UNIVERSITY OF LJUBLJANA
FACULTY OF ECONOMICS

MASTER’S THESIS

HOW READY ARE BANKS IN THE REPUBLIC OF KOSOVO TO IMPLEMENT AN INFORMATION SECURITY POLICY?

Ljubljana, May, 2014

FLAMUR ABDYLI

AUTHORSHIP STATEMENT

The undersigned Flamur Abdyli, a student at the University of Ljubljana, Faculty of Economics, (hereafter: FELU), declare that I am the author of the master's thesis entitled How Ready are Banks in the Republic of Kosovo to Implement an information security policy, written under supervision of Prof. Dr. Bostjan Jazbec and co-supervision of Prof. Dr. Borka Jerman Blažič.

In accordance with the Copyright and Related Rights Act (Official Gazette of the Republic of Slovenia, Nr. 21/1995 with changes and amendments), I allow the text of my master's thesis to be published on the FELU website.

I further declare:

- the text of my master's thesis to be based on the results of my own research;
- the text of my master's thesis to be language-edited and technically in adherence with the FELU's Technical Guidelines for Written Works which means that I
    - cited and / or quoted works and opinions of other authors in my master's thesis in accordance with the FELU's Technical Guidelines for Written Works and
    - obtained (and referred to in my master's thesis) all the necessary permits to use the works of other authors which are entirely (in written or graphical form) used in my text;
- to be aware of the fact that plagiarism (in written or graphical form) is a criminal offence and can be prosecuted in accordance with the Copyright and Related Rights Act (Official Gazette of the Republic of Slovenia, Nr. 21/1995 with changes and amendments);
- to be aware of the consequences a proven plagiarism charge, based on the submitted master's thesis, could have for my status at the FELU in accordance with the relevant FELU Rules on Master's Thesis.

Ljubljana, May, 2014 Author's signature: ________________________

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

INTRODUCTION

Banks will not be capable to operate in their field without accessing to their data resources. Nowadays, it is a requirement for banks to guarantee that their information resources are effectively secured against any threats. Threats toward information security take some extents including also, human vs. non-human, and accidental vs. intentional. Therefore, the protection of information is known as information security, which to a large extent will be defenceless on the behaviour of individuals inside organizations or society (Niekerk, 2010).

It is well-known that the number of employees, applications and systems increase day to day, thus the managing of the organizations information these days is much more challenging aspect due to the increase of the vulnerabilities inside the organizations. In its sense, information security is well-defined as a critical organizational plan and accomplishment, essential to mitigate the risks related with the handing out information in organizations (Wylder, 2003).

To control and protect the usage of information technology, also enabling and encouraging the employees behaviour toward daily tasks, organizations must enforce information security policies. An information security policy is a combination of principles, regulations, methodologies, techniques and tools (Tryfonas et al., 2001) established to protect the organization from threats. Facing these, an effective information security management is possible to be achieved over effective policies, standards, procedures and action plans that contribute to ensure the confidentiality, integrity and availability of information in organizations (Killmeyer, 2006).

Moreover, with this research, we can support the banking sector with a guideline or even a standard on which an information security policy shall be developed, implemented and updated. This can be done in two ways, both theoretically and practically.

The results give a general overview on what banks shall be oriented on having a proper information security policy implemented and by providing support steps on defining the policies by taking in consideration the most important factors.

Nowadays, any organization is subject to data losses, considering the global revolution that directly affects information management. Additionally, taking into consideration that organizations, respectively banks, gather information about customer profiles more than before due to business operations and advancement in technology, information security is becoming a very important issue. To prevent this, a special attention needs to be paid on formulating and implementing of an information security policy. There are different parts on formulating an information security policy that organizations nowadays need to take into consideration.

Therefore, the aim of this research is to examine the present situation in the banks regarding information security and the readiness of banks in the Republic of Kosovo to implement an information security policy with the intention to reach proper threat control. Information security is a multipart issue, and it is crucial for the sustainable development of financial institutions as information is a valuable asset, defined by the IOS[1], BS ISO 27002 (2013), which like other significant business assets, has value to a bank and therefore requires special treatment in order to be secured.

Nowadays, for banks, the importance of investments in technologies and tools has become a standard which emphases the organization future protection. However, researches advise us that this would no longer be a circumstance. The main focus of information security should be directed towards the culture and the code of conduct of the banks and the employees and their behaviour towards information security.

There are significant demonstrations that information security has an important and a crucial role for banks image and reputation by implementing a security culture towards employees, general security climate, security programmes awareness, and proper implementations of information security policies.

1 PROBLEM DESCRIPTION

After the war in Kosovo in the 1999, the banking system was totally destroyed. It took more than one year to establish the first bank with the initiative of several internationally-owned financial institutions where the implementation of latest technologies was set out as a highly priority issue. Nevertheless, the banks were mainly focused in generating fast profit and did not invest in IT systems as much as it was necessary. Moreover, due to the arrival of many international organizations to Kosovo such as KFOR[2], UNMIK[3], USAID[4], UNDP[5], OSCE[6], UNICEF[7], UNHCR[8], World Bank, World Health Organization, BRITISH COUNCIL and many others, as well as the rapid increase of the number of local businesses, the demand and the need for banks increased drastically. Currently, there are eight (8) banks operating in the Republic of Kosovo, six (6) of them being foreign banks.

[1] IOS stand for *International Organization for Standardization*

[2] KFOR stands for *Kosovo Force*

[3] UNMIK stands for *United Nations Mission in Kosovo*

[4] USAID stands for *United States Agency for International Development*

[5] UNDP stands for *United Nations Development Programme*

[6] OSCE stands for *Organization for Security and Co-operation in Europe*

[7] UNICEF stands for *United Nations Children's Fund*

[8] UNHCR stands for *United Nations High Commissioner for Refugees*

Based on these figures, it is evident that the need for a well secured and advanced information security system in the banks is more than essential for the individual development and growth of financial institutions on a competitive market. Nowadays, the banking sector has a value to customers. Therefore, the role of banks in a way is to protect client's sensitive data. The banking sector became fully aware of the risk of information leak due to the competitiveness which is constantly growing. Therefore, innovation and technology development, in particular Information Technology, nowadays provides opportunities with which banks were forced to invest more money and place greater emphasis on upgrading the internal systems and not just generate profit. With the surge of competition in the banking sector, the need for protection of sensitive information increases as well. As such, this is the reason why this research is dealing with the implementation of information security policy as an essential part of financial stability of the institution on the market.

Therefore, bank information asset can be considered any data related to the bank, and it may be, but not limited to, a single character, a message received, knowledge about a bank and its clients' data acquired through experience in the bank, data stored in removable storage, paper based files and dossiers, software developed in the bank, bank employees details, as used by the human resources department. Since information security threatens a significant part in protecting the assets of a bank, it is required that banks need to be entirely aware of the requirements for more resources in order that this aspect is to be completed properly. The results of this research will contribute to the banking sector by presenting and disseminating the real situation, and thus help them understand the relevance of securing sensitive information in the banking sector.

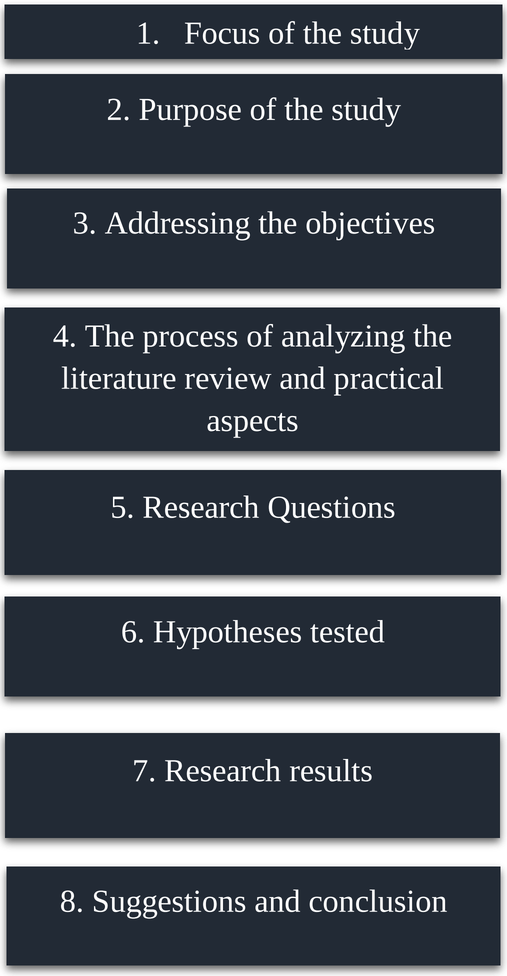
So far, this is the first research done in the Republic of Kosovo on information security, by assessing the technical and functional experience and the expertise of banks in the Republic of Kosovo regarding the willingness to invest time and money in making their systems more secure and reliable.

