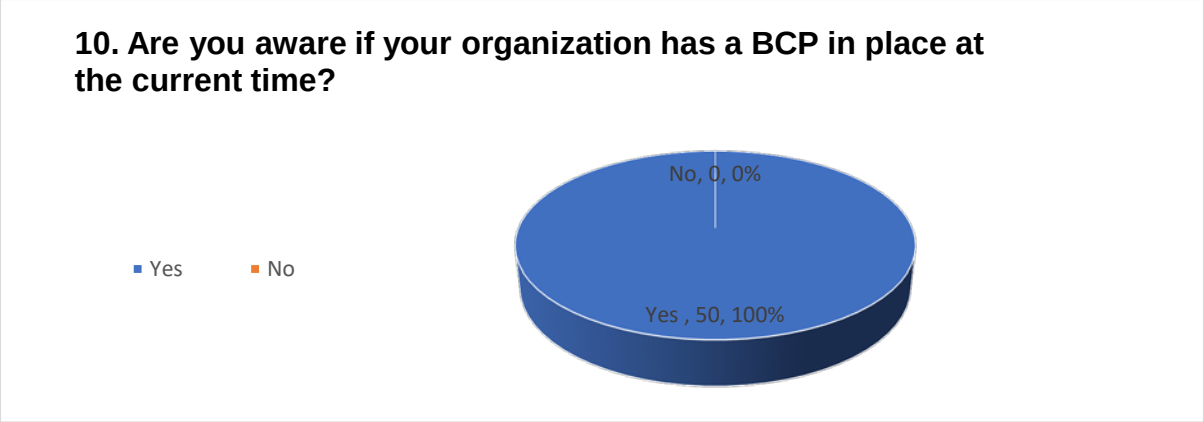
Financial risk is relating to fraud and other types of financial crime. Jointly with settlement risk, this is the highest area of concern having both financial and reputation risks associated with it. The policy objective should maintain the maximum resource to fully mitigate this risk. Avoid markets and products prone to high levels of risk.

Strategic risk is the risk that might cause to a corporation by unsuccessful business choices or lack therefrom. Strategic risk is usually a major factor in determining company's value, notably noticeable if the corporate experiences a pointy decline in a very short amount of your time. Quarterly meetings with the Board of Directors of the electronic money & payment institution and discuss issues relating to the competitive

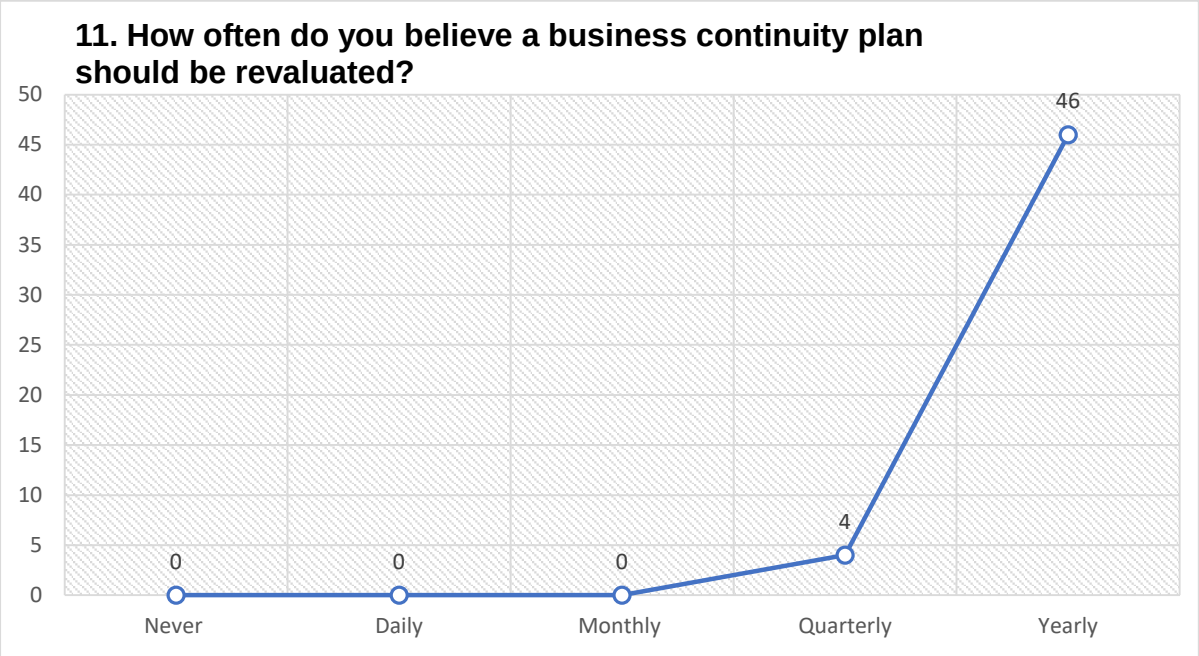
advantage of organization competition and opportunities the company can seek. Clients' retention is an essential element of the company's business to prevent any material losses.

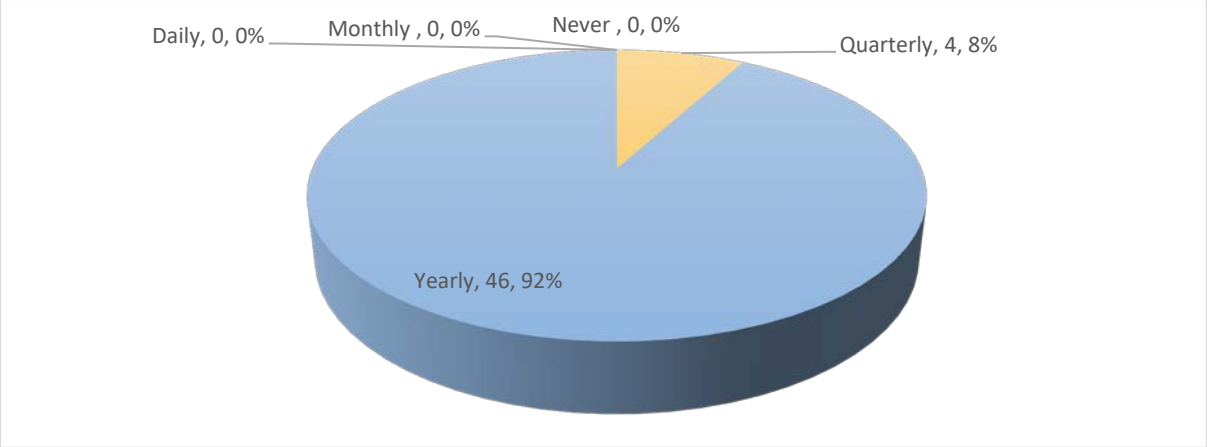


The above graph and chart demonstrate the question of total surveys: How often do you take trainings internal or external regarding issues of risk management? 1-2 per year, it involves the highest response of 33 individuals with a rate of 66%. 3-4 per year, it involves response of 14 individual's ith a rate of 28%. The researcher is able observe that the institutions with 96% rate are focusing on the performance and proficiency of employees as it has been proven by the above findings. The beautiful thing about learning is nobody can take it away from you as stated by B. B. King.

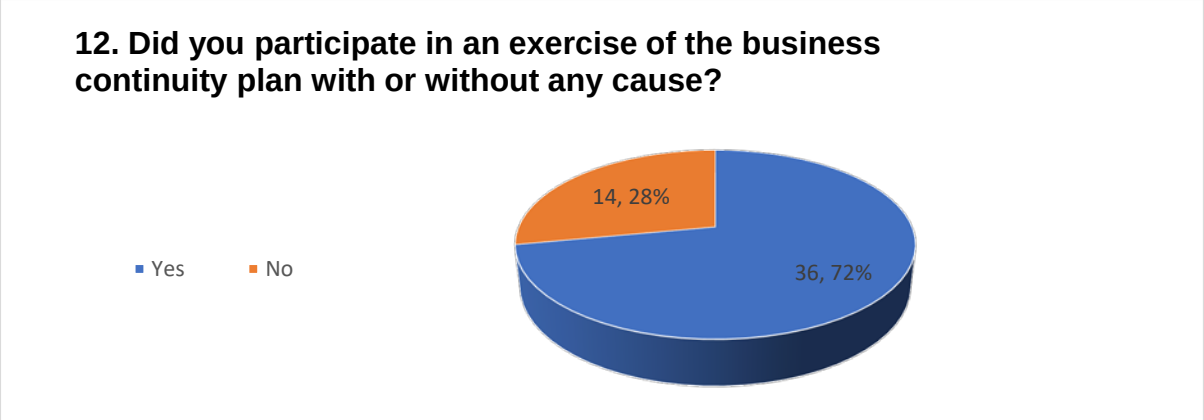


The above chart demonstrates the question of total surveys: Are you aware if your organization has a BCP in place at the current time? Yes, it involves the highest response of 50 individuals with a rate of 100%. No, it involves response with a rate of 0%. Following the responses, the researcher retrieve from interview question 6 of all individuals #1, #2,#3 and #4 and according to the above survey, the researcher is able to observe that all institutions since is part of regulatory obligations stemming out of PSD2.



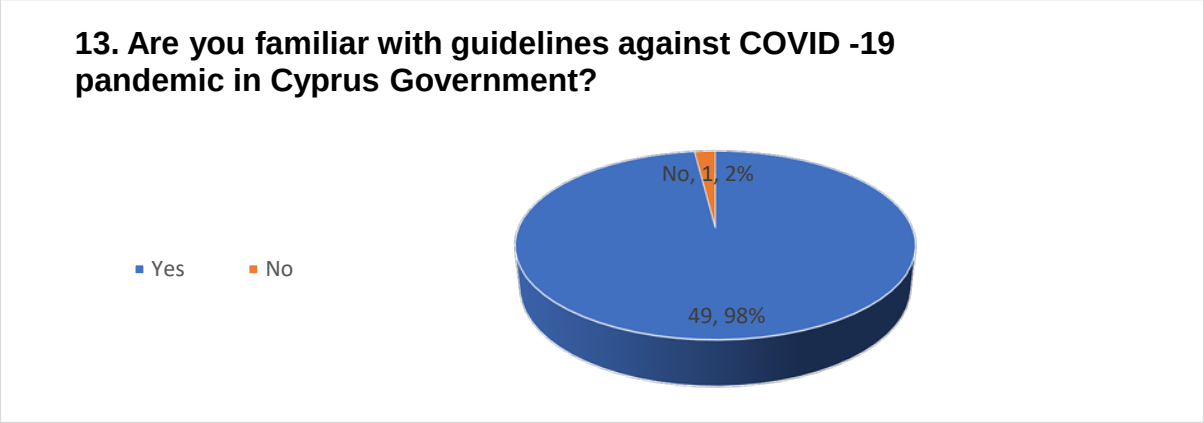


The above graph and chart demonstrate the question of total surveys: How often do you believe a business continuity plan should be revaluated? Yearly, it involves the highest response of 46 individuals with a rate of 92%., Quarterly, it involves the response of 4 individuals with a rate of 8%. Following the responses, the researcher retrieve from interview question 6 of all individuals #1, #2,#3 and #4 and according to the above survey, the researcher is able to observe that a business continuity plan should be re-evaluated at least once per year and/ or whenever there is a need throughout a year.

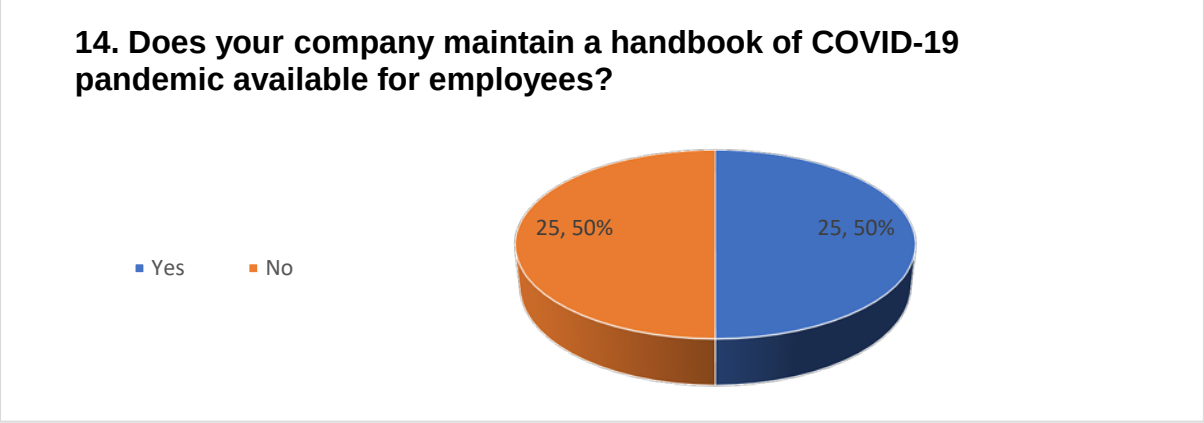


The above chart demonstrates the question of total surveys: Did you participate in an exercise of the business continuity plan with or without any cause? Yes, it involves the response of 36 individuals with a rate of 72%. No, it involves the response of 14 individuals with a rate of 28%. Following the responses, the researcher retrieve from interview question 6 of all individuals #1, #2, #3 and #4 and according to the above survey, the researcher is able to observe that participation of business continuity plan is enhancing systems used by the company and it proven to be important for the successful management of several crisis events. The institution makes sure that all employees understand their responsibilities in case of an emerged scenario or a disruption of normal

operations. should be reevaluated at least once per year and whenever there is a need throughout a year.