Moreover, one should take into account that banks' management is responsible for the appropriate set up of an adequate framework to ensure proper implementation of information security considering the fact that the banks' business and trust is largely dependent on the information used to provide services to clients.

This thesis is structured to present important stages on announcing and collecting the information that were used to build the final results. The first phase is the introduction, where the literature revision is presented with the aim to define the concept of information security and finally conclude the analysis of investigation. Then, the research methodology is presented with the strategy to introduce and discus the final results and the applied concept in daily usage. After that, we will present the main findings, analysis, and conclusions of the study and will try to discuss them in details in relation to what this research aims to offer. The thesis will end by offering recommendations for banks in the Republic of Kosovo, some suggestion for future research and some short limitations.

The framework of the thesis is outlined as in Figure 1.

Figure 1. The Outline of the Thesis


1. Focus of the study
2. Purpose of the study
3. Addressing the objectives
4. The process of analyzing the literature review and practical aspects
5. Research Questions
6. Hypotheses tested
7. Research results
8. Suggestions and conclusion

2 PURPOSE AND OBJECTIVES OF MASTER THESIS

In general, the central theme of the research is to directly examine the level of technical observation on information security with a special focus on information security policies. This will provide us information about the knowledge of banking sector employees regarding the information security in the Republic of Kosovo. This is very important as in order to have a successful implementation of the policy, the employees should have the basic knowledge about the information security.

This research will address the following objectives:

- Evaluate the ability to invest in the information security policies. The literature and research shows that these systems are usually costly;
- Define main problems the banks in the Republic of Kosovo are facing in this field. Here we will find out whether employees are ready to support the implementation of these policies;
- Evaluate the role of human factor, in our case the bank employees, in managing restricted and confidential information. This objective will focus on the past problems the banks faced and will provide us with the necessary information and knowledge in solving these problems by defining and adequate information security policy which responds to the needs of growing and steadying financial institutions.

In order to accomplish these objectives, this master's thesis will be based on the analysis of literature review and practical knowledge.

Overall, based on the results of this research, we will provide recommendations that each bank should consider in order to improve and develop a proper information security policy.

2.1 Research questions

Research questions will be organized by analysing the current situation regarding information security in the banks in the Republic of Kosovo. In order to do this, the following key hypotheses have been tested based on the research objectives to fulfil the purpose of this thesis:

Hypothesis 1: Is the banking sector in the Republic of Kosovo ready to comply with Information Security Policies?

Hypothesis 2: Are bank employees ready to comply with information security policies in the Republic of Kosovo?

3 LITERATURE REVIEW

This chapter presents the literature revision of this research, and includes historical and contemporary writing, opinions regarding the description, evaluation of the information security, organizational perspective, in this case banks, and the risks related to the information security.

3.1 Benefits of information security management

In order to open this section of the thesis, which is significant, the following subsections of the thesis will be structured on the recommendations of the ISO standards associated to information security.

Therefore ISO 27002 (2013), defines the following categories:

- Information security policy;
- Organizational security;
- Asset classification and control;
- Physical and environmental security;
- Communication and operation management;
- Aspects of business continuity management;
- Compliance with the legal requirements;
- Internal information security.

On the following subsection, we will also compare other standards other than ISO 27002 (2013).

3.1.1 What is information security?

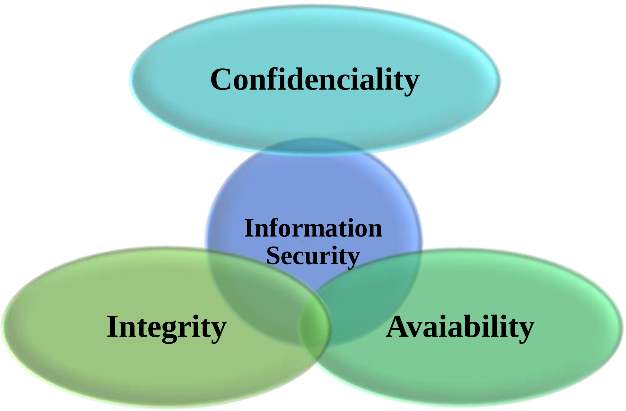
Based on ISO 27001, information is an asset that, similar to other significant business assets, is essential for a bank daily business and thus needs to be protected. As a result of this increasing interconnectivity, information nowadays is subject to a visible increase due to the technological developments and a broader change of threats and weaknesses. Therefore, in different forms, organization’s information can be hardcopy format or paper based, stored in an electronic form (ISO 27001, 2013). Further, banks need to protect their assets by setting adequate controls. Banks might also adjust to the concept that information is used to generate or control daily processes, through managing the requirements in different situations.

Moreover ISO 27001 (2013), defines that whatever the method of information holds during the processes, it must be continuously secured in a proper manner. Information security is the protection from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Different controls must to be recognized, applied, revised and upgraded with necessary methods in order to confirm that adequate security and business goals of the bank are not eluded.

Taking into consideration the security standards, such as ISO/IEC 27002, the management of information security will drive to an important level. Between the key important units that ISO/IEC 27002 consists, the part of information security policy directs the responsibilities of the employees to protect and maintain the information within banks. In general, banks shall establish information security policies within the bank. Different studies that have shown developments in information security, have reasoned that research in this field has been a subject by orienting the approach for improving the management of information security (Dhillon & Backhouse, 2001).

Figure 2: Confidentiality Integrity Availability Triangle.



Source: International Organization for Standardization, *ISO 27001*, 2013, p. 21

There are different theoretical models which treat the information security. The most well-known one is the CIA[9] triad or CIA triangle showed in Figure 2. It has been used for over 20 years as the standard of information security based on the applicability of the information, whichever involves the confidentiality, integrity and availability, ISO 27001 (2013).

Additionally, according to ISO 27002 (2013), information security includes three aspects:

[9] CIA stands for *Confidentiality, Integrity and Availability.*

- Confidentiality - relies to the safeguard of information by illegal admission regardless in what form is stored;
- Integrity - is described as the protection of information, applications, systems and networks from unauthorized change, be it intentional or accidental. Assuming that information consist integrity, this means that addressee can determine that information is in its untouchable form and it has not been changed (Laudon and Laudon 2002). If the integrity of the information is touched or changed, this means that it can also result from internal sources, within the organization (Whitman, 2009);
- Availability - is the affirmation that information, assets and resources are available only to those authorized. Consequently, information provided to the users is not allowed to be admitted, and that must be in the accurate setup (Whitman, 2009).

Confidentiality in our case is to ensure that information is available simply to those individuals who are authorized accordingly, and integrity aims to safeguard the correctness of information and processing approaches.

All the three aspects relate to safeguard the information from unapproved access, unauthorized change, be it intentional or accidental, and that assets are available only to authorized users. Moreover, these three components are concerned with the progress of all information security programmes in banks, such as information security awareness programmes. As to their submission to designing security programs, the very narrow origin of these three elements is considered a cause for concern. In the long established interpretation, these three components administer to information as data or evidence alleged on computer systems and structures where confidentiality is the prevention of unapproved disclosure, integrity is the prevention of the unauthorized change, and availability is the prevention of illegal withholding of resources (Dhillon & Backhouse, 2001).

The definition of information security policy states management’s commitment and sets out the organizations approach to managing information security. The ISO 27002 standards may be considered as guidance document by the banks for the content covered, when the information security policy are established or revised. As the information security is an important and pervasive factor of governance and managing, first thing that should be defined is establishment of the universe for evaluation, consisted of a set of controls and processes for assessing the design and operating usefulness and adeptness of information security policies.

According to ISO 27001 (2013), the management of information security policy must work in the way to support the information security according to the business needs and in compliance with the laws and central bank rules and regulations. Management review cycle should be introduced (at least once per year and trigger mechanism for updates should be established as well) that will allocate resources on the highest level (Risk Management Committee).

Based on ISACA[10] (2012), the policy document should contain:

- A definition of information security, the objectives and scope;
- An announcement of management conducted, supporting the areas and principals;
- An outline for locating the controls, by using the risk treatment plan;
- A brief description and statements of the security policies;
- A definition of overall and detailed duties and requirements for information security management;
- Any other internal organization documents which could maintain the policy; i.e. set of action plans that need to be addressed by the management of the organization.

It is important for the banks to have a written information security policy to control the procedures, actions and tools in order for the information to be safeguarded. The bank must set an administrative unit which outlines the roles and responsibilities of different participants who are in charge of implementation and monitoring various aspects of information security (Pavlov, 2011).

Furthermore, Shon elaborates that a security framework is essential in protecting the bank and its overall assets. Additionally, he defines that many banks do not follow a life cycle approach in developing, implementing and maintain their security management policy. This is because they do not know, or they feel as though this approach is cumbersome and a waste of time (Shon, 2010).

Without setting up a life cycle method to a security framework in order to maintain the internal program, an organization is doomed to treat security as merely another project (Shon, 2010).

While, Kissel (2009) states that every business needs written policies to identify acceptable practices and expectations for business operations. They need to be communicated clearly to each employee. In this case it will help the bank management to hold personnel responsible for any violation. Within banks, there should be punishments for ignoring policies and these punishments should be clearly communicated to every employee. And, those penalties should be enforced fairly and consistently for everyone in the bank that violates the information security policy.

On the other hand, according to Photopoulos (2008), the implementation process and loyalty to the proper policies will demonstrate assurance to the data, and will prove due diligence in continuing the values of the policy. Additionally, policies should be known to

[10] ISACA stands for *Information Systems Audit and Control Association.*

allow a repeatable process to attain parallel consequences for parallel responsibilities. Through distinguishing among the policy and its execution, the bank can encourage flexibility and cost-effectiveness by proposing different implementation methods to realizing the policy benefits which are as follows:

- To create clear, regular, and constant security procedures;
- To deliver bank employees the assurance that they are to accomplish their responsibilities in line with the bank's rules and regulations;
- To safeguard that the costs of security tools and controls are considered in relation to the benefits that are set by the bank management;
- To provide strong data security by a competitive advantage for banks engaging in business-to-business activity.

From the literature review and discussions, it is clear that defining and implementing the policy is a framework that banks must manage, must identify all the security risk including indicators of the effects and costs associated to risks and to evaluate by making sure appropriate protection measures are implemented for each information asset.

As a result, it seems logical to consider the lifecycle of the policy defined by excluding the planning, organizing, implementing, operating, maintaining, monitoring and evaluating.

3.1.2 What is an information security policy?

This section describes bank goals in our case and the vision related to information security, what objectives shall a bank follow and to what extent.

The objective of information security policy to a bank is to provide the management a direction and support for information security in accordance with business requirements and relevant laws and regulations (ISO 27002, 2013). While management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

In order to have controls, an information security policy document should be approved by management bodies, and published and communicated to all employees and relevant external parties. Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities (ISO 27002 2013). Policy is a high-level document that represents the bank. In order to be effective, policies must be clear and concise (ISACA, 2012).

The policy shall be considered as a must read source of information for everybody within the bank. A good security policy must define the following key fundamentals:

- In what way sensitive information must be controlled;
- By what methods a bank needs to respond to a potential security incident.

According to Ying and Mikko (2011), information security policy is an important component of a management system in an organization. Usually, the policy contains regulations on the following aspects: network, devices, data, operation, sanctions. Bank management must recognize the needs for internal or external professional information security assistance, and evaluate and coordinate results of the advice throughout the organization (ISO 27002, 2013). According to Whitman (2004), an effective security policy should consider specific organizational duties, define approved usages of the systems and tools, deliver settings for employee on reporting the known or suspected threats to the system, explain consequences meant for violations, and deliver tools to revise the information security policy on annual basis. The revision process of the information security policy must take into consideration the consequences of bank management evaluations (ISO 27001, 2013).

Based on the ISO 27001 (2013), the contribution to the management evaluation should take into account the information on:

- Advice from interested bodies;
- Consequences of self-determining reviews;
- Position of preventive and helpful activities;
- Consequences of prior management reviews;
- Process performance and information security policy compliance;
- Modifications that might disturb the banks method in handling the information security, including deviations to the organizational setting, business conditions, regulatory, and legal conditions. Overall, the security of information methods must be regularly revised (ISO 27001, 2013).

3.1.3 Organizational security of information security

This subsection will evaluate the management of information security, its components, the sectors that are involved and their roles.

Based on the ISO 27001, in order to ensure security across the organization, and to guarantee clients that the banks can be righty handed for their operations in general, security policies must be realized to take into account a lot components such as, policies and techniques that manage how the bank uses technology on daily operations, to protect and distribute information, and offer services to clients. Many businesses nowadays, especially those in financial sector, must comply with several rules and regulations for the protection and privacy of client's information in their industry. In our case, banks must be diligent in creating their information security policies to follow the local regulations, to employ risk mitigation techniques to escalate any violation.

When possible, banks are looking to automated solutions to subordinate expenditures, improve productivity, and recover the reliability of monitoring security information. Security is applied through a mixture of people, procedures, standards, processes, and technology. The automation process of information security is treaties mainly with systematizing the features of security that involve human collaboration (NIST, 2011). As automation competence or properties are added, banks may reflect increasing the monitoring process of density. Also, if resource availability declines, the banks shall consider to adjust the concerned monitoring density to confirm that security-related information is properly investigated (NIST, 2011).

3.1.4 Governor of asset classification

According to ISO 27001 (2013) standard, the objective of asset classification and control is to continue and maintain the appropriate security of organizational resources. All main information assets must stand accounted for and possess an owner. The responsibility for assets support to safeguard that proper protection is kept and continued. The owners of information shall be acknowledged for all key resources. The security classification of information assets must encounter individual businesses and operational needs and it should be treated based on the risk assessment. The accountability for applying controls may be delegated or outsourced by specialists.

The four aspects of asset classification and controls based on ISO 27001 (2013), are as follows:

3.1.4.1 Inventory of assets

Records or inventory of assets will support banks to safeguard that effective asset protection are taken into account, and which can also be an obligation for any other purposes, such as financial one. The process of gathering a catalogue of assets is a significant phase of risk management. In this case, a bank requires being able to classify the assets and the relative value of those assets.

3.1.4.2 Information classification

Information must be treated and classified in relation to legal requirements, value, and criticality to unauthorized disclosure or modification.

Ordering, sorting of information related to protective controls should take into account the daily operation needs by adding additional controls to prevent the information to be shared to unauthorized users. Assets, other than information, can also be classified in conformity with classification of information which is stored in, processed by or otherwise handled or protected by the asset.

Classification included in the banks daily operations, can be consistent and coherent across the bank. Results of classification should indicate value of assets depending on their sensitivity and criticality to the bank, i.e. in relation to confidentiality, integrity and availability. Results of classification should be updated in accordance with changes of their value, sensitivity and criticality through their lifecycle.

An example of an information confidentiality classification scheme could be based on four levels which are the following:

- Disclosure causes no harm;
- Disclosure causes minor embarrassment or minor operational inconvenience;
- Disclosure has a significant short term impact on operations or tactical objectives;
- Disclosure has a serious impact on long term strategic objectives or puts the survival of the organization at risk.

3.1.4.3 Information classification and handling

It is important for a bank, to set proper controls and measures in order to define information labelling and handling in accordance with the classification structure implemented by the bank and approved by the management. These actions require covering information assets in hardcopy and softcopy formats. For every single classification, handling measures must be well-defined to cover the following categories of information on handing activities:

- Copying;
- Storage;
- Communication through post, fax machines, and e-mailed through systems;
- Communication through spoken word, including mobile phone, voicemail, answering machines;
- Destruction methods to be applied.