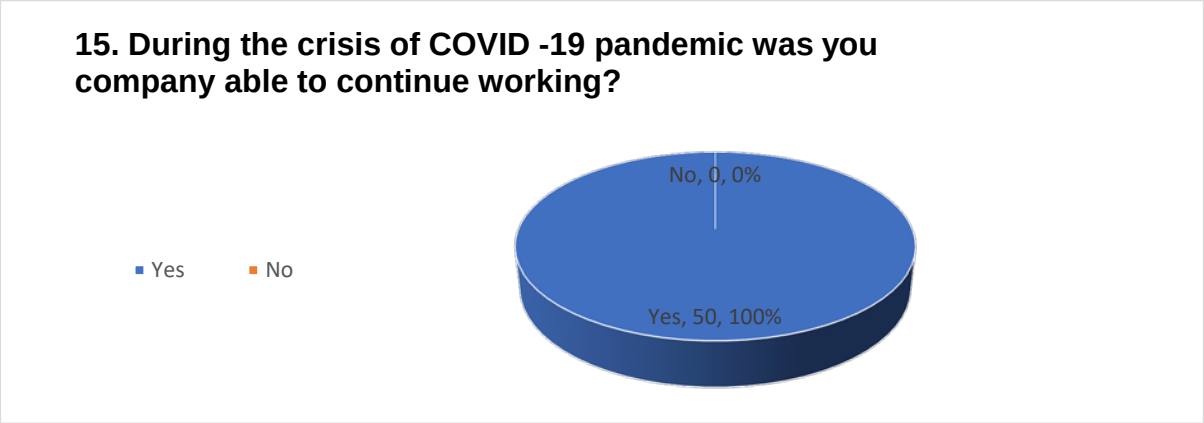


The above chart demonstrates the question of total surveys: Are you familiar with guidelines against COVID -19 pandemic in Cyprus Government? Yes, it involves the highest response of 49 individuals with a rate of 98%. No, it involves the response of 1 individual with a rate of 2%. The researcher is able to observe that the rate of 2%. responded was probably by a human error, it has been 1 year the guideline against the pandemic are available on publicity information resources e.g., news, newspapers and TV announcements.

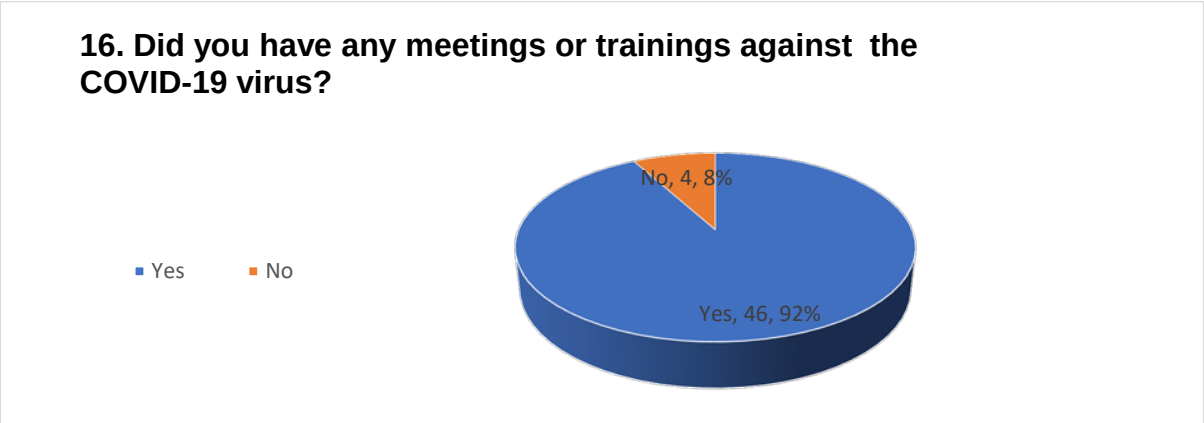


The above chart demonstrates the question of total surveys: Does your company maintain a handbook of COVID-19 pandemic available for employees? Yes, it involves the highest response of 25 individuals with a rate of 50%. No, it involves the response of 25 individual with a rate of 50%. Following the responses, the researcher retrieve from interview question 7 of individuals #2, #3 and #4 and according to the above survey, the researcher is able to argue if the mentioned institutions have a handbook of COVID-19 pandemic since during the collection the researcher received negative replies. Interviewing

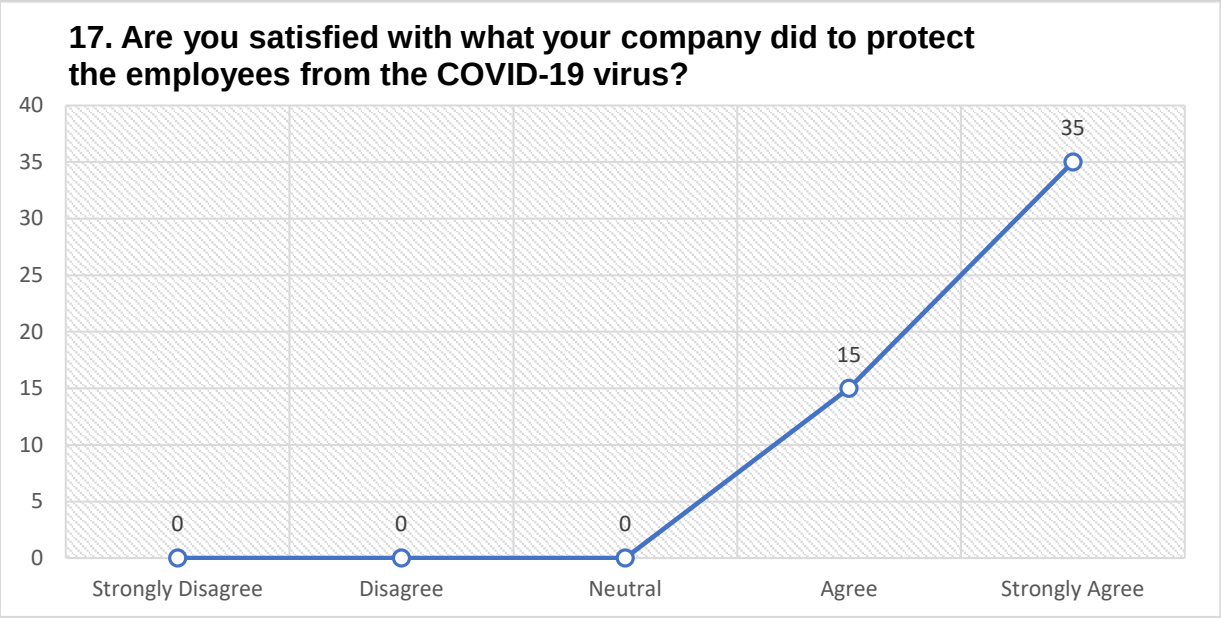
individual #1 only answer positively to the questions. The researcher would say that Yes, it should involve 18 individuals with a rate of 36% and a rate of 50%. Results of the above questions case due to human error probably because of press information office website: https://www.pio.gov.cy/coronavirus/ it looks like the Cy Government prepared a manual against the pandemic and this may confuse the participants.

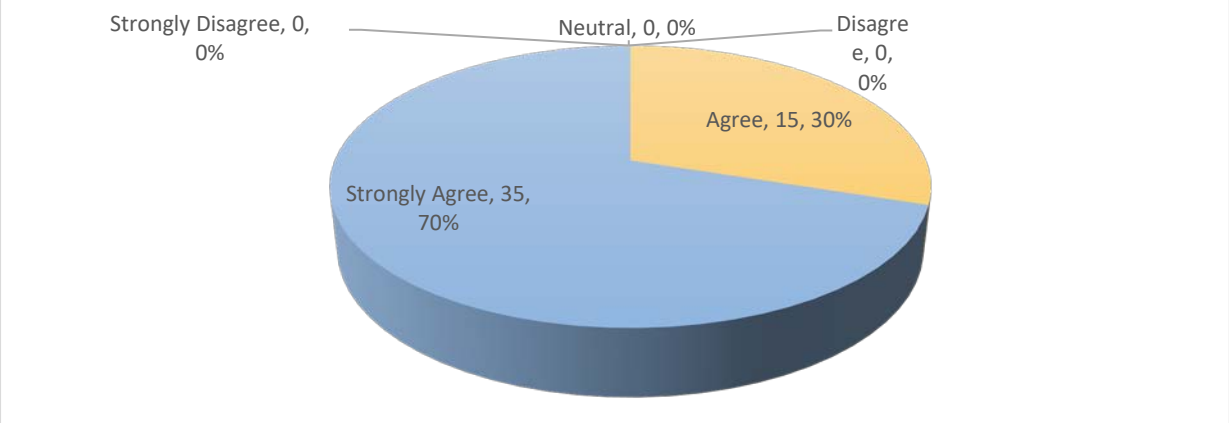


The above chart demonstrates the question of total surveys: During the crisis of COVID -19 pandemic was you company able to continue working? Yes, it involves the responses of 50 individuals with a rate of 100%. Following the responses, the researcher retrieve from interview question 7 of all individuals #1, #2,#3 and #4 and according to the above survey, the researcher is able to observe that electronic money and payments institutions were able to continue uninterrupted and the management took various meetings to access the situation based on each announcement made by the government while implementing the social distancing by using web technologies to communicate and providing support. The fact that EMI and PIs are FinTech entities and the use technology to provide financial services to businesses or consumers also helped the continuation of normal operational activities.

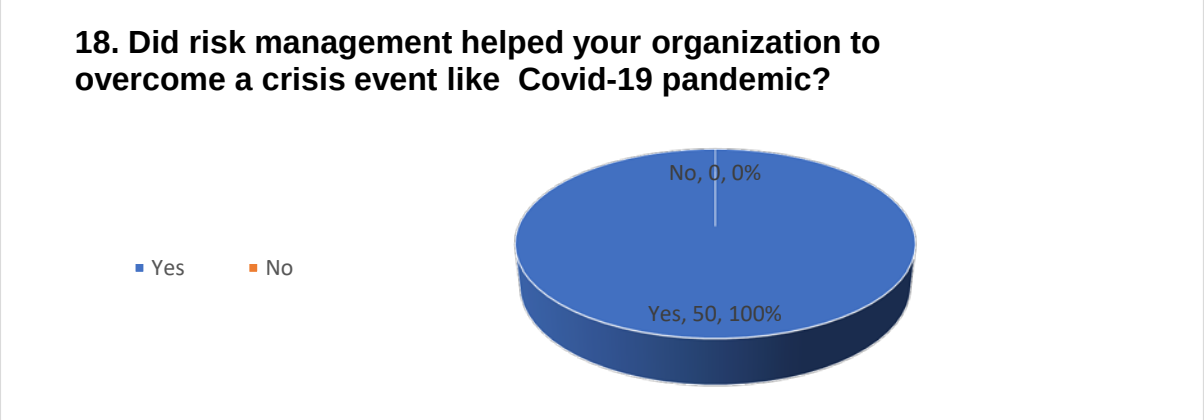


The above chart demonstrates the question of total surveys: Did you have any meetings or trainings against the COVID-19 virus? Yes, it involves the responses of 46 individuals with a rate of 92%. No, it involves the responses of 4 individuals with a rate of 8%. Following the responses, the researcher retrieve from interview question 7 of all individuals #1, #2, #3 and according to the above survey, the researcher is able to observe that electronic money and payments institutions took several meetings. According to interviewing individual #1, Various meetings were taken place while implementing the social distancing against the virus. According to interviewing individual #2, the management took regular meetings to assess the situation based on each announcement made by the Cy government. According to individual #3, Against the virus, the organization had two meetings for issues relevant to the pandemic. Individual #3, did not clearly specific regarding execution of meetings nevertheless information had been communicated to all employees as to the way they need to be protected against the virus.





The above chart demonstrates the question of total surveys: Are you satisfied with what your company did to protect the employees from the COVID-19 virus? Strongly Agree, it involves the responses of 35 individuals with a rate of 70%. Agree, it involves the responses of 15 individuals with a rate of 30%. Following the responses, the researcher retrieve from interview question 9 of all individuals #1, #2,#3 and #4 and according to the above survey, the researcher is able to observe that electronic money and payments institutions strongly agree or either agree. Employees are feeling satisfied with what the company did to protect them against the pandemic since the management took several meetings, has continuously inform the employees regarding announcements of Cy government, social distancing, less people at the office while implementing the working from home scenario.