3.1.5 Physical and environmental security

Based on the ISO 27002 (2013) standard, the objective of the physical and environmental security is to avoid unapproved access, loss and conflicts to business sites. Serious or sensitive business information processing facilities must be stored in protected areas, secured by a clear security limit with appropriate security barriers and entry controls. The safeguard delivered must be matching with the acknowledged risks. In this case, banks must define additional procedures in order to adopt and secure physical security.

3.1.6 Communication and operation management

Based on the IS 27001, the objective of this control is to ensure the accurate and confident procedures of information processing facilities. Accountabilities and measures for the management and operation of all information processing facilities should be defined and recognized. This may include the enlargement of proper operational instructions and incident response measures or processes. Mostly, by taking into consideration the principles and guidelines of the ISO 27001 (2013), banks can benefit on managing and defining the information security policies.

3.1.7 Information security aspects of business continuity management

Information security continuity should be embedded in the organization's business continuity management systems (ISO 27002 2013; 2013). The business continuity management process of a company or a bank is a complex process that comprises contingency planning, business continuity and recovery. An efficient management system is needed to establish and maintain such a process.

According to ISO 27001, the business continuity is to respond to disruptions to business activities and to safeguard serious business processes from the effects of key disasters. In this context, a business continuity management process should be applied to cut the interruptions in systems or daily activities caused by disasters and security failures.

According to BSI Standard 100-4 (2009), the bank management bodies must define what is understood by the term business continuity management and which tasks and competencies belong to business continuity framework. In addition, management systems such as IT management systems have generally already been set up in an organization, all areas interfacing or overlapping with information security management, building management, quality management, or risk management should be determined.

The business continuity management process consists of the following phases: initiation of business continuity management, contingency planning, and implementation of the contingency planning concept, business continuity response, tests and exercises, as well as maintenance and continuous improvement of the business continuity management process.

There should be an effective and controlled process for developing and updating the business continuity throughout the organization.

Overall, the management bodies of banks shall be responsible for setting up the appropriate framework to enable the continuity of critical processes as defined. The roles, responsibilities, competences and authorities shall be clearly defined, and persons and their substitutes shall be appointed for each role or position.

The business continuity plan should be treated in an annual basis in order to indicate how and at what time each component of the plan should be tested.

3.1.8 Internal information security policies

In order to control this aspect, it is recommended by the ISO 27002 (2013) for all information security accountabilities to be well-defined and allocated. Treatment and the need for internal policies for information security vary across organizations. Internal policies are especially useful in larger and more complex organizations where those defining and approving the expected levels of control are segregated from those implementing the controls or in situations where a policy applies to many different people or functions in the organization. Policies for information security can be issued in a single information security policy document or as a set of individual but related documents.

3.2 International information security standards

Taking into consideration that in the international Information Security field there are some international standards and guidelines which are available to help and support the organizations on management of Information Security, these standards are available to establish different rules and regulations.

Table 1: International Security Standards, Years 2001 – 2013

Standard	Description
ISO 27001 2013	The objective of the standard itself is to provide requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System.
ISO 27002 2013	The standard established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization. The standard is also intended to provide a guide for the development of organizational security standards and effective security management practices and to help build confidence in inter-organizational activities.

ISO 27003	The purpose of this development standard is to provide help and guidance in implementing an Information Security Management System,
ISO 27004	It is intended to help an organization establish the effectiveness of its Information Security Management System implementation process.
ISO 27006	Its formal title is Information technology - Security techniques**.** Requirements for bodies providing audit and certification of information security management systems and it consists of 10 chapters and four Annexes.
PCI/DSS Payment Card Industry	Payment Card Industry Data Security Standard - This standard is used to the security of clients personal information on online card transaction industry.
ITIL or ISO/IEC 2000 series	Information technology Infrastructure Library - Dwells on the service processes of IT and considers the central role of the user.
BS7799	British Standards Institute - Is a standard that was written and maintained by the British Standards Institute, and they provide comprehensive information on the standard as well as where to obtain it from. In addition. Guidelines for Information Security Risk Management. It support ISO 270010 (2013) standard and covers the main aspects for risk assessment.
BSI IT	Baseline Protection Manual - Aims to achieve a security level for IT systems and industry that is responsible and acceptable to satisfy normal protection requirements.

(table continues)
(continued)

Source: E. Moore, *Network Security: A beginner's guide Osborne,* 2001, p 13.

Moore (2001) observes that without standards that provide objective criteria for Information Security choices, Information Security experts make choices based on undeserved aspects that might include lack of knowledge, supposed constraints, inappropriate confidence and personal motivations. Table 1 depicts some of the Information Security standards.

It is recognized that standards described in the Table 1 have an important role and impact on their subject. Organizations, in our case banks, shall take into consideration the minimum of these international standards in order to have properly defined information security policies with regards to what they cover. These standards can be implemented by banks due to importance and controls set from these standards. It is recommended that internal policies defined by the banks are to be applicable and in line with these international standards. The support of the Management Board of banks is necessary on the implementation phase of these standards.

3.3 Information security formulation process

At the highest level, organizations should define an information security policy which is revised and approved by bank management and which sets out the banks' approach on handling its information security objectives (ISO 27002, 2013).

Information security policies should address some of the requirements created by:

- Business strategy;
- Regulations, legislation and contracts;
- The current and projected information security threat environment;
- The purpose of information security, goals and principles to guide all activities relating to information security;
- Processes for handling deviations and exceptions.

Whereas, based on the ISO 27001 (2013), top management shall establish an information security policy that:

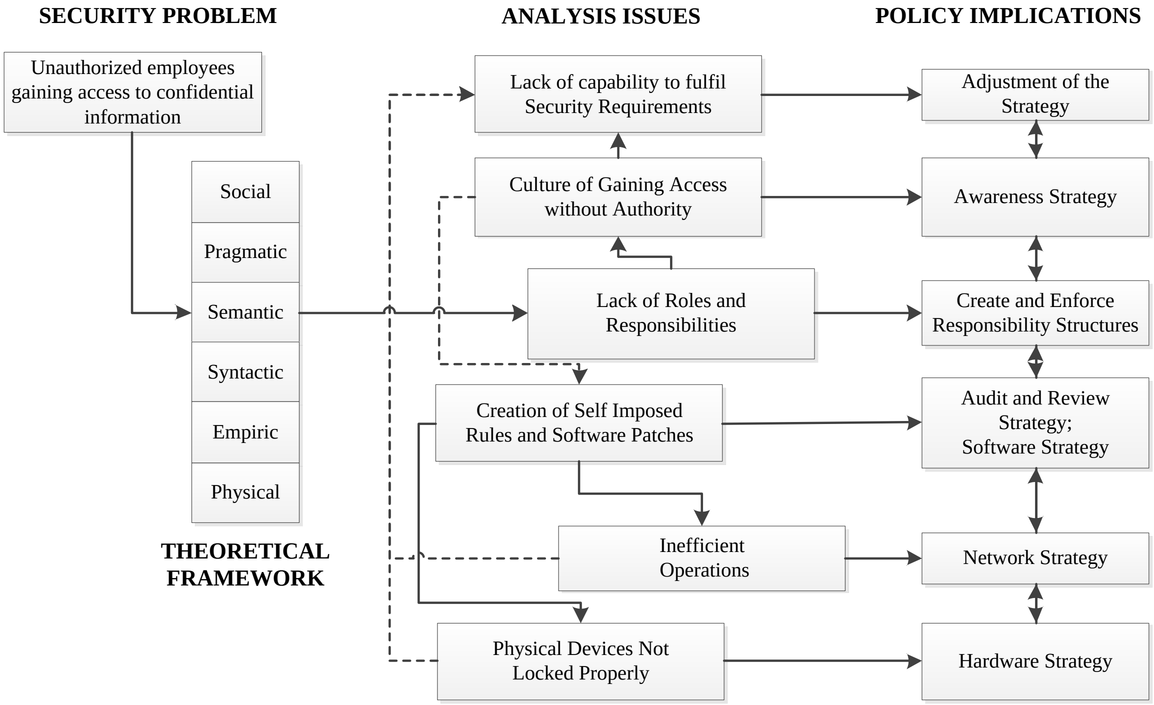
- Is applicable for the purpose of the bank;
- Consists of information security objectives (or provides the framework for setting information security objectives);
- Consists of engagement to fulfil applicable requests related to information security, and
- Includes commitment to continuous enlargement and revision of the information security management system.

At a lower level, the information security policy has to be supported by topic-specific policies, which further mandate the execution of information security tools and controls and are typically structured to address the needs of certain target groups within an organization or to cover certain topics (ISO 27002, 2013).

Moreover, the others steps towards increasing the bank's security is the overview of a detailed enforceable security policy, by informing staff on the various aspects, their responsibilities, overall use of banks resources including systems and clarifying in what way the sensitive information must be controlled and processed. Studies have shown that the policies shall describe the aspects of the meaning of acceptable use, and also by specifying the forbidden activities or actions. Basically, the main reasons behind the creation process of a security policy is to set banks information security fundamentals, to give clarifications to staff on what they are responsible to protect the information assets (Dancho, 2003).

In order to provide a clear picture of the conceptual framework, we will use the following chart to enrich security analysis and Information Security formulation, (May & Dhillon, 2010).

Figure 3: Detailed Analysis of One Tower Security Problem


SECURITY PROBLEM
ANALYSIS ISSUES
POLICY IMPLICATIONS
Unauthorized employees gaining access to confidential information
Social
Pragmatic
Semantic
Syntactic
Empiric
Physical
THEORETICAL FRAMEWORK
Lack of capability to fulfil Security Requirements
Culture of Gaining Access without Authority
Lack of Roles and Responsibilities
Creation of Self Imposed Rules and Software Patches
Inefficient Operations
Physical Devices Not Locked Properly
Adjustment of the Strategy
Awareness Strategy
Create and Enforce Responsibility Structures
Audit and Review Strategy; Software Strategy
Network Strategy
Hardware Strategy

Source: J. May & G. Dhillon, *A holistic approach for enriching information security*, 2010, p.10.

As shown in the above chart, the preliminary part for any investigation related to information security might be the theoretical framework. In order to consider this issue, the employees can retrieve confidential data in an unapproved method, thus the issue can be as such that this clearly has consequences due to a lack of a clear classification of roles and accountabilities.

For example, Figure 3 shows that a lack of roles and accountabilities can lead to a philosophy of receiving admission without the right at Tower which then provides a setting where self-imposed instructions for software patches and upgrades may be developed as dominant (May & Dhillon, 2010).

This in turn results in an environment of inefficient operations and one where physical devices are not properly secured.

Figure 3, also shows how all of these issues generated via one tower security problem then led to substantial implications for an enriched security policy. A lack of roles and responsibilities produces the need for developing a system for creating and enforcing responsibility structures of information security. (May & Dhillon, 2008).

By using this illustration, we can determine that information security policy must be formulated in a comprehensive way, which covers these arguments and addresses these important issues. From this chart, banks might find the way for the policy implications to be addressed and these implications can be important towards information security policy and employees.

Studies have shown that the information security policy accelerates the security management process and its framework. Basically, developing an IT strategy is a process that needs its management tools; therefore, in order for the approach or strategy to be effective, it must be in line with the overall business strategy, so the business departments need to be involved. Information Technology and business departments can no longer function individually. Once the arrangement between business departments and Information Technology has been accomplished and accepted, after this process is done, the bank shall initiate the defining of the information security policy (Anderson, 2002).

It is a requirement for all boundaries into the banks' IT infrastructure and systems to be inspected and standardized. Usually these boundaries will be secured through a SLA (Service Level Agreement) in the situation of an internal boundary or a Non-Disclosure Agreement should be developed and signed if the line includes a third party company (Anderson, 2002). When a bank defines the internal information security policy, a monitoring procedure for that approach can then be defined as well. Effective methods of defining the information security approach is to hold a workshop and take inputs of different stakeholders including risk management department, business departments, information technology and its infrastructure. These key stakeholders should be involved in the development process. The significance of the security approach, taking the stakeholders as an input is an acute stage in providing exact safeguard (Anderson, 2002).

3.4 Implementation of a proper information security policy and its guidelines

This part discusses issues that are important to be considered in defining the information security policy and the requirements that nowadays banks shall apply.

The International Standard ISO 27002 (2013), regarding the information security policy as an internal document, has stated that it shall have management board commitment and shall set out the banks methods and tools on handling information security. The policy might cover the following points:

- Its general purposes and scope;

- Defining the support to principles of information security in the direction with the business objectives;
- An outline that takes controls and purposes;

A brief interpretation of the security policies, values, principles and compliance requirements of specific position to the bank;

- Setting the fines of information security policy for noncompliance;
- A classification of overall and detailed duties on behalf of information security management function;
- The banks should define other detailed security procedures and standards for particular information systems and rules that bank employees should fulfil.

Madigan (2004), simplifies that policy implementation includes assuring that the guidelines of the policies are accepted by all involved persons, units within banks department, by frequently testing and controlling to see if the effective policies are being implemented properly and the employees are complying with it, and that banks shall define additional method, tools and guidelines that should include management of incidents and violation of the policy. Moreover, in relation to this issue, Sorcha (2003) clarifies that the information security policy can only be enforced by means of proper implementation, including training of the staff.

The aim of information security policies is to enforce and change the behaviours of bank personnel. According to Sorcha (2003), some principles that the banks should take into consideration in order to implement the information security policy efficiently and protect banks assets properly, regarding the policy at hand, the requirements are fitted to banks code and business operations, whereas the document should not be defined as a technical document, but it should be simple in order for the staff to be understandable, effective, and identify the responsibilities of all units.

In another perspective, to ensure that the information security policy is committed to protect the confidentiality, integrity and availability of information assets of the bank and to guarantee that regulatory and operational internal requirements are taken into consideration.

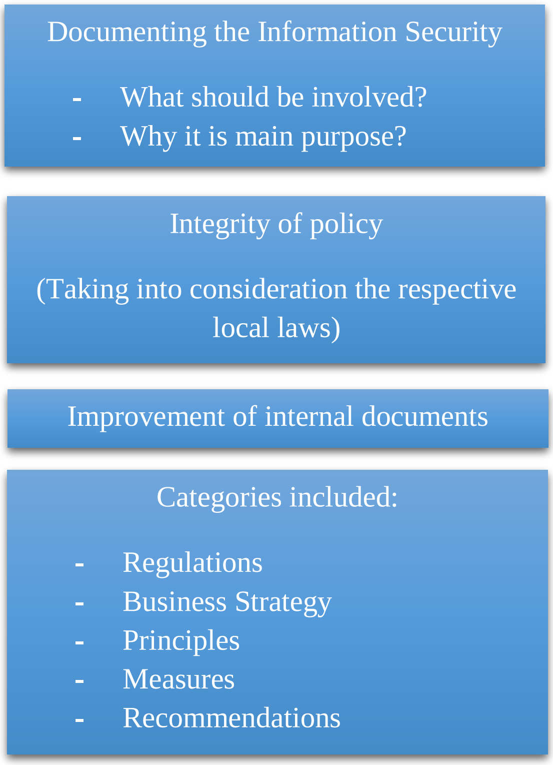
On the other hand, information security management in banks seeks to create controls and mechanisms related to security technologies to decrease the risks of the unauthorized disclosure of information (Layton, 2005).

Facing this, an effective information security management is likely to be achieved through effective policies, standards and measures that tend to safeguard the confidentiality, integrity and availability of information in banks (Killmeyer, 2006).

Studies have shown that these steps must be taken into consideration in order to have a proper information security policy. In our case, these steps will be provided to the banks as benefits in order to produce and implement an effective policy.