The above chart demonstrates the question of total surveys: Are you satisfied with what your company did to protect the employees from the COVID-19 virus? Yes, the researcher can observe that risk management did help the organization to overcome a crisis event like COVID-19 pandemic according to the above responses of 50 individuals with a rate of 100%.

Following the responses, the researcher retrieve from interview question 9 of all individuals #1, #2 and #3 and according to the above survey, the researcher is able to observe that the risk management role of the company played an important role in regarding to the pandemic. According to interviewing individual #1, there was a scenario on how to deal with the virus. The scenario was updated by the risk management that informed the senior management and the staff. According to interviewing individual #2, the fact that the company had in place proper manuals and policies as well the quick response of the management played an important role in handing the crisis. According to

individual #3, Risk management is a crucial and an essential department but also the setup of the company helped to overcome the pandemic. Interviewing individual #4 mentioned that, the controls, policies and procedures that are implemented by the company all contribute to overcome the crisis.

4.3 Interview Questions Analysis

Table 3. Interviewing Individuals Approach

Code Name	Role within the company	Why the reseacher felt it necessary to interview them.
#1	Compliance Manager & AMLCO	The specific individual belongs to the Middle Management of the company and he has previous experince in banking and EMI institutions for 20 years. He holds an MBA degree and a dimploma of AML and Compliance. Cooperates regularly with Risk Department or Manager and/or Risk Committee.
#2	Head of Compliance & AMLCO	The specific individual belongs to the Senior Management of the company and he has previous experince in EMI institutions for 5 years. He holds an MSc degree and a dimploma of AML and Compliance. Cooperates regularly with Risk Department or Manager and/or Risk Committee.
#3	Executive Director	The specific individual is a Director and he belongs to the Senior Management of the company. He has previous experince in EMI institutions for 5-10 years and holds an MSc degree. Belongs to the Risk Committee of the institution
#4	Compliance Manager & AMLCO	The specific individual belongs to the Senior Management of the company. She holds an MSc degree and a dimploma of AML and Compliance. Cooperates regularly with Risk Department or Manager and/or Risk Committee.

1. **Does your organization have a procedure manual and policies of risk management?**

Answer from interview question #1 Yes, it is a regulatory requirement for EMI's to have a set of policies and procedures regarding risk management.

Answer from interview question #2 Yes, the company maintains a Risk Management Manual.

Answer from interview question #3 Yes, our institution has both AML and Risk management procedure manuals and policies since is mandatory requirement by law.

Answer from interview question #4 Yes – The organization has a Risk Policy which covers the details relating to the identification, management and monitoring of risks. In view of the size and complexity of operations, EcommBX Ltd (the "Company") risk management procedures are being developed. Furthermore, it should be noted that the Company is continuously working on enhancing its risk procedures as the complexity and size of operations grow.

Thematic Analysis of Interview Data:

Following the responses, we obtained from the 4 interviewing individuals we can positively say that electronic money and payments institutions have procedure manual and policies of risk management since is a mandatory requirement set by Central Bank of Cyprus the regulator. The operations are continuously working on enhancing risk procedures to reach the maximum level of protection.

Risk management manual provides an overview of the risk management process and a practical guidance for the supervision of risks within departments and teams, to decrease the frequency of incidents and to reduce impact of incidents if they occur. Risk management policy is to provide guidance regarding the management of risk, to support the accomplishment of business objectives, safeguard employees and business assets while ensure financial sustainability.

2. Which are the most material risks an EMI organization faces during specific crises?

Answer from interview question #1 During crisis depending on the type and causes, always being able to continue operating is an important factor while minimizing the losses. Material risks may include operational risks and financial risks.

Answer from interview question #2 With regards to specific crises, I understand that you refer to CovID-19 and not any crises. I would say that these are fraud risk, cyber-attack, failure of technology and systems/platforms used; hence the various back-up tools and mechanisms the company has put in place.

Answer from interview question #3 Most material risks during a specific crisis I would say:

- Anti-money laundering or Regulatory risk
- Reputational risk
- Geographical risk
- Fraud risk
- Operational Risk
- Technology Risk

Answer from interview question #4 In view of the type of business that an EMI conducts, the risks faced are (usually) independent from crisis situations (e.g., unlike a banking institution where a financial crisis would impact credit risk). The primary source of risk for the Company, is operational risk and particularly information communication and technology risk and security risk. This particular risk stems from the fact that the Company is a fintech entity, which uses technology to operate, and thus its susceptibility to operational and ICT risk. Therefore, in view of this, the Company reviews a number of sub-risks under the ICT umbrella, including security risk.

Thematic Analysis of Interview Data:

Following the responses, we obtained from #1, #2, #3 and #4 interviewing individuals it involves, interviewer #1, Material risks may include operational risks and financial risks. Interview #2, Material risks these are fraud risk, cyber-attack, failure of technology and systems/platforms used; hence the various back-up tools and mechanisms the company has put in place. Interview #3, Material risk are, anti-money laundering or regulatory risk, reputational risk, geographical risk, fraud risk, operational risk and technology risk. Interview #4, Material risks may include

operational risk and particularly information communication and technology risk and security risk.

To summarize, the similar responses the research was able to observe on regard to material risks from the 4 interviewers individuals were related to Operational risk, Technology and Fraud risk. The aim is to enable the detection of all risks to which the organization might be exposed to and to facilitate the implementation of corrective measures to eliminate or mitigate those risks to the maximum level.

3. **How to manage, reduce or eliminate a possible manifestation of material risks with potential negative impacts?**

Answer from interview question #1 Reducing or eliminating possible material risks and their potential negative impacts can be achieved by having policies and procedures in place which provide for such risks by having actions plans in place to manage each case and employees trained to implement these procedures.

Answer from interview question #2 The management of the company (and the Board of Directors) shall make sure that effective controls are in place in order to avoid exposure. At the same time, the risk manager (or risk committee in cases that a company does not employee a dedicated risk manager) shall perform regular assessment reviews on the risks faced by the company. In cases where any deficiencies are noted, these need to be reported and escalated to management along with relevant suggestions on how to minimize the company's exposure. The management and the board need to make sure that the suggestions on how to mitigate risks are in line with and relevant to the operations of the company and if yes, to monitor that these are implemented.

Answer from interview question #3 *With* the use of technologies and with the right policies and procedures in place. Of course, capable personnel to observe and catch up with material risks.

Answer from interview question #4 The management of risk is primarily performed through the establishment of controls. These, take the form amongst others, of policies and procedures, segregation of duties between different functions and different persons within the same functions, 4-eye review and the continuous training of all the members of staff and management.

Thematic Analysis of Interview Data:

Following the responses, we obtained from #1, #2, #3 and #4 interviewing individuals mainly responded with the same way by having the establishment of controls, right policies and procedures in place, a capable personnel and trainings for implementation of the procedures. Interview #1 also mention that by having actions plans in place may help to reduce or eliminate a possible manifestation of material risks. Interviewer #2 mentioned that the risk manager or risk committee should perform assessment reviews. In case of any deficiencies need to be reported and escalated to the management with suggestions on how to minimize those risks. The management need to make sure that suggestions are in line in order to monitor that are implemented. Interviewer #3 mentioned that the risk manager of the company shall perform regular assessment reviews on the risks faced by the company and if any risks are identified the risk manager should report to the board the findings and suggest on how to eliminate or minimize company's exposure. Interviewing individual #4 mentioned that 4-eye review and the continuous training of all the members of staff and management establishment may bring sufficient control to the management of risks.

According to our findings we can positively disclose that the researcher agrees with all interviewing professionals. The risk manager and risk committee should aim to manage, reduce or eliminate a possible manifestation of material risks with potential negative impact by:

a) Identifying the risk itself and on time.
b) Avoid or eliminate the risk itself.
c) Use the transfer approach, transfer the risk to a third party.
d) Mitigate, with mitigation we reduce the likelihood of risk incidence or it reduce the impact of the risk within acceptable limits.

4. **What are risk management prevention measures in use and in relation to the identified risks?**

Answer from interview question #1 First is to perform a risk assessment and identify all risks the organization is facing. Based on the risk assessment to set controls and or mechanisms in order to manage those risks.

Train employees in identifying any risks arising from their daily operations and informing the RM Unit. Have plans in place for each risk that may have a material impact in order to be ready to response avoid wasting valuable time, secure the proper level resources and work smoothly in order to overcome all obstacles.

Answer from interview question #2 To perform regular assessment reviews of the risk factors faced by the company based on the scale and complexity of their operations. As part of this assessment shall be to monitor the exposure of the company and evaluate if the score of each risk factor changed. If yes (either increased or decreased), to understand if this would have any impact on the company's operations. The assessment exercise shall also aim to set proper controls in place to avoid any of the risk factors actually imposing a large threat to the company that could potentially harm and/or disrupt the operations.

Answer from interview question #3 Our risk-based approach by law and risk assessment tools that give us risk categorization for each type of risk.

Answer from interview question #4 As noted above, the main risk management procedures that are used in the management of operational risks (incl. ICT and security risks), relate to the following:

- An appropriate organizational structure, in line with regulatory requirements has been implemented. Amongst others a relevant Risk Committee has been set up which amongst other, ensures the appropriate and effective implementation of controls.
- An Information Security Policy and Change Management Policy has been implemented and communicated to all members of staff.
- The HR Manual documents the Code of Conduct and Code of Ethics, and identifies the way that employees need to conduct themselves.
- All personnel undergo training to be familiar with the Company's rules and regulations, including training on business conduct and information security.
- Independent assurance from the Company's internal auditor is obtained, to

identify the Company's conformity to policies, practices, and regulations.

- A Business Continuity Plan ("BCP") and Disaster Recovery Plan ("DRP") has been adopted.
- Penetration testing is performed on a bi-annual basis with the results being taken into consideration for any updates and system enhancements.
- All customer physical files have been scanned electronically and the original files are kept at a separate physical location away from the head office.

Thematic Analysis of Interview Data:

Following the responses, we obtained from interviewing individuals #1 and #2 , is to perform risk assessment and identify risks related to the company. They also mention that the aim is to set proper controls and mechanism to manage those risks. Interviewing #1 mentioned that by having plans in place for each risk would help to response avoid wasting valuable time, secure the proper level resources to overcome all obstacles. Responses we received form interviewing individual #2, to evaluate the scoring of each risk factor to understand if this would have any impact on the company's operations. Interviewing individual #3 mentioned that their risk-based approach as set by law and their risk assessment tools gives them risk categorization of each type of risk. Interviewing individuals #1 and #4 also mentioned that training the employees to identify any risks arising from daily obligation, related to company rules and business code of conduct. Interviewing individual #4 has given specific details on risk management prevention measures in used and in relation to information technology risk and security risk as clearly stated above.

Following the above responses and according to our research findings the aim is to be able to identify and manage potential risks that may affect the workplace and we positively agree with all the above responses stated by the interviewing professionals.

Risk management prevention measures are actions taken in response to the identified risk factors that may potentially cause an insistent or harm the organization activities. The management measures should either be designed to minimize the risks or eliminate them fully, with the latter clearly being most popular.

5. **Does your organization maintain a risk register scoring the likelihood, impact and severity of potential risks that may affect business performance or obligations?**

Answer from interview question #1 Yes, we have a risk register that is updated periodically or when there is a major change.

Answer from interview question #2 Yes, we do perform the above exercise for all risks relevant to the operations of EMIs based on the guidelines published by the EBA and the obligations stemming out of PSD2.

Answer from interview question #3 Yes, in the form of risk management report which is filed annually with the Central Bank of Cyprus

Answer from interview question #4 Yes

Thematic Analysis of Interview Data:

Following the responses, we obtained from interviewing individual #1, #2 and #4 we clearly recognize that they maintain a risk register according to the EBA and the obligations stemming out of PSD2. The response received by individual #3 is to argue if they have a risk register in place since the answer responded was not clear enough. Risk management repot is a mandatory obligation set by the regulator CBC for all EMIs and PIs to perform an annual report.

Risk register with scoring the likelihood, impact and severity of potential risks that may affect business obligations should be maintained since it is a tool used to manage risks and to comply with regulatory acts as repository of all identified risks.

6. **Did you participate in an exercise of the business continuity plan with or without any cause? Does your company have any contingency or disaster recovery plan in place? How often do the employees take trainings internal or external regarding issues of risk management?**

Answer from interview question #1 Yes at least once per year we have an emergency drill. Yes, we have a disaster recovery plan. It is part of our regulatory obligations that we have to keep up to date with the business developments. Employees take periodic trainings 3-4 times per year on various subjects depending on an annual training plan that is prepared by the risk management unit.

Answer from interview question #2 The company does have a business continuity plan in place. The said plan is being tested at least once a year to make sure that all employees understand their responsibilities in case something (like a pandemic) may disrupt the normal way of operations. These tests also aim to check that the systems used by the company (e.g., remote connectivity, back-up servers, etc.) are correctly activated as part of the business continuity policy or disaster recovery plan.

Answer from interview question #3 Yes, I have personally participated to a business continuity exercise without any cause. Our company maintain a disaster recovery plan. The employees are taking trainings once a year.

Answer from interview question #4 Both the BCP and DRP consider the risks that the Company is subject to, however a further enhancement with the introduction a business assessment process will be undertaken, which allow for both BCP and DRP to become more risk sensitive.

With regards to trainings, a risk management training to both Board and members of staff will be undertaken within 2021. It should be noted however that the Company's staff and management undergo trainings relevant to information security, GDRP, phishing to ensure that they remain updated on matters that may give rise to operational risk.

Thematic Analysis of Interview Data:

Following the responses, we obtained from interviewing individuals #1, #2 and #3 we clearly understand that their companies and themselves participate to a business continuity and disaster recovery plan since it is part of their regulatory obligations. According to interviewing individual #1 employees take periodic trainings 3-4 times per year. According to interviewing individual #2 and #3 employees take trainings once per year. Interviewing individual #4 clearly specify that further enhancement with the introduction a business assessment process will be undertaken, which allow for both BCP and DRP to become more risk sensitive. Within 2021 the Board and the staff of institution #4 will undertake training relevant to risk management.

Business continuity and disaster recovery plan should be test regularly in order be verified how efficiently is in real time scenarios. Risk management training can benefit the organization since it helps the employees to understand how important is to be

able to recognize and manage the organizational risks while exercising their dally duties. Trainings will improve employee's performance and the broader enterprise.

7. **Does your company maintain a handbook of COVID-19 pandemic available for employees? During the pandemic was you company able to continue working? Did you have any meetings or trainings against the virus?**

Answer from interview question #1 Yes, part of the measures to combat the pandemic was to develop a Covid 19 handbook that will provide accurate and up to date information to all employees regarding the virus as well as instructions on how to respond on predetermine scenarios in order to avoid confusion, minimize risks and handle the situation effectively. Various meeting were taken place while implementing the social distancing, using web technologies to communicate and providing full support to all staff to continue operate as usual. These measures were proved to be important for the successful management of the pandemic crisis.

Answer from interview question #2 We do not maintain a handbook for the employees as we believe that due to our size this was not relevant. Regular updates were sent instead via emails. Yes, the operations of the company continued uninterrupted.

The management took regular meetings to assess the situation based on each announcement made by the government.

Answer from interview question #3 No, we do not maintain this kind of handbook. The company was able to continue operate normally during the pandemic. Against the virus, we had two trainings for issues relevant to the pandemic.

Answer from interview question #4 No separate employee handbook is maintained for COVID-19, however information has been communicated to all employees as to the way they need to be protected against the virus. In view of the fact that the Company is a fintech entity, during the pandemic the Company continued working with no interruptions.

Thematic Analysis of Interview Data:

Following the responses, we obtained from interviewing individual #1 we clear understood that the company maintain a handbook of COVID 19 pandemic and these measures were proved to be important for the successful management of the pandemic crisis. According to interviewing individuals #2, #3 and#4 we realized that

their company did not maintain a handbook of COVID19 pandemic however the companies continue operating normally. Interviewing individuals #1 and #2 confirmed that various meetings took place to assess the situation based on announcements made by the government. Interviewing individual #2 sayed that the company had two trainings for issues relevant to the pandemic. Interviewing individual #4 sayed that information has been communicated to all employees as to the way they need to be protected against the virus.

A handbook of COVID-19 could be considered as progressive for an organization since the virus came to our lives without any warnings. Business were mainly struggling to safeguard their continues performance and to avoid any discontinuation of their business obligations. Employees are part of the organization and the employer should consider them as a true asset since they contribute to success of an organization this is why meeting and trainings are significant against the virus combating. Meeting have taken place correctly from organizations #1, #2 and #3 in order to protect the organization and the company itself while preventing from closer. According to interviewing individual #4 they did not perform trainings even though information and/or instructions have been given to employees.

8. How to utilize a crisis and adapt it into organizational opportunity (e.g., covid-19 vs electronic banking)

Answer from interview question #1 Sometimes during crises, opportunities arise. For example, during the pandemic people were forced to stay home. Due to that online sales were skyrocketed and the need of having an account with an EMI was even greater. EMIs offered cheap, reliable and fast payment solutions to businesses and consumers.

Answer from interview question #2 In such situations, although it may seem that opportunities are created for the online commerce and online banking/e-wallets etc. this is not always the case. This is because the market also needs to be able to accept this change and/or something new and technologically savvy versus the traditional and conventional solutions already being used. For example, the pandemic gave rise to online shopping which in turn increased the demand of online payment processors and providers of online payment solutions but at the same time the lockdown

decreased the volumes in businesses such as travel/hotels/hospitality, taxis and licensed sports betting shops. As a result, a company's portfolio of clients shall be as diversified as possible. Nonetheless, this crisis gave opportunities and created the need for companies who operate in this industry of online payments.

Answer from interview question #3 During the pandemic there was a massive shift from cash to contactless payments so we can positively say that this was an organizational or business opportunity for EMI and PI institutions.

Answer from interview question #4 The COVID-19 events have not particularly affected the way of operations of the Company. In effect the pandemic has in fact solidified the need for technology and the need for e-banking services. To this end, the Company has utilized the learning of the crisis in designing its strategy.

Thematic Analysis of Interview Data:

Following the responses, we obtained from interviewing individuals #1, #2 , #3 and #4 we can clearly say that EMI and PI institutions were benefit from the crisis of COVID19. According to interviewing individual #1 during the lockdown people were forced to stay home, because of that online sales were skyrocketed and the need of having an electronic account was greater in order to execute their online purchases since EMIs offered cheap, reliable and fast payment solutions to businesses and consumers. According to interviewing individual #2 the company's portfolio of clients was diversified since EMI and PI institutions gave raise during the pandemic virus from a different clientele. Mostly people have shown an increased interest on the demand of online payment processors and providers of online payment solutions but at the same time the lockdown decreased the volumes in businesses such as travel/hotels/hospitality, taxis and licensed sports betting shops. Nonetheless, this crisis gave opportunities and created the need for companies who operate in this industry of online payments. According to interviewing individual #3, during the pandemic there was a massive shift from cash to contactless payments and this shift have created an opportunity to EMI and PI institutions. According to Interviewing individual #4 the pandemic has in fact solidified the need for technology and the need for e-banking services.

Following the responses, we obtain from all interviewing individuals #1, #2, #3 and #4 we can positively say that with Lockdown and restrictions announced by the government on in-individual services, have obliged the banks to immediately arrange an enhanced number of virtual services. EMI companies where already into that part of services and they were positively benefit from it. If you are expanding digital services, you are reducing time and cost.

With COVID-19 pandemic the EMI and PI organizations were able to increase customer relationships, data protection and cyber security. Upgrading their software development apps, use contactless cards and apple pay payments since the pandemic has dramatically accelerated the rate of digital adoption in financial services.

9. Did risk management helped your organization to overcome a crisis event like the Covid-19 pandemic?

Answer from interview question #1 Yes, risk management played an important role. In our business continuing there was one scenario on how to deal with a pandemic. This scenario was updated by the risk management that informed the Senior Management and staff. Due to this the company was able to continue its operations without any disruptions, servicing customers while complying all regulatory obligations.

Answer from interview question #2 Yes, the fact that the company had in place proper manuals and policies as well as the quick response of the management played an important role in handling the crisis and continue the operations of the company as smooth as possible.

Answer from interview question #3 Risk management is crucial and an essential department within the institution although I would not say only risk management, but the setup of the company helped to overcome the Covid 19 pandemic.

Answer from interview question #4 The COVID-19 crisis has contributed to substantially changing the way everyone works and lives. In view of the heightened stress that people may feel, as a result of isolation measures there may be an increase in operational risk and specifically human resources and processes related risk. The controls that are implemented by the Company as noted above, including dual review and the 4 eye principle, the policies and procedures implemented, all contribute to ensuring that any additional risk arising as a result of the pandemic is appropriately managed.

Thematic Analysis of Interview Data:

Following the responses, we obtained from interviewing individuals #1, #2 and #3 it seems that Risk Management function is considered to be an important role, crucial, an essential department and with the right or proper manual and policies as well as the setup of the company including top management played an important role in handling the crisis and to continue normal operations of the institutions. According to interviewing individual #4 we did not receive an actual response if risk management helped the organization to overcome the crisis.

Within the latest risk assessment results COVID -19 pandemic has been categorized as a high-risk level worldwide. A risk interconnectivity analysis should be assessed to understand other major business risks triggered by the virus. The current internal audit testing plans should be re-examined to ensure that they sufficiently cover pandemic risk aspects. Have risks been emerged such as enhanced cyber risks due to a remote workforce that need to be addressed. Procedures should be in place to report, gather and analyze evolving risks as this situation progresses. COVID-19 may impact your controls reporting to stakeholders and the service organization's controls reporting. Risk is the main cause of uncertainty in any organization. Therefore, companies should be focusing on identifying and managing risks that may or may not cause disruption or discontinue of daily obligations and business performance.

CHAPTER 5

DISCUSSION

Recommendations, Future Research and Conclusion

The last main division of the research study comprises the summing up. The author will clearly state the answers to the main research questions of the research paper entitled: How do organisations such as Electronic Money and Payment Institutions in Cyprus turn threats and crisis situations into strategic opportunities in times of crisis management? The researcher will summarize and reflect on the research to identify gaps between literature review and real time in addition will propose recommendations on future research and the knowledge the researcher has contribute.

5.1 Answers to the main research questions

5.1.1 Which are the most material risks an EMI organization faces during specific crises?

To clearly state the answer related to material risks, the researcher is able to observe that EMIs and PIs are equivalent to regulatory, operational, fraud and technology risks according to collected questionnaires. The researcher argues we the above responses not because the mentioned risks are not the most material according to our findings but as stated by (Ward, 1999) “A common problem in project of risk management processes is the need to determine the relative significance of different sources of risk so as to guide subsequent risk management effort and ensure that the business remains cost effective and efficient concerning to organizational performance”. According to Ward, (1999) A mutual approach is to classify risks in terms of opportunity and impact to determine causes of risk which can take the primary attention since risk is the main cause of uncertainty in any organization.

To look at the shortcomings of this system on guiding the analysis and management of risks while take into account the data required for a correct assessment of priority risks.

For efficient management it is fascinating to tell apart not solely between the scale of impacts and chance of impacts occurring, however conjointly alternative factors such as the possibility of obtainable responses correlated to time similar to the pandemic or unexpected events this would reflect to arising more risks that the institutions would be normally subject to.

5.1.2 How to manage, reduce or eliminate a possible manifestation of material risks with potential negative impacts?

To clearly state the answer related to how to manage, reduce or eliminate material risks with potential negative impacts. The researcher positively agrees to a medium level with the responses retrieved from interviewing professionals by having the establishment of controls, right policies and procedures in place, a capable personnel and trainings for implementation of the procedures. As stated by Salem Press, (2014:1) "Principles of risk management are needed even more today than ever before." During older times, several corporations did not have someone dedicate and they either overlook the risks or they were living by them while facing the negative effects triggered by numerous of risks. Caused of the apathetic way, many businesses came into bankruptcy or closer. Therefore, risk management nowadays is an important, essential and a principal function within financial institutions. (Salem Press, 2014)

A continuously self-improvement of technology process to fintech entities relates to manuals and polices or mechanics with the prospect to automate more the financial services would be a higher solution level to identify and avoid risks relevant to information technology risks. Therefore, if a financial institution will not keep up with new technology could become uncompetitive and prevent profitability loss and consumer inattention.

Regulatory Risk: The complaint unit has procedures for monitoring European and National legislation, it also identifies changes and informs affected parties to implement the new requirements. In addition, the complaint unit should maintain a register with the new legislation in force. Where it is deemed necessary legal consultation is seeking.

Operational Risk: With the application of this six-stage process, EMI and PI organizations obtain the implementation of a robust risk management framework. The framework

allows the institution to manage risk more efficiently, it also improves the dynamic intensity among risk and prospect (Kluwer, 2011).

The manageable framework for operational risk management is to comply with the multitude of regulatory requirements:

1. Risk detection
2. Basic risk management procedure
3. Reporting
4. Crucial risks, scenarios and wealth calculation
5. Risk appetite
6. Operational & audit contribution and reconsideration

(Kluwer, 2011).

Where practical, companies may employ three lines of defense as part of their operational risk governance and risk management structure. A robust risk culture with a well defined communication and comprehension and a solid sense of risk consciousness can deliver comfort when used in combination with this approach (The Financial Service Authority, 2011)

The three lines to consist of the following:

1. The first line is provided by the business units – comprising the business units, support functions and embedded risk staff.
2. The second line is provided by the risk management function – comprising the operational risk management function and the compliance functions.
3. The third line is the Governance and oversight provided by the internal and external auditors.
   (The Financial Service Authority, 2011)

Fraud Risk: Internal fraud arise when a present or ex-worker take the opportunity to thieve, amend or destroys organizational information (such as customer data) or assets (such as computer software or physical assets) for private benefit.