Danchev (2003), elaborates that at the moment when the security policy is formulated, reviewed, restructured and approved by management board, the implementation process should also be followed by information security specialists. He adds that this is typically the harder part than the establishment of the policy, due to the circumstances that the banks need to train the employees at this stage in order to perform in a confident manner. And ensuring that each of the requirements are respected. It is required that the approved version of the policy should be available to the employees that have access to bank information assets. The policy must be accessible at any time and published on the internal bank's intranet. An appropriate implementation requires also exchanging their role in the effort to protect critical bank data.

Figure 4: Flowchart for Information Security Documentation


Documenting the Information Security
- What should be involved?
- Why it is main purpose?
Integrity of policy
(Taking into consideration the respective local laws)
Improvement of internal documents
Categories included:
- Regulations
- Business Strategy
- Principles
- Measures
- Recommendations

Source: V. Etsebeth, *Legal implication of information security governance*, 2003, p. 14.

It is important to design mechanisms to ensure that in order for the people to adopt a more responsible approach to protect themselves, information security policies will need to take account of the realities of human behaviour by keeping the alternative options simple. Also, given rapid technical change, policy solutions must also be flexible and adaptable to changes in people's computing habits. Therefore, additional clarifications will essentially have to be concentrated on encouraging employees to take additional responsible point of view on the direction of assuring (Baddeley, 2011).

Basically, a flowchart for information security documentation presents some necessary steps to be taken into account while documenting a policy.
The Governance Framework includes the following parts, (King et al., 2001):

- Policies, which are developed to inform all information resources users and how the information resources should be handled and what direction executive management has set for the use of these resources;
- Standards, which are the specific compulsory rules and conventions that must be followed when handling information resources;
- Baselines, which are the minimum rules and conventions that need to be applied for the protection of information resources;
- Guidelines, which offer some recommendations on how standards are to be implemented; but are not compulsory;
- Procedures, which are the plans, steps and specification of how to go about handling information resources.

The standards, strategies and additional procedures shall establish the level and maturity of the particular discipline to be found in a bank (JTC 1/SC 27 IT Security Techniques, 2001). From the above flowchart and classifications, we can summarize that a definition of an information security policy for banks must consist a structure that contains also additional documents such as procedures, standards, manuals, instructions in order for the end user to be easier to understand its responsibilities.

The IT Governance Institute (2006) defines that information security authority creates important benefits, such as:

- Increases the value of the bank;
- Increases predictability and reduces uncertainty of business operations;
- The structure and outline improves distribution of inadequate security resources;
- Assurances of effective information security policy and compliance.

According to Straub (1990), information security policies address the integrity, availability and confidentiality of information; it is the precondition to ensure effective deterrents. Moreover, Wood (1995) policies also act as a clear statement of management intentions as well as demonstrate the fact that employees should focus at information security.

As stipulated above, the benefits of implementation of information security are related to reduction of the impact of risk. Information security can increase the bank reputation in general and self-assurance is generated from others with whom business is conducted through different channels. The information security policy must be an updated and effective document and it needs to be implemented and supported by the executive management.

3.5 Costs and values of information security policy

As stated above, information is an asset similar to other bank’s assets and has a specific value. The value of information is not fully realized until the failure occurs (SANS). Most of the organization employees take for granted the opportunity to e-mail colleagues when collaborating on projects or scheduling meetings. Only when e-mail is not available, the employees do realize the impact it has on the way they work, thus this leads to one method of determining the value of the assets, by taking it away and estimating the impact to the business if the asset will disappear, go offline or stop functioning without notice, (SANS Institute). In some cases, a less cost efficient workaround could be used instead of the usual system.

Moreover, an additional business cost or loss occurs until the functionality of the failed system of the asset is restored. According to Brecht and Nowey (2012), information security costs are defined as the period that refers to costs that are related with all types of procedures or action plans including practical as well as organizational aspects within a bank that are meant to reduce information security associated risks for its information assets.

A bank policy for information security affects an essential objection for information security specialist: determining about the ability of investing in precise technologies, considering that the market offers tools and IT equipment with several abilities (Cavusoglu et al., 2004), and determining in what way to continue and manage an effective information security policy (Dhillon, 2007).

In this field, it is really a problem for banks to take a decision on what is a good or a required type of technology. But for banks, highlighting investments in information technologies has become the model and the requirement. Safe networks, however, would not be determined by comparable technologies only, nevertheless similarly by the employees’ activities (Bulgurcu et al., 2010).

Moreover Brecht and Nowey (2012) identified four main interpretations of the term cost of information security:

In recent developments, information is important and valuable asset more than ever before. Information is important for daily business processes, meanwhile management of banks needs to be involved on making critical decisions, conduct their examination, plan the main actions, fulfil those strategies, control and follow up the progress, and finally report the results to management of the bank.

Table 2. Brief Overview of Information Security Costs, 2012

Goal	Explanation / Implications
Budgeting	Providing rules and procedures of how much a bank is ready to spent, classifying to provide internal correlation
Cost Accounting	Typically, no extraordinary method of dealing using security, the main goal is to meet compliance about financial aspects
Benchmarking	Correlation with other organizations in same market, identification of differences, pointing out not the same approaches or starting points
Risk Management	Preparation for controlling and follow up, decide on opportunities of measures
Cost-benefit-analysis of Investments/Projects	Economic valuation of specific actions/developments, return on investment analyses and the general costs of a measure
Surveys / research	Identification of tendencies, predisposition in the direction of higher/lower security costs, purpose of preferences

Source: M. Brecht and T. Nowey, *A closer look at information security costs*, 2012, p. 9

Nowadays, for banks, the availability, integrity and confidentiality of information is not at all just a business requirement as there are different legal and regulatory demands, therefore they must follow them. With the current thrust towards data protection and privacy laws, securing business data is fast becoming obligatory for banks in many countries BS ISO/IEC11 27002.

As long as the organization has information that has value, the organization will be subject to risks. The function of any information security control mechanism (technical or policies) is to control different risks to a tolerable level. Information security policies are a risk management mechanism and must consequently be planned and established in response to specific risks.

Banks nowadays have different aims and goals for measuring the costs in common and information security costs in a specific manner. Information might require different perceptions on information security costs, hence to answer the question properly, we consider that Table 2 provides a brief and important summary. Consequently, a flexible cost model is required to fulfil different difficulties by allowing various perspectives on information security costs in the organizations (Brecht & Nowey, 2012).

Table 3. Cost Categories for Information Security, 2009

Cost category	Description
Employees Costs	Includes total staff costs supporting information security units and its implementation
Hardware	Committed security hardware (e. g. security gateways, disaster recovery hardware)
Software	License costs of software committed to managing security systems and the overall IT infrastructure
Outsourcing/Managed Security Services (MSS)	Costs of monitoring and managing the security devices, systems and developments or other costs related to Managed Security Services

Source: Gartner Inc, *Cost categories for information security*, 2009, p. 17.

To shelter the costs disbursed on information security, Gartner (2009) uses a structure which is distinct among the four different costs types tabulated in Table 3.

Overall, this methodology is the first stage towards the classification of information security costs. The arrangements in hardware, software, personnel and outsourcing of

[11] BS ISO/IEC stands for *British Standard e International Organization for Standardization (ISO)*

information security costs may also be good for banks as well on conducting planning related to information security (Brecht & Nowey, 2012).

On the other hand, organizations face different difficulties on cost of information security investments so they pay on establishment and start-up of using an information security system, meanwhile it is paid once at the beginning, while the recurring cost is annual expenditure recurred to maintain the system operating. The set-up cost consists of the following costs (Lockstep, 2004, Humaigani & Dunn, 2004):

- Software;
- License fee (IT products/licensed software's);
- Hardware;
- Consultancy on analysis and configuration;
- Training of bank employees;
- Facility;

- While the regular cost is basically based on the two following costs (Lockstep, 2004; Humaigani & Dunn, 2004):
- Support and maintenance fee;
- Human resource for monitoring.

In order for the information security policies to be implemented, the budget needs to be adequate due to the large investments that should be done. Management bodies need to allocate funds in implementation phase of a policy in order to have proper security of information inside the banks. License, softwares, hardwares, trainings, implementing different controls need to be implemented to have a proper security of information, which costs.