The risk mitigation process could include:

1. Security Awareness Program
2. Physical Access Management
3. Two-factor authentication (external)
4. Advanced Email Solution (Microsoft)
5. Backup of all important information

Technology Risk: The chief technology officer should participate in an IT think tank team of the organization that monitors technological advancements, trends opportunities and threats while close monitoring any technological upgrades. Implement a cyber risk insurance policy available from insurance agencies.

The risk manager and risk committee should aim to manage, reduce or eliminate a possible manifestation of material risks with potential negative impact by implementing the below.

a) Identifying the risk itself and on time.
b) Avoid or eliminate the risk itself.
c) Use the transfer approach, transfer the risk to a third party.
d) Mitigate, with mitigation we reduce the likelihood of risk incidence or it reduce the impact of the risk within acceptable limits.

5.1.3 What are risk management prevention measures in use and in relation to the identified risks?

To clearly state the answer related to what are risk management prevention measures in use and in relation to the identified risks. The researcher positively agrees to a medium level with the responses retrieved from interviewing professionals. Following the responses collected from all interviewing individuals and according to our research findings the aim is to be able to identify and manage potential risks that may affect the workplace. Risk management prevention measures are actions taken in response to the identified risk factors that may potentially cause an insistent or harm the organization activities. The management measures should either be designed to minimize the risks or eliminate them fully, with the latter clearly being most popular.

In general businesses are subject to a range of risks, some of which are anticipated but many of which are either unexpected or not effectively managed. Adopting a formal risk

management framework can assist businesses in planning more effectively, understanding why things have not gone according to plan and ideally in acting before losses are incurred. The goal in having an efficient risk management framework is to be pro-active instead of reactive in managing the risks inherent in an exceedingly business model (Koblanck, 2016).

The researcher is suggesting the usage of ISO 31000, Risk Management Guidelines since it provides the principles, a framework and a process for handling risk. It can be applied by any organization or institution irrespective the size, activity or sector. By the usage of ISO 31000 the organizations or institutions can achieve an overall increase of the likelihood of achieving objectives, would enhance the detection of opportunities and threats and they would efficiently allocate and use resources for risk treatment. Nevertheless, ISO 31000 cannot be utilized for certification reasons, even though it does offer guidance for internal or external audit programs. Organizations or Institutions who are using it can compare their risk management practices with an internationally recognized standard, providing the right principles for an efficient management and corporate governance.

5.1.4 How to utilize a crisis and adapt it into organizational opportunity (e.g., covid-19 vs electronic banking)

To clearly state the answer related to what are risk management prevention measures in use and in relation to the identified risks. The researcher positively agrees with the responses retrieved from interviewing professionals and according to our research findings we can say that with lockdown and limits on in-person services, financial institutions were compelled to get organized for an enhanced volume of electronic services. EMI companies where already into that part of services and they were positively benefit from it. If you are expanding digital services, you are reducing time and cost. With COVID-19 pandemic the EMI and PI organizations were able to increase customer relationships, data protection and cyber security while upgrading their software development apps, use contactless cards and apple pay payments. The pandemic has dramatically accelerated the rate of digital adoption in financial services.

With regards to institutions #2, #3 and #4 the researcher agrees to a medium level according to the responses retrieved from interviewing professionals since we realized that their company did not maintain a handbook of COVID19 pandemic however the companies continue operating normally. The researcher would suggest the adoption of a proper and valid manual against pandemics or virus for precautionary measures. Purpose of that is to provide an accurate and up to date information to all employees as well instructions on how to respond on predetermined scenarios. To avoid confusion, minimize risk and handle the situation more effectively.

5.2 Summarize

The results of the research study have been utilized to understand and discuss how Electronic Money and Payment institutions react in cases of crisis even occur. The outcome has proven the medium existence of a suitable and appropriate crisis management in the field of financial institutions, however a continues risk management implementations are indicated where relevant. Real scenarios describe how the institutions created prospects while continue operating without any crisis disruption. The effects of the results were critically examined and recommendations of future research is suggested.

5.3 Limitations

The researchers main target was to approach all the EMIs and PIs in Cyprus to get the maximum results from 12 operating institutions. The researcher manages to collect data from 4 institutions due to confidentiality policy, reporting obligations, deadlines given by the regulator CBC and restrictions of Covid-19 pandemic. The data collection from the questionnaires was not the ultimate since the time that the questionnaires were available in the EMI and PI institutions was during the second lockdown period in Cyprus which a significant amount of personnel was either working from home or was on obligatory leave.

The lack of previous research studies on the topic and Covid-19 pandemic did not affect the researcher from being accurate and the performing results was satisfactory. Nevertheless, the researcher can positively disclose that a sample of the data collection surveys with dimension of 83% response rate and interviews questions of 100% response rate may bring significant and reliable outcome.

5.4 Recommendations on Future Research and Conclusion

The results of the research study how do organisations operating in the Electronic Money and Payment Institutions of Cyprus turn threats and crisis situations into strategic opportunities in times of crisis management have proven an appropriate risk management in the area of fintech entities such as Electronic Money and Payment Institutions. Nevertheless, the researcher agrees to medium level with financial institutions in regard to responses retrieved through of data collection. The author was able to gain knowledge through recommendations and suggestions to an improved risk management performance via following implementations.

Firstly, a common approach is to rank risks in terms of chance and impact to spot sources of risk. To look at the shortcomings of this system on guiding the analysis and management of risks while consider the data required for a correct assessment of priority risks. For efficient management, it is impressive to tell apart not solely between the scale of impacts and chance of impacts occurring, however conjointly alternative factors such as the possibility of obtainable responses correlated to time similar to the pandemic or unexpected events this would reflect to arising more risks that the institutions would be normally subject to.

Secondly, a continuously self-improvement of technology process to fintech entities relates to manuals and polices or mechanics with the prospect to automate more the financial services. A manageable framework for operational risk management and where practical, companies may employ three lines of defense as part of their operational risk governance and risk management structure (The Financial Service Authority, 2011). The risk manager and risk committee should aim to manage, reduce or eliminate a possible manifestation of material risks.

Thirdly, the researcher is suggesting the usage of ISO 31000 Risk Management Guidelines since it provides the principles, a framework and a process for handling risk. By the usage of ISO 31000 the organizations or institutions can achieve an overall increase of the likelihood of achieving objectives, would enhance the detection of opportunities and threats and they would efficiently allocate and use resources for risk treatment.

Finally, the researcher would suggest the adoption of a proper and valid manual against pandemics or virus for precautionary measures. Based on all the above, the author would propose to the participants to take into consideration suggestions trigger thought of this research study with prospect of enhancing and improving risk management approach to the maximum level while safeguarding the institutional activities and business obligations daily. Additionally, the current findings, results and analysis will be shared with the relevant participated financial institutions, as promised via email and telecommunication.

REFERENCES

Allianz P.L.C., (2017). Solvency and Financial Condition Report for the year ended 31 December 2017. https://www.allianz.ie/regulatory-information/allianz-sfcr-2017.pdf

Allianz Group, (2018). Solvency and Financial Condition Report 2018 https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/investor-relations/en/results-reports/sfcr/en-AllianzGroup-SFCR-2018.pdf

American Psychological Association. (2020). Publication Manual of the American Psychological Association (7th ed.) https://doi.org/10.1037/0000165-000

Analyzing & Managing Risk. (2014). Ipswich, Massachusetts: Salem Press. Accessed April 28, 2021. http://search.ebscohost.com/login.aspx?direct=true&db=e020mww&AN=777890&site=eds-live

Aven, T. (2010). Risk Management. In: Grimvall G., Holmgren Å., Jacobsson P., Thedéen T. (eds) Risks in Technological Systems. Springer Series in Reliability Engineering. Springer, London.

Bachtiar, G. (January 2014). Implementing Enterprise Risk Management with ISO 31000:2009. https://www.slideshare.net/goudotmobi/implementing-enterprise-risk-management-with-iso-31000-2009

Borge, D. (2001). The Book of Risk. New York: John Wiley and Sons. pp.4

Brewer, J., & Hunter, A. (1989). Multimethod research: A Synthesis of styles. Newbury Park, CA: Sage Publications.

Brown, L. S. (2018). Theories of Psychotherapy Series. Feminist Therapy (2nd ed.). American Psychological Association.

Central Bank of Cyprus. (2020). https://www.centralbank.cy/

Central Bank of Cyprus. (2021). Licensing and supervision of electronic money institutions. https://www.centralbank.cy/en/licensing-supervision/electronic-money-institutions/licensing-and-supervision-of-electronic-money-institutions

Central Bank of Kenya. (January 2013). Risk Management Guidelines. Central Bank of Kenya, https://www.centralbank.go.ke: Risk management guidelines, 2013.

Chernobai, A., Rachev, S., & Fabozzi, F. (2007). Operational Risk. A guide to Basel 2 Capital Requirements, Models and Analysis. Hoboken, New Jersey: John Wiley and Sons.

Clarke, C., & Varma, S. (1999). Strategic Risk Management: The New Competitive Edge. Long Range Planning, 32/4, pp.414-424.

Creswell, J., & Clark V. (2011). Designing and Conducting Mixed Methods Research. 2nd Edition, Los Angeles: Sage Publications.

Creswell, J. (2015). A concise introduction to mixed methods research. Los Angeles: Sage Publications.

Creswell, J., W., Clark V., Gutmann, M., & Hanson, W. (2003). Advanced Mixed Methods Research Designs. In Tashakkori, A., & Teddlie C. (Eds.), Handbook of Mixed Methods in Social and Behavioral Research. Thousand Oaks, CA: Sage Publications. pp.209–240.

Deloitte. (2016). Fraud Risk Management: Awareness, prevention, detection and investigation. https://www2.deloitte.com/mt/en/pages/risk/articles/mt-risk-article-fraud-risk-management.html

Demb, A., & Funk, K. (September 1999). What Do They Master? Perceived Benefits of the Master's Thesis Experience. NACADA Journal, 19/2, pp. 18–27.

Faghfouri, P. (2012). The Role of Governance Structure in the Context of Crisis Management: An Empirical Analysis on a German Sample of Non-Family and Family Businesses. Essen, Germany: Springer Gabler.

Federation of European Risk Management Associations (FERMA). (2011). A structured approach to enterprise risk management (ERM) and the requirement of ISO 31000. https://www.ferma.eu/app/uploads/2011/10/a-structured-approach-to-erm.pdf

Fink, S. (2002). Crisis management: Planning for the inevitable. IUniverse. pp.54

Fraser, J., & Simkins, B. (2010) - Enterprise Risk Management pp.100 New Jersey : Wiley pp.100.

Goles, T., & Hirschheim, R. (2000). The paradigm is dead, the paradigm is dead . . . long live the paradigm: the legacy of Burrell and Morgan. Omega: The International Journal of Management Science 28/ pp. 249–68.

Greene, J. (2007). Mixed methods in social inquiry. CA: John Wiley and Sons

Greene, J., Caracelli, V., & Graham, W.(1989). Toward a Conceptual Framework for Mixed-Method Evaluation Designs. Educational Evaluation and Policy Analysis, 11/3 pp. 255-274.

International Organization for Standardization. (2009). ISO 31000:2009, Risk management - Principles and guidelines. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en

International Organization for Standardization. (2009). ISO Guide 73:2009, Risk Management- Vocabulary"2009, Geneva. https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

International Organization for Standardization. (2018). ISO 31000:2018, Risk management - Guidelines. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

International Organization for Standardization. ISO 31000 Risk Management https://www.iso.org/iso-31000-risk-management.html

James, W. (2000). What pragmatism means. In Pragmatism and the Classical American Philosophy: Essential Readings and Interpretive Essay, 2nd ed. Edited by Stuhr, J. New York: Oxford University Press, pp. 193–202.

Jick, T. (1979) Mixing Qualitative and Quantitative Methods: Triangulation in Action. Administrative Science Quarterly, 24/4, pp. 602-611.

Kaushik, V., and Walsh, A., C. (2019). Pragmatism as a Research Paradigm and Its Implications for Social Work Research. Social Sciences 8/9, pp. 255.

Kumar, T. (January 2008). The Methodology Behind Risk and Control Self-Assessment. https://www.theglobaltreasurer.com/2008/01/02/the-methodology-behind-risk-and-control-self-assessment/

Ministry of Finance Cyprus, (February 2017). Own Risk and Solvency Assessment (ORSA). http://mof.gov.cy/assets/modules/wnp/articles/201702/223/editor/orsa.pdf. (Feb. 2021).

Morgan, L., D. (2014) Integrating Qualitative and Quantitative Methods: A Pragmatic Approach. Thousand Oaks: Sage.

Morse, J., M., & Niehaus, L. (2009). Mixed method design: Principles and procedures. Walnut Creek: Left Coast Press.

Official Journal of the European Union. (December 2015). Directives. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN

Official Journal of the European Union. (October 2009). Directives. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=EN

Official Journal of the European Union. (October 2009). Electronic Money Law Of 2012 https://www.centralbank.cy/images/media/redirectfile/Electronic%20Money%20Institutions/EMI-DIRECTIVE-EN-UNOF-TRANSL-241-29062012.pdf

Pansiri, J., (2005). Pragmatism: A methodological approach to researching strategic alliances in tourism. Tourism and Hospitality Planning and Development 2/ pp. 191–206.

Patton, M., Q. (1990). Qualitative evaluation and research methods (2nd ed.). Newbury Park, CA: Sage Publications.

Pearson, C., & Clair, J. (1998) Reframing crisis management. Academy of Management Review, 23/1, pp:59-61.

PricewaterhouseCoopers. (2020). Electronic Money & Payment Institutions. https://www.pwc.com.cy/en/industries/assets/electronic-money-and-payment-institutions.pdf

PricewaterhouseCoopers. (2020). Regulatory Risk Management. https://www.pwc.com/la/en/risk-assurance/regulatory-risk-management.html

Proença, D., Estevens, J., Vieira, R., & Borbinha, J. (August 2017). Risk Management: A Maturity Model Based on ISO 31000. Greece: Institute of Electrical and Electronics Engineers.

Quantum Leben. (May 2018). Solvency and Financial Condition Report. https://www.quantumleben.com/de/assets/upload/quantum-leben-ag-sfcr-2017.pdf

Ramar, R. (2014). Operations Risk Management: RCSA Management and Analysis. https://analyticsindiamag.com/operations-risk-management-rcsa-management-and-analysis/

Segal, S. (2011). Corporate Value of Enterprise Risk Management: The Next Step in Business Management. Hoboken (NJ): Wiley, pp:24

Seuss, T. (1978). I can read with my eyes shut. United Kingdom: HarperCollins.

Tashakkori, A., & Teddlie, C. (2008). Mixed Methodology: Combining Qualitative and Quantitative Approaches. Thousand Oaks: Sage Publications.

Tashakkori, A., & Teddlie, C. (Eds.). (2010). Handbook of Mixed Methods in Social and Behavioral Research. Thousand Oaks, CA: Sage Publications. pp.209–240.

The institute of Operational Risk. (2020). Embedding an Operational Risk Management Framework.https://www.ior-institute.org/sound-practice-guidance/embedding-an-operational-risk-management-framework

The Financial Service Authority.(2011). Enhancing frameworks in the standardized approach to operational risk–Guidance note. https://docplayer.net/11852670-Enhancing-frameworks-in-the-standardised-approach-to-operational-risk.html

Koblanck, A. (2016). Digital Financial Services and Risk Management. The MasterCard Foundation and IFC's. https://www.ifc.org/wps/wcm/connect/92ac1a71-6bd5-43db-84ff-1b6794f82653/Digital+Financial+Services+and+Risk+Management+Handbook.pdf?MOD=AJPERES&CVID=mxxEJFZ

Kluwer, W. (September 2011). Six stages to a robust operational risk framework https://www.bobsguide.com/guide/news/2011/Sep/20/six-stages-to-a-robust-operational-risk-framework/

Vasile, E., & Croitoru, I. (2012). Integrated Risk Management System: Key Factor of the Management System of the Organization. Rijeca, Croatia: Janeza Trdine.

Ward, S. (December 1999). Assessing and Managing Important Risks. International Journal of Project Management, 17/6, pp. 331-336.

Westfall, L. (2001). Software Risk Management. The Westfall Team, Milwaukee(2000): 32.

World health organization. (June 2020). Coronavirus disease (COVID-19): Health and safety in the workplace. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/coronavirus-disease-covid-19-health-and-safety-in-the-workplace

Yefimov, V. (2004). On Pragmatist Institutional Economics. IDEAS Working Paper Series from RePEc; Munich: Munich Personal RePEc Archive

APPENDIX 1
QUESTIONNAIRE

Dear Participants,

I invite you to participate in the research study entitle: How do organisations such as Electronic Money and Payment Institutions in Cyprus turn threats and crisis situations into strategic opportunities in times of crisis management?

We do not know enough about crisis management in EMIs and PIs. This lack of knowledge is exposing organisations to disruptions such as those caused by COVID19, including losses in revenue, missed strategic opportunities and impacts their reputation. Therefore, it is imperative to address this lack of research with purposive research that focuses on this crisis management predicament faced by EMIs and PIs in Cyprus.

I am currently enrolled in the MSc of Enterprise Risk Management at the Open University of Cyprus and I am in the process of writing my master's thesis.

The questionnaire is completely voluntary and will take less than 15 minutes to complete. Results will be used only for the purposes of the current study and not for any other reason.

Thank you for your time.

Best Regards,
Anastasis Spyrides

PART A: Demographics

Please tick the below

Gender: ☐Male ☐Female ☐ (Prefer not to answer)

Age:

Less than 25☐

25-35☐

36-45☐

46-55☐

56-65☐

Over 65☐

Prefer not to answer☐

Education Level: ☐Primary ☐Secondary Tertiary: ☐BSc ☐ MSc ☐PhD

Type of Business you work:

Electronic Money and Payment Institution Organization in Cyprus ☐

Level of the company's hierarchy you currently have

Front line☐

Back office☐

Middle management☐

Senior Management☐

Work Experience in the Current Position:

Less than 1 Year☐

1 - 2 Years☐

2 - 5 Years☐

5 - 10 Years☐

Over 10 Years☐

PART B: Data Collection Survey

1. **Do you consider risk management an important function for your organization?**

   Strongly Disagree☐
   Disagree☐
   Neutral☐
   Agree☐
   Strongly Agree☐

2. **Does risk management improve business performance?**

   Strongly Disagree☐
   Disagree☐
   Neutral☐
   Agree☐
   Strongly Agree☐

3. **Is top management involved in risk management processes?**

   Yes☐
   No☐

4. **Does your organization have a procedure manual and policies of risk Management?**

   Yes☐
   No☐

5. **Does your organization maintain a risk register scoring the likelihood, impact and severity of potential risks that may affect business performance or obligations?**

   Yes☐
   No☐

6. **Have you ever been informed what kind of risks your organization might be exposure to?**

   Yes☐
   No☐

7. **What type of risks it could have the highest impact in your company?**

Strategic Risk☐

Regulatory Risk☐

Operational Risk☐

Technology Risk☐

Financial Risk☐

Fraud Risk☐

Reputational Risk☐

8. **What type of risk it could have the lowest impact in your company?**

Strategic Risk☐

Regulatory Risk☐

Operational Risk☐

Technology Risk☐

Financial Risk☐

Fraud Risk☐

Reputational Risk☐

9. **How often do you take trainings internal or external regarding issues of risk management?**

Never☐

1-2 per year☐

3-4 per year☐

5-6 per year☐

More than 7☐

10. **Are you aware if your organization has a business continuity plan in place at the current time?**

Yes☐

No☐

11. **How often do you believe a business continuity plan should be revaluated?**

Never☐

Daily☐

Monthly☐

Quarterly☐

Yearly☐

12. **Did you participate in an exercise of the business continuity plan with or without any cause?**
    Yes ☐

    No☐

13. **Are you familiar with guidelines against COVID -19 pandemic in Cyprus Government?**
    Yes☐

    No☐

14. **Does your company maintain a handbook of COVID-19 -19 pandemic available for employees?**
    Yes☐

    No☐

15. **During the crisis of COVID -19 pandemic was you company able to continue working?**
    Yes☐

    No☐

16. **Did you have any meetings or trainings against the COVID-19 virus?**
    Yes☐

    No☐

17. **Are you satisfied with what your company did to protect the employees from the COVID-19 virus?**

    Strongly Disagree☐

    Disagree☐

    Neutral☐

    Agree☐

    Strongly Agree☐

18. **Did risk management helped your organization to overcome a crisis event like the Covid-19 pandemic?**
    Yes☐

    No☐

PART C: Interview Questions

1. **Does your organization have a procedure manual and policies of risk management?**

2. **Which are the most material risks an EMI organization faces during specific crises?**

3. **How to manage, reduce or eliminate a possible manifestation of material risks with potential negative impacts?**

4. **What are risk management prevention measures in use and in relation to the identified risks?**

5. **Does your organization maintain a risk register scoring the likelihood, impact and severity of potential risks that may affect business performance or obligations?**

6. **Did you participate in an exercise of the business continuity plan with or without any cause? Does your company have any contingency plan or disaster recovery plan in place? How often do the employees take trainings internal or external regarding issues of risk management?**

7. **Does your company maintain a handbook of COVID-19 -19 pandemic available for employees? During the pandemic was you company able to continue working? Did you have any meetings or trainings against the virus?**

8. **How to utilize a crisis and adapt it into organizational opportunity (e.g., covid-19 vs electronic banking)**

9. **Did risk management helped your organization to overcome a crisis event like the Covid-19 pandemic?**

APPENDIX 2

PART A: Demographics

Participants	Gender	Age	Education Level	Type of Business you work	Level of the company's hierarchy you currently have	Work Experience in the Current Position
1	Male	36-45	BSc	EMI & PI	Senior Management	Over 10 years
2	Male	46-55	MSc	EMI & PI	Middle Management	Over 10 years
3	Male	56-65	BSc	EMI & PI	Senior Management	Over 10 years
4	Male	36-45	BSc	EMI & PI	Senior Management	2-5 years
5	Male	36-45	BSc	EMI & PI	Senior Management	Less than 1 year
6	Male	36-45	MSc	EMI & PI	Middle Management	5-10 years
7	Male	36-45	BSc	EMI & PI	Middle Management	2-5 years
8	Male	25-35	MSc	EMI & PI	Middle Management	2-5 years
9	Female	36-45	BSc	EMI & PI	Middle Management	2-5 years
10	Female	25-35	BSc	EMI & PI	Middle Management	Less than 1 year
11	Female	25-35	BSc	EMI & PI	Back Office	Less than 1 year
12	Female	25-35	BSc	EMI & PI	Back Office	1-2 years
13	Female	25-35	BSc	EMI & PI	Back Office	1-2 years
14	Male	25-35	MSc	EMI & PI	Back Office	1-2 years
15	Female	25-35	BSc	EMI & PI	Back Office	2-5 years
16	Female	Less than 25	BSc	EMI & PI	Front Line	1-2 years

17	Male	36-45	MSc	EMI & PI	Senior Management	1-2 years
18	Male	46-55	MSc	EMI & PI	Senior Management	2-5 years
19	Female	25-35	BSc	EMI & PI	Front Line	1-2 years
20	Female	25-35	BSc	EMI & PI	Back Office	2-5 years
21	Male	46-55	MSc	EMI & PI	Senior Management	5-10 years
22	Male	46-55	MSc	EMI & PI	Senior Management	2-5 years
23	Female	36-45	MSc	EMI & PI	Senior Management	2-5 years
24	Male	25-35	MSc	EMI & PI	Middle Management	2-5 years
25	Male	25-35	BSc	EMI & PI	Back Office	2-5 years
26	Female	36-45	MSc	EMI & PI	Middle Management	2-5 years
27	Female	25-35	MSc	EMI & PI	Middle Management	2-5 years
28	Female	Less than 25	BSc	EMI & PI	Front Line	Less than 1 year
29	Male	36-45	MSc	EMI & PI	Senior Management	2-5 years
30	Female	25-35	MSc	EMI & PI	Middle Management	2-5 years
31	Female	25-35	MSc	EMI & PI	Back Office	2-5 years
32	Female	36-45	MSc	EMI & PI	Senior Management	1-2 years
33	Female	36-45	MSc	EMI & PI	Middle Management	2-5 years
34	Male	25-35	MSc	EMI & PI	Back Office	2-5 years
35	Male	36-45	MSc	EMI & PI	Senior Management	5-10 years

36	Female	25-35	BSc	EMI & PI	Back Office	Less than 1 year
37	Female	Less than 25	BSc	EMI & PI	Back Office	1-2 years
38	Female	25-35	MSc	EMI & PI	Back Office	2-5 years
39	Male	25-35	MSc	EMI & PI	Back Office	2-5 years
40	Male	25-35	BSc	EMI & PI	Back Office	1-2 years
41	Male	25-35	BSc	EMI & PI	Back Office	2-5 years
42	Female	25-35	BSc	EMI & PI	Back Office	2-5 years
43	Female	25-35	MSc	EMI & PI	Middle Management	2-5 years
44	Male	36-45	MSc	EMI & PI	Senior Management	2-5 years
45	Female	25-35	MSc	EMI & PI	Senior Management	2-5 years
46	Male	36-45	MSc	EMI & PI	Senior Management	Over 10 years
47	Male	46-55	MSc	EMI & PI	Senior Management	1-2 years
48	Male	56-65	BSc	EMI & PI	Senior Management	5-10 years
49	Female	25-35	BSc	EMI & PI	Senior Management	5-10 years
50	Female	36-45	MSc	EMI & PI	Senior Management	2-5 years