Bjorck (2002), defines budget as the financial ability which initially assesses the costs and secondly assesses the admission required to the properties to realize proper implementation of information security. Organizations require acceptable funding (Doherty & Fulford, 2005) in order to realize adequate information security. Budgets usually depend on the method in which entities' investments translate to results, but the effect of security investment regularly depends not only on the investor's personal results but also on the decisions of others (Anderson & Moore, 2006). The lack of information on security budgeting in banks leads to under-investment in appropriate controls (Garry, 1999).

In our case, banks discover much demanded issue to define the value of information security assets and investments, primarily because an information security investment is likely to return a tangible benefit (Sonnenreich et al., 2006).

Basically, by not defining an information security policy, banks shall have financial impact, operational impact, customer related impact and employees impact due to security breaches that may come. These categories are defined into the following impacts (Xiaomeng, 2006):

- Financial impact
    - Loss of sales, preparations or agreements;
    - Loss of tangible assets within the bank;
    - Fines and legal liabilities;
    - Unexpected costs.

- Operational impact
    - Loss of management control;
    - Loss of competitiveness;
    - New ventures held up;
    - Breach of operating standards.

- Clients-related impact and control
    - Delayed deliveries to customers or clients;
    - Loss of clients;
    - Loss of confidence by key institutions;
    - Damage to reputation.

- Employee-related impact
    - Reduction in personnel motivation and productivity;
    - Injury within working hours.

In addition, it is recommended that banks should balance the investments on information security educational programmes, i.e. through providing additional investments to information security awareness programme for educating and training their employees. By providing or rising these funds in such way, security consultants might pay supplementary attention or considerations to employees in individual basis.

The contracted consultants can recognize their employees’ characters better and by considering their job description, their attitude towards their responsibilities at work, and their carefulness towards information security. Notwithstanding, security consultants might be able to recognize employees that are more motivated to participate themselves in escalating behaviour. Accordingly, security specialists can identify these employees, particularly in order to restrict them by working in an incompliance way with the banks information security policies.

3.6 Critical success factors of information security policies

There is a lack of studies on information regarding the critical success factors for information security policies, however, Sorcha, 2003; Doherty and Fulford, 2005; all derived to an agreement that recognized values, like international standard ISO 27002 2013, 2005, that they may be considered as a preliminary point for determining the information security policy to improve the information security in a bank.

Moreover, ISO 27002 (2013) presents some strategies associated to successful implementation of information security, and is mostly intended at management of a bank in order to support making decisions and then pass the essential actions to employees in management positions.

ISO 27002 (2013) standard defines some critical factors that are often critical to implement the information security in organization:

- Security policy, purposes and actions that properly follow business aims;
- A method and an outline to implement, update, monitor, and improve the information security that is consistent with the business values;
- Bank should have support from management;
- Appropriate distribution and direction on security policy to all bank employees and any third parties;
- Effective 'marketing' of security to employees (including senior and specialist employees);
- Delivery of adequate education and training to employees;
- An understanding of risk identification and risk management;
- A method to security implementation which is consistent with the banks' code of conduct;
- A broad measurement system to measure status of information security management and improve it by giving suggestions feedback.

However, a security policy cannot make a bank to reduce threats without external issues and tools that must be effective to direct the successful maintenance of the information security policy (Al-Awadi & Renaud, 2010).

By taking into consideration these factors, information security policy should be announced to all bank employees in a method that is applicable, available and clear to the end users.

3.7 Clear management commitment and support

It is recommended that bank management should support and review the policy within the bank perspective, established commitment, explicit assignment, business requirements, relevant laws and regulations, and acknowledgment of information security responsibilities (ISO 27002, 2013).

On the other hand, management needs to be sure that the information by their employees is required only to conduct their responsibilities, and is accessible only to those who need to know and use it and that the integrity is kept.

As Ed Tittel, Chapple and Stewart (2003) explain, the line managers' role is assigned to the person who is responsible for the security function maintained and who should be most worried about the safeguarding of its assets. The line manager must sign off on all policy subjects. There is no effective security policy if the line manager does not approve and support it. The line manager is the person accountable for the overall achievements or failure of a security strategy and is accountable to plan trainings in order to support the implementation.

Kajava (2006) explains that top managers often lack a proper information security understanding. This may cause them to do non-conductive decisions in order to raise the organizations security level. It has been found very important to raise the security awareness among employees. Another success factor is to raise this level among senior management. Senior Managers must assume an overall responsibility of the information security with their decisive role.

3.8 Provision of adequate education and training to staff regarding the information security

Training of bank personnel is measured as one of the methods to confirm that they are in compliance with security policies (Puhakainen & Mikko, 2010). Based on the International Standard ISO 27002 (2013), all personnel of the bank and contractors as well as the third party employees should receive proper awareness training and updates in organizational guidelines and measures, as significant factor for their job purpose. The security awareness and training events should be appropriate and relevant to the employee's job description, responsibilities and should include information to threats, who to contact for additional security guidance and the clear channels for reporting incidents.

An information security awareness programme must be established in line with the banks information security policies and relevant measures, taking into consideration the banks information to be protected and the controls that have been implemented to protect the information. The awareness programme should include a number of awareness-raising activities such as campaigns (i.e. an information security day) and issuing booklets or newsletters (ISO 27002, 2013).

Basically, employees should be provided with induction trainings when they start working for a bank and this training should be obtained regularly and evaluated properly (Wilson & Hash, 2003). These steps shall be defined in the information security policy and trainings must be mandatory to all employees.

According to ENISA[12] (2007), policies themselves are not effective and operational unless employees recognize them. The bank's security unit shall give induction trainings to all newcomers that clarify the bank's security policies. This direct communication provides employees an opportunity to discuss subjects on which they are interested in with the security unit.

Bank employees training and education in building a safe culture may influence and activate their rational manner for engaging with information security. Information security trainings are the highest accepted method to increase employee's information security performance and their activities (Puhakainen & Siponen 2010).

While it is essential that bank employees understand information security policy, the aim of training is not to just to support them to remember and understand policy over distributing to employees beyond handing them a prospect to investigate or reflect on information. An example of such security policy is the one-way spread of information to the personnel, without any response and discussion.

Gurpreet (1999) discusses that institutions need to have continuing instructions and training plans to accomplish the required consequence after the implementation of an information security policy. McKay (2003) determined that institutions are inadequate to make their personnel aware of the security concerns and the costs. The acknowledged perception is that there is a requirement to set efforts into instructing the personnel, because they will need to comply with the information security instruments and standards. Despite this, how potent the technical security supporting of the systems are, or how strict the guidelines or strategies are.

On the other hand, Ed, Mike and Michael (2003) evaluated that training is to instruct the personnel to accomplish their responsibilities and to comply with the security policy. All new personnel need certain level of training so they will be competent to comply with all principles, rules, and measures directed by the security policy.

[12] European Network and Information Security Agency.

Taking another point of view, according to Niekerk (2010), e-learning platforms must be taken into consideration for achieving all recognized requests for information security training. It can be argued that e-learning platform is the most proper distribution way for information security education accessible to institutions.

Information security education and training should take place periodically. Initial education and training applies to those who transfer to new positions or roles with substantially different information security requirements, not just to the newcomers and should take place before the role becomes active (ISO 27002, 2013).

Training curriculums are the best possible way to include video-based or instructor-led training meetings. It is significant to perform any training program interesting and up-to-date, and employee’s retention of information can be increased through repetition on annual basis.

Employees in banking sectors must be trained and educated to build a secured culture in banking sector. These trainings may influence and activate their personal thinking of processes to engage with information security policies.

3.9 Employee factor on security policies

The human factor is considered as a major issue in implementing the policies designed for security purpose. Moreover, according to Gonzalez, Jose and Agata (2002), security scheme, no matter how well planned and applied, will be dependent on bank employees. The fact that human factors play a considerable role in the common of incidents is a troubling component of recent security know-how.

Bulgurcu (2008) stated that personnel who fulfil the requirements of the information security policies are reflected as the first link of protection in regard to any security threats.

However, it seems that employees frequently establish rules of their own about implementation of information security policies. By these two cases, we can summarize that bank employees have an important role in implementing security policies.