PART B: Data Collection Surveys

Q1	Q2	Q3	Q4	Q5	Q6	Q7
Agree	Agree	Yes	Yes	Yes	Yes	Strategic, Regulatory, Operational, Reputational
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Operational
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Strategic, Regulatory, Operational, Reputational
Strongly Agree	Neutral	Yes	Yes	Yes	Yes	Strategic, Regulatory, Operational, Technology, Financial, Fraud, Reputational
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Strategic, Regulatory, Operational, Reputational
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Regulatory, Operational
Strongly Agree	Agree	Yes	Yes	Yes	Yes	Strategic, Regulatory, Operational, Fraud, Reputational
Strongly Agree	Agree	Yes	Yes	Yes	Yes	Regulatory, Operational, Fraud, Reputational
Agree	Neutral	Yes	Yes	Yes	Yes	Regulatory, Operational, Reputational
Strongly Agree	Agree	Yes	Yes	Yes	Yes	Regulatory, Operational, Reputational
Strongly Agree	Agree	Yes	Yes	Yes	Yes	Regulatory, Fraud
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Financial, Fraud
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Regulatory, Operational
Strongly Agree	Agree	Yes	Yes	Yes	Yes	Strategic, Regulatory, Operational, Fraud, Reputational
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Regulatory, Operational
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Regulatory, Operational, Reputational
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Strategic, Regulatory, Operational, Technology, Fraud
Agree	Agree	Yes	Yes	Yes	Yes	Operational, Technology

Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Regulatory, Operational, Fraud, Reputational
Agree	Strongly Agree	Yes	Yes	Yes	Yes	Strategic, Regulatory, Operational, Financial
Strongly Agree	Agree	Yes	Yes	Yes	Yes	Regulatory, Operational, Technology, Fraud, Reputational
Agree	Agree	Yes	Yes	Yes	Yes	Strategic, Regulatory, Operational, Technology, Fraud
Strongly Agree	Agree	Yes	Yes	Yes	Yes	Regulatory, Operational, Technology, Financial, Fraud
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Regulatory, Technology, Fraud
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Regulatory, Operational, Fraud
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Regulatory, Operational
Agree	Strongly Agree	Yes	Yes	Yes	Yes	Strategic, Regulatory, Operational, Reputational
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Strategic, Regulatory, Financial
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Regulatory, Technology, Fraud
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Regulatory, Operational, Technology, Fraud, Reputational
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Regulatory, Operational, Technology, Fraud, Reputational
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Regulatory, Operational, Technology, Fraud, Reputational
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Regulatory, Technology, Fraud, Reputational
Agree	Agree	Yes	Yes	Yes	Yes	Regulatory, Technology, Fraud, Reputational
Agree	Agree	Yes	Yes	Yes	Yes	Regulatory, Operational, Technology, Fraud, Reputational
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Strategic, Regulatory, Operational, Technology, Fraud
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Regulatory, Operational, Technology, Fraud

Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Regulatory, Operational, Technology, Fraud
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Regulatory, Operational
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Regulatory, Operational, Reputational
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Regulatory, Operational
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Strategic, Regulatory, Operational, Technology, Financial
Strongly Agree	Agree	Yes	Yes	Yes	Yes	Strategic, Regulatory, Operational, Technology, Financial, Fraud
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Strategic, Regulatory, Operational, Technology
Agree	Agree	Yes	Yes	Yes	Yes	Regulatory, Operational, Fraud, Reputational
Strongly Agree	Neutral	Yes	Yes	No	Yes	Fraud, Reputational
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Strategic, Regulatory, Operational, Technology, Financial, Fraud, Reputational
Strongly Agree	Agree	Yes	Yes	Yes	Yes	Regulatory, Reputational
Strongly Agree	Agree	Yes	Yes	Yes	Yes	Regulatory, Reputational
Strongly Agree	Strongly Agree	Yes	Yes	Yes	Yes	Regulatory, Operational, Technology, Financial, Fraud, Reputational

Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15
Technology, Financial, Fraud	3-4 per year	Yes	Yearly	No	Yes	Yes	Yes
Financial	3-4 per year	Yes	Yearly	Yes	Yes	Yes	Yes
Technology, Financial, Fraud	5-6 per year	Yes	Yearly	Yes	Yes	Yes	Yes
Strategic	3-4 per year	Yes	Quarterly	Yes	Yes	Yes	Yes
Technology, Financial, Fraud	3-4 per year	Yes	Yearly	No	Yes	Yes	Yes
Technology, Fraud	1-2 per year	Yes	Yearly	No	Yes	Yes	Yes
Technology, Financial	1-2 per year	Yes	Yearly	Yes	Yes	Yes	Yes
Strategic, Technology, Financial	3-4 per year	Yes	Yearly	Yes	Yes	Yes	Yes
Technology, Financial	1-2 per year	Yes	Yearly	Yes	Yes	Yes	Yes
Strategic, Technology, Financial, Fraud	1-2 per year	Yes	Yearly	No	Yes	Yes	Yes
Technology	1-2 per year	Yes	Yearly	No	Yes	Yes	Yes
Technology	1-2 per year	Yes	Yearly	Yes	Yes	Yes	Yes
Technology, Financial, Reputational	1-2 per year	Yes	Yearly	No	Yes	Yes	Yes
Technology, Financial	1-2 per year	Yes	Yearly	Yes	Yes	Yes	Yes
Financial	1-2 per year	Yes	Yearly	Yes	Yes	Yes	Yes
Financial, Fraud	Never	Yes	Yearly	Yes	Yes	Yes	Yes
Reputational	1-2 per year	Yes	Yearly	No	Yes	Yes	Yes
Fraud, Reputational	1-2 per year	Yes	Yearly	No	Yes	Yes	Yes
Strategic, Technology, Financial	1-2 per year	Yes	Yearly	No	Yes	No	Yes

Technology, Fraud, Reputational	1-2 per year	Yes	Yearly	No	Yes	No	Yes
Strategic, Financial	1-2 per year	Yes	Yearly	Yes	Yes	Yes	Yes
Financial, Reputational	3-4 per year	Yes	Yearly	Yes	Yes	No	Yes
Financial	1-2 per year	Yes	Yearly	Yes	Yes	No	Yes
Strategic, Financial	3-4 per year	Yes	Yearly	Yes	Yes	No	Yes
Strategic, Technology, Financial, Reputational	1-2 per year	Yes	Yearly	Yes	Yes	No	Yes
Technology, Fraud	3-4 per year	Yes	Yearly	Yes	Yes	No	Yes
Technology, Financial, Fraud	1-2 per year	Yes	Yearly	No	Yes	No	Yes
Operational, Reputational	Never	Yes	Yearly	No	Yes	No	Yes
Strategic	1-2 per year	Yes	Yearly	Yes	Yes	No	Yes
Financial	1-2 per year	Yes	Yearly	Yes	Yes	No	Yes
Financial	1-2 per year	Yes	Yearly	No	Yes	No	Yes
Strategic, Financial	1-2 per year	Yes	Yearly	Yes	Yes	Yes	Yes
Reputational	3-4 per year	Yes	Yearly	Yes	Yes	Yes	Yes
Strategic, Financial	3-4 per year	Yes	Yearly	Yes	Yes	No	Yes
Strategic, Financial	1-2 per year	Yes	Yearly	Yes	Yes	No	Yes
Reputational	3-4 per year	Yes	Yearly	Yes	Yes	No	Yes
Financial, Reputational	1-2 per year	Yes	Yearly	Yes	Yes	No	Yes
Strategic, Financial, Reputational	1-2 per year	Yes	Yearly	Yes	Yes	No	Yes

Financial, Reputational	3-4 per year	Yes	Yearly	Yes	Yes	No	Yes
Strategic, Financial	1-2 per year	Yes	Yearly	Yes	Yes	No	Yes
Strategic, Technology, Reputational	3-4 per year	Yes	Yearly	Yes	Yes	No	Yes
Fraud, Reputational	1-2 per year	Yes	Yearly	Yes	Yes	No	Yes
Reputational	3-4 per year	Yes	Yearly	Yes	Yes	No	Yes
Financial, Reputational	1-2 per year	Yes	Yearly	Yes	Yes	Yes	Yes
Strategic, Technology, Fraud	1-2 per year	Yes	Yearly	Yes	Yes	No	Yes
Operational, Financial	1-2 per year	Yes	Quarterly	No	No	Yes	Yes
Strategic	1-2 per year	Yes	Yearly	Yes	Yes	No	Yes
Strategic	1-2 per year	Yes	Quarterly	Yes	Yes	Yes	Yes
Strategic	1-2 per year	Yes	Quarterly	Yes	Yes	Yes	Yes
Strategic	1-2 per year	Yes	Yearly	Yes	Yes	Yes	Yes

Q16	Q17	Q18
Yes	Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
Yes	Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
No	Agree	Yes
Yes	Strongly Agree	Yes
No	Strongly Agree	Yes

No	Strongly Agree	Yes
Yes	Agree	Yes
Yes	Strongly Agree	Yes
Yes	Agree	Yes
Yes	Agree	Yes
Yes	Agree	Yes
Yes	Strongly Agree	Yes
Yes	Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
Yes	Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes

Yes	Strongly Agree	Yes
Yes	Agree	Yes
Yes	Strongly Agree	Yes
Yes	Agree	Yes
Yes	Agree	Yes
Yes	Strongly Agree	Yes
Yes	Strongly Agree	Yes
No	Strongly Agree	Yes
Yes	Strongly Agree	Yes
Yes	Agree	Yes
Yes	Agree	Yes
Yes	Agree	Yes

PART C: Interview Questions #1

Participant: Compliance Manager and AMLCO #1

PART A: Demographics

Please tick the below

Gender: ☒Male ☐Female ☐ (Prefer not to answer)

Age:

Less than 25☐

25-35☐

36-45☐

46-55☒

56-65☐

Over 65☐

Prefer not to answer☐

Education Level: ☐Primary ☐Secondary Tertiary: ☐BSc ☒ MSc ☐PhD

Type of Business you work:

Electronic Money and Payment Institution Organization in Cyprus ☒

Level of the company's hierarchy you currently have

Front line☐

Back office☐

Middle management☒

Senior Management☐

Position within the Company: Compliance Manager and AMLCO

Work Experience in the Current Position:

Less than 1 Year☐

1 - 2 Years☐

2 - 5 Years☐

5 - 10 Years☐

Over 10 Years☒

Interview Questions #1

1. **Does your organization have a procedure manual and policies of risk management?**

   Yes, it is a regulatory requirement for EMI's to have a set of policies and procedures regarding risk management.

2. **Which are the most material risks an EMI organization faces during specific crises?**

   During crisis depending on the type and causes, always being able to continue operating is an important factor while minimizing the losses. Material risks may include operational risks and financial risks.

3. **How to manage, reduce or eliminate a possible manifestation of material risks with potential negative impacts?**

   Reducing or eliminating possible material risks and their potential negative impacts can be achieved by having policies and procedures in place which provide for such risks by having actions plans in place to manage each case and employees trained to implement these procedures.

4. **What are risk management prevention measures in use and in relation to the identified risks?**

   First is to perform a risk assessment and identify all risks the organization is facing. Based on the risk assessment to set controls and or mechanisms in order to manage those risks.

   Train employees in identifying any risks arising from their daily operations and informing the RM Unit. Have plans in place for each risk that may have a material impact in order to be ready to response avoid wasting valuable time, secure the proper level resources and work smoothly in order to overcome all obstacles.

5. **Does your organization maintain a risk register scoring the likelihood, impact and severity of potential risks that may affect business performance or obligations?**

   Yes, we have a risk register that is updated periodically or when there is a major change.

6. **Did you participate in an exercise of the business continuity plan with or without any cause? Does your company have any contingency or disaster**

recovery plan in place? How often do the employees take trainings internal or external regarding issues of risk management?

Yes at least once per year we have an emergency drill. Yes, we have a disaster recovery plan. It is part of our regulatory obligations that we have to keep up to date with the business developments. Employees take periodic trainings 3-4 times per year on various subjects depending on an annual training plan that is prepared by the risk management unit.

7. **Does your company maintain a handbook of COVID-19 pandemic available for employees? During the pandemic was you company able to continue working? Did you have any meetings or trainings against the virus?**

   Yes, part of the measures to combat the pandemic was to develop a Covid 19 handbook that will provide accurate and up to date information to all employees regarding the virus as well as instructions on how to respond on predetermine scenarios in order to avoid confusion, minimize risks and handle the situation effectively. Various meeting were taken place while implementing the social distancing, using web technologies to communicate and providing full support to all staff to continue operate as usual. These measures were proved to be important for the successful management of the pandemic crisis.

8. **How to utilize a crisis and adapt it into organizational opportunity (e.g., covid-19 vs electronic banking)**

   Sometimes during crises, opportunities arise. For example, during the pandemic people were forced to stay home. Due to that online sales were skyrocketed and the need of having an account with an EMI was even greater. EMIs offered cheap, reliable and fast payment solutions to businesses and consumers.

9. **Did risk management helped your organization to overcome a crisis event like the Covid-19 pandemic?**

   Yes, risk management played an important role. In our business continuing there was one scenario on how to deal with a pandemic. This scenario was updated by the risk management that informed the Senior Management and staff. Due to this the company was able to continue its operations without any disruptions, servicing customers while complying all regulatory obligations.

PART C: Interview Questions #2

Participant: Head of Compliance and AMLCO #2

PART A: Demographics

Please tick the below

Gender: ☒Male ☐Female ☐ (Prefer not to answer)

Age:

Less than 25☐

25-35☐

36-45☒

46-55☐

56-65☐

Over 65☐

Prefer not to answer☐

Education Level: ☐Primary ☐Secondary Tertiary: ☐BSc ☒ MSc ☐PhD

Type of Business you work:

Electronic Money and Payment Institution Organization in Cyprus ☒

Lever of the company's hierarchy you currently have

Front line☐

Back office☐

Middle management☐

Senior Management☒

Position within the Company: Head of Compliance and AMLCO

Work Experience in the Current Position:

Less than 1 Year☐

1 - 2 Years☐

2 - 5 Years☒

5 - 10 Years☐

Over 10 Years☐

Interview Questions #2

1. **Does your organization have a procedure manual and policies of risk management?**

   Yes, the company maintains a Risk Management Manual.

2. **Which are the most material risks an EMI organization faces during specific crisis?**

   With regards to specific crises, I understand that you refer to CovID-19 and not any crises. I would say that these are fraud risk, cyber-attack, failure of technology and systems/platforms used; hence the various back-up tools and mechanisms the company has put in place.

3. **How to manage, reduce or eliminate a possible manifestation of material risks with potential negative impacts?**

   The management of the company (and the Board of Directors) shall make sure that effective controls are in place in order to avoid exposure. At the same time, the risk manager (or risk committee in cases that a company does not employee a dedicated risk manager) shall perform regular assessment reviews on the risks faced by the company. In cases where any deficiencies are noted, these need to be reported and escalated to management along with relevant suggestions on how to minimize the company's exposure. The management and the board need to make sure that the suggestions on how to mitigate risks are in line with and relevant to the operations of the company and if yes, to monitor that these are implemented.

4. **What are risk management prevention measures in use and in relation to the identified risks?**

   To perform regular assessment reviews of the risk factors faced by the company based on the scale and complexity of their operations. As part of this assessment shall be to monitor the exposure of the company and evaluate if the score of each risk factor changed. If yes (either increased or decreased), to understand if this would have any impact on the company's operations. The assessment exercise shall also aim to set proper controls in place to avoid any of the risk factors actually imposing a large threat to the company that could potentially harm and/or disrupt the operations.

5. **Does your organization maintain a risk register scoring the likelihood, impact and severity of potential risks that may affect business performance or obligations?**

   Yes, we do perform the above exercise for all risks relevant to the operations of EMIs based on the guidelines published by the EBA and the obligations stemming out of PSD2.

6. **Did you participate in an exercise of the business continuity plan with or without any cause? Does your company have any contingency or disaster recovery plan in place? How often do the employees take trainings internal or external regarding issues of risk management?**

   The company does have a business continuity plan in place. The said plan is being tested at least once a year to make sure that all employees understand their responsibilities in case something (like a pandemic) may disrupt the normal way of operations. These tests also aim to check that the systems used by the company (e.g., remote connectivity, back-up servers, etc.) are correctly activated as part of the business continuity policy or disaster recovery plan.

7. **Does your company maintain a handbook of COVID-19 pandemic available for employees? During the pandemic was you company able to continue working? Did you have any meetings or trainings against the virus?**

   We do not maintain a handbook for the employees as we believe that due to our size this was not relevant. Regular updates were sent instead via emails.

   Yes, the operations of the company continued uninterrupted.

   The management took regular meetings to assess the situation based on each announcement made by the government.

8. **How to utilize a crisis and adapt it into organizational opportunity (e.g., covid-19 vs electronic banking)**

   In such situations, although it may seem that opportunities are created for the online commerce and online banking/e-wallets etc. this is not always the case. This is because the market also needs to be able to accept this change and/or something new and technologically savvy versus the traditional and conventional solutions already being used. For example, the pandemic gave rise to online shopping which in turn increased the demand of online payment processors and providers of online payment solutions

but at the same time the lockdown decreased the volumes in businesses such as travel/hotels/hospitality, taxis and licensed sports betting shops. As a result, a company's portfolio of clients shall be as diversified as possible. Nonetheless, this crisis gave opportunities and created the need for companies who operate in this industry of online payments.

9. **Did risk management helped your organization to overcome a crisis event like the Covid-19 pandemic?**

   Yes, the fact that the company had in place proper manuals and policies as well as the quick response of the management played an important role in handling the crisis and continue the operations of the company as smooth as possible.

PART C: Interview Questions #3

Participant: Executive Director #3

PART A: Demographics

Please tick the below

Gender: ☒Male ☐Female ☐ (Prefer not to answer)

Age:

Less than 25☐

25-35☐

36-45☒

46-55☐

56-65☐

Over 65☐

Prefer not to answer☐

Education Level: ☐Primary ☐Secondary Tertiary: ☐BSc ☒ MSc ☐PhD

Type of Business you work:

Electronic Money and Payment Institution Organization in Cyprus ☒

Level of the company's hierarchy you currently have

Front line☐

Back office☐

Middle management☐

Senior Management☒

Position within the Company: Executive Director

Work Experience in the Current Position:

Less than 1 Year☐

1 - 2 Years☐

2 - 5 Years☐

5 - 10 Years☒

Over 10 Years☐

Interview Questions #3

1. **Does your organization have a procedure manual and policies of risk management?**

   Yes, our institution has both AML and Risk management procedure manuals and policies since is mandatory requirement by law.

2. **Which are the most material risks an EMI organization faces during specific crisis?**

   Most material risks during a specific crisis I would say:

   - Anti-money laundering or Regulatory risk
   - Reputational risk
   - Geographical risk
   - Fraud risk
   - Operational Risk
   - Technology Risk

3. **How to manage, reduce or eliminate a possible manifestation of material risks with potential negative impacts?**

   With the use of technologies and with the right policies and procedures in place. Of course, capable personnel to observe and catch up with material risks.

4. **What are risk management prevention measures in use and in relation to the identified risks?**

   Our risk-based approach by law and risk assessment tools that give us risk categorization for each type of risk.

5. **Does your organization maintain a risk register scoring the likelihood, impact and severity of potential risks that may affect business performance or obligations?**

   Yes, in the form of risk management report which is filed annually with the Central Bank of Cyprus.

6. **Did you participate in an exercise of the business continuity plan with or without any cause? Does your company have any contingency or disaster recovery plan in place? How often do the employees take trainings internal or external regarding issues of risk management?**

Yes, I have personally participated to a business continuity exercise without any cause. Our company maintain a disaster recovery plan. The employees are taking trainings once a year.

7. **Does your company maintain a handbook of COVID-19 pandemic available for employees? During the pandemic was you company able to continue working? Did you have any meetings or trainings against the virus?**

   No, we do not maintain this kind of handbook. The company was able to continue operate normally during the pandemic. Against the virus, we had two trainings for issues relevant to the pandemic.

8. **How to utilize a crisis and adapt it into organizational opportunity (e.g., covid-19 vs electronic banking)**

   During the pandemic there was a massive shift from cash to contactless payments so we can positively say that this was an organizational or business opportunity for EMI and PI institutions.

9. **Did risk management helped your organization to overcome a crisis event like the Covid-19 pandemic?**

   Risk management is crucial and an essential department within the institution although I would not say only risk management, but the setup of the company helped to overcome the Covid 19 pandemic.

PART C: Interview Questions #4

Participant: Compliance Manager #4

PART A: Demographics

Please tick the below

Gender: ☐Male ☒Female ☐ (Prefer not to answer)

Age:

Less than 25☐

25-35☐

36-45☒

46-55☐

56-65☐

Over 65☐

Prefer not to answer☐

Education Level: ☐Primary ☐Secondary Tertiary: ☒BSc ☒ MSc ☐PhD

Type of Business you work:

Electronic Money and Payment Institution Organization in Cyprus ☒

Level of the company's hierarchy you currently have

Front line☐

Back office☐

Middle management☐

Senior Management☒

Position within the Company: Compliance Manager

Work Experience in the Current Position:

Less than 1 Year☒

1 - 2 Years☐

2 - 5 Years☐

5 - 10 Years☐

Over 10 Years☐

Interview Questions #4

1. **Does your organization have a procedure manual and policies of risk management?**

   Yes – The organization has a Risk Policy which covers the details relating to the identification, management and monitoring of risks. In view of the size and complexity of operations, EcommBX Ltd (the "Company") risk management procedures are being developed. Furthermore, it should be noted that the Company is continuously working on enhancing its risk procedures as the complexity and size of operations grow.

2. **Which are the most material risks an EMI organization faces during specific crises?**

   In view of the type of business that an EMI conducts, the risks faced are (usually) independent from crisis situations (e.g. unlike a banking institution where a financial crisis would impact credit risk). The primary source of risk for the Company, is operational risk and particularly information communication and technology risk and security risk. This particular risk stems from the fact that the Company is a fintech entity, which uses technology to operate, and thus its susceptibility to operational and ICT risk. Therefore, in view of this, the Company reviews a number of sub-risks under the ICT umbrella, including security risk.

3. **How to manage, reduce or eliminate a possible manifestation of material risks with potential negative impacts?**

   The management of risk is primarily performed through the establishment of controls. These, take the form amongst others, of policies and procedures, segregation of duties between different functions and different persons within the same functions, 4-eye review and the continuous training of all the members of staff and management.

4. **What are risk management prevention measures in use and in relation to the identified risks?**

   As noted above, the main risk management procedures that are used in the management of operational risks (incl. ICT and security risks), relate to the following:

- An appropriate organizational structure, in line with regulatory requirements has been implemented. Amongst others a relevant Risk Committee has been set up

which amongst other, ensures the appropriate and effective implementation of controls.

- An Information Security Policy and Change Management Policy has been implemented and communicated to all members of staff.
- The HR Manual documents the Code of Conduct and Code of Ethics, and identifies the way that employees need to conduct themselves.
- All personnel undergo training to be familiar with the Company's rules and regulations, including training on business conduct and information security.
- Independent assurance from the Company's internal auditor is obtained, to identify the Company's conformity to policies, practices and regulations.
- A Business Continuity Plan ("BCP") and Disaster Recovery Plan ("DRP") has been adopted.
- Penetration testing is performed on a bi-annual basis with the results being taken into consideration for any updates and system enhancements.
- All customer physical files have been scanned electronically and the original files are kept at a separate physical location away from the head office.

5. **Does your organization maintain a risk register scoring the likelihood, impact and severity of potential risks that may affect business performance or obligations?**

   Yes

6. **Did you participate in an exercise of the business continuity plan with or without any cause? Does your company have any contingency or disaster recovery plan in place? How often do the employees take trainings internal or external regarding issues of risk management?**

   Both the BCP and DRP consider the risks that the Company is subject to, however a further enhancement with the introduction a business assessment process will be undertaken, which allow for both BCP and DRP to become more risk sensitive.

   With regards to trainings, a risk management training to both Board and members of staff will be undertaken within 2021. It should be noted however that the Company's staff and management undergo trainings relevant to information security, GDRP, phishing to ensure that they remain updated on matters that may give rise to operational risk.

7. **Does your company maintain a handbook of COVID-19 pandemic available for employees? During the pandemic was you company able to continue working? Did you have any meetings or trainings against the virus?**

   No separate employee handbook is maintained for COVID-19, however information has been communicated to all employees as to the way they need to be protected against the virus. In view of the fact that the Company is a fintech entity, during the pandemic the Company continued working with no interruptions.

8. **How to utilize a crisis and adapt it into organizational opportunity (e.g., covid-19 vs electronic banking)**

   The COVID-19 events have not particularly affected the way of operations of the Company. In effect the pandemic has in fact solidified the need for technology and the need for e-banking services. To this end, the Company has utilized the learning of the crisis in designing its strategy.

9. **Did risk management helped your organization to overcome a crisis event like the Covid-19 pandemic?**

   The COVID-19 crisis has contributed to substantially changing the way everyone works and lives. In view of the heightened stress that people may feel, as a result of isolation measures there may be an increase in operational risk and specifically human resources and processes related risk. The controls that are implemented by the Company as noted above, including dual review and the 4 eye principle, the policies and procedures implemented, all contribute to ensuring that any additional risk arising as a results of the pandemic is appropriately managed.