3.10 Summary of literature review and discussion

This chapter introduced the definition and a detailed analysis of information security policy. The discussion of the existing literature evaluation in the area of information security is essential to obtain an understanding of current academic approaches and interpretations of information security, and to identify the limitations of these methods. From the review of definitions, some attributes that define information security were identified. Employees in organizations need to have considerable level of knowledge on information and at the same time the employees shall be supported on this regard by defining adequate policies.

Additionally, what have been showing from the literature review process is that there are important factors which shall be taken into account in order to achieve a proper information security policy. The costs were also discussed in a general way and presented that organizations shall have support from management basically to successfully implement an information security policy. In order to minimize the security risks, a special budget allocation must be provided by organizations.

The international information security standards were also discussed in this chapter, which recognize that a policy is very important part in an organization and therefore needs to be treated and covered form the beginning and also in different organizational internal documents such as: standards, procedures, baselines, guidelines and instructions.

Moreover, the management review cycle of information security policy should be introduced at least once per year and trigger mechanisms for updates should be established too, that will allocate resources on the highest level key committees of the banks. Inputs and outputs of the Management review on the yearly basis should be defined appropriately.

Trainings for information security are required for organization employees in order to be assured that the information security policy is implemented. In this context, it is recommended that annual tests shall be in place as an additional control that end users have recognized the policy. The chapter discusses also some subjects of characteristic plans of e-learning platform for information security that can be used for educational purposes.

The next chapter will provide a summary regarding the research methodologies.

4 RESEARCH METHODOLOGY

Nowadays, banks are interrelated using information technology, building massive prospects to grow their daily business success, whereas at the same time announcing large exposure of their key property, their information as an asset.

Considering that daily operations lead to decision-making, some regulated by information technology, there is a need to increase information security in order not to bypass important significances. This thesis pursues to deliver an understanding whether the banks are able to implement an information security policy by knowing the risk and difficulties.

Considering that the factors and international security standards in formulating and defining information security policies have been discussed, this chapter provides a description of the research methodology. It shows the methods that were preceded in this research. In addition, it follows with a description and justifies the methodology approach that was involved in this research, by starting with a general overview and presented by a comprehensive explanation of the approaches used for data grouping, the source of data and analysis model.

Regardless of how information security policies are conceptualized, there is a broad consensus in the literature as to their importance for the protection of information as well as systems and entities that operate it. Despite the significant number of studies on the topic of ISPs, until mid-2000s, the literature revealed a limited number of empirical studies on this security measure. The majority of the works in this last set of studies promoted surveys that addressed the intentions and behaviours of employees, examining factors which facilitate or inhibit compliance with information security policies.

4.1 The purpose of the research

The key focus and the principal aim of this study is evaluating and determining how ready the banks in Republic of Kosovo are to implement the information security policy and secondly, how well bank employees comply with the information security policies. The literature that was analysed was done in order to focus on the principals and international standards of implementation of the information security policy.

Moreover, this chapter describes to the reader the methodology used in this research. We will try to explain, respectively present the methods that were used in direction to verify the reliability and variability of the data composed.

In order to elaborate and address these questions, we will use two different methods:
First, a literature review considering the factors in formulating and defining information security policies.

Second, a structured questionnaire was conducted based on the literature review, and was used to identify the questions that would address the research objectives and develop the questionnaire which will be handed over to information security managers/officers and employees of the banks, and based on their responses, all the suggestions/recommendations and conclusions will be achieved.

We used the survey method to test our model. The survey was designed based on the literature revision and the contents of the international security standards, as described in the Table 2 of the previous chapter.

4.2 Research process and method

The strength of the results obtained shall offer significant implications for the research that was build. The research purposes and the approaches used in the scope of the thesis goals should be stated obviously in order to allow the reader to mark judgments on the proper choice of methodology and whether they conformed the standards (Meyrick, 2006).

The banks in the Republic of Kosovo will be surveyed for this research. Based on the current figures of the Central Bank of the Republic of Kosovo, there are eight (8) commercial banks in the Republic of Kosovo, two (2) of them are local banks and the remaining are foreign banks. The sample number of the people that will be interviewed from the local and foreign banks would be from 100-150.

Research process begins with the definition of the questionnaire which is designed according to the literature review, experience on the subject, by taking into consideration the international security standards, the critical success factors of information security and the empirical study that was expected to be filled in by bank employees.

The research process started by contacting the banks via e-mail or directly by phone to arrange meetings with the responsible staff who deal with information security. Due to the subject of this research, all employees of the banks, including management members, senior managers, heads of departments, head office staff and branches staff were planned to take the survey on a voluntary basis.

4.3 Main data collection and subject pool

The data used in this thesis were collected from questionnaires. The questionnaire was planned to be the given in hardcopy to the employees that are responsible for information security or Risk Department. The list of contact persons was retrieved from the banks' official websites or by conducting phone calls directly to people in charge. Due to sensitive issues, the questionnaire was accepted by the banks only in hard copy. We agreed for the filled questionnaires to be delivered after two weeks.

In order to accept the participation, some of the banks requested additional information as why this research is being done, thus we have arranged various number of meetings and sometimes conversation calls were used in order to convince the bank to participate on this research.

Moreover, some of the banks were able to distribute the questionnaires in time, while some of them were contacted via phone on weekly basis in order for this process to be completed. The entire process was concluded in 5 weeks. This technique of data collection method was very costly for us due to time consumption. The questionnaire is attached as Appendix A of this research.

Knowing the fact that in the Republic of Kosovo three official languages are spoken (Albanian, Serbian and English), the questionnaire was translated into these languages and was distributed to meet the rights of minority groups employed in the banks.

Meyrick (2006) elaborated that it is significant to deliver adequate awareness into the direction that was pursued from the data to the final results. The precise direction might differ from study to study but the reader must take adequate information to pursue the process and reviewer how reasonable or regular the process or steps were taken.

The questionnaire was handled to the banks in printed version due to the anonymity that the banks required to have, meanwhile, they did not support with answers in any electronic way because of the security reasons that this issue has. The designed questionnaire for the research was given to the responsible employees that are dealing with information security and they have distributed it to the bank employee.

Taking into the consideration that it was not possible to get access on the total number of employees of actual operating banks in the Republic of Kosovo, we have received 273 responses to our survey. Among these participants, respective departments of the banks informed us that all the bank employees were informed about this research, nevertheless, on a vulnerary basis.

4.3.1 Questionnaire design

The survey consists of demographics and work related questions.

Question from 1 to 9 contain the following type of questions:

- Gender;
- Age;
- Development of knowledge;
- Knowledge about IT and usage of computers;
- Usage of computers – years;
- Division in bank;
- Actual job position;
- Work experience in years;
- Work experience in the current job - in years.

These categories of questions were requested in order to understand the professional development of staff that is working in the banking industry and their experience related to Information Technology, and of course to know the rate of gender.

Question number ten (10) in the survey is about the availability of information security policies to employees in the bank, and their level of implementation. This question shall be marked from 1 to 7, and the first being the least available and seven the highest available documents amongst banks. The next question that is listed in the survey is about the documentation of information security policies in a clear and understandable manner. Moreover this question helps in understanding whether the security policies are clear to end users. Furthermore, question twelve (12) is about any particular trainings and awareness programme offered by the bank regarding information security.

4.4 Data analysis and details

The research phase begins with the questionnaire which was developed by taking into consideration the literature including international standards related to information security (Table 2: International Security Standards) review and experience in this field. The data will be presented with tables and will be analysed based on the response of respondents through questionnaires and shall provide documentation on the analysis methods.

The data analysis and outcomes will be presented in details in the following chapter.

Table 4: The Receipt Status of the Questionnaires

Response choices	**Distributed**	**Received**	**Distribution (%)**
Head Offices	120	101	84.17
Branches	200	172	86.00
Total	300	273	91.00

Table 4 indicates the results of the questionnaires distributed and received. The total number of the questionnaires that we have received is 237 or 91%, which is considered a good result for this research.

Besides that, the status gender of the respondents is presented as follows:

Table 5: The Receipt Gender of the Respondents

Gender of the respondents	Frequency	Distribution (%)
Female	112	41
Male	161	59
Total	273	100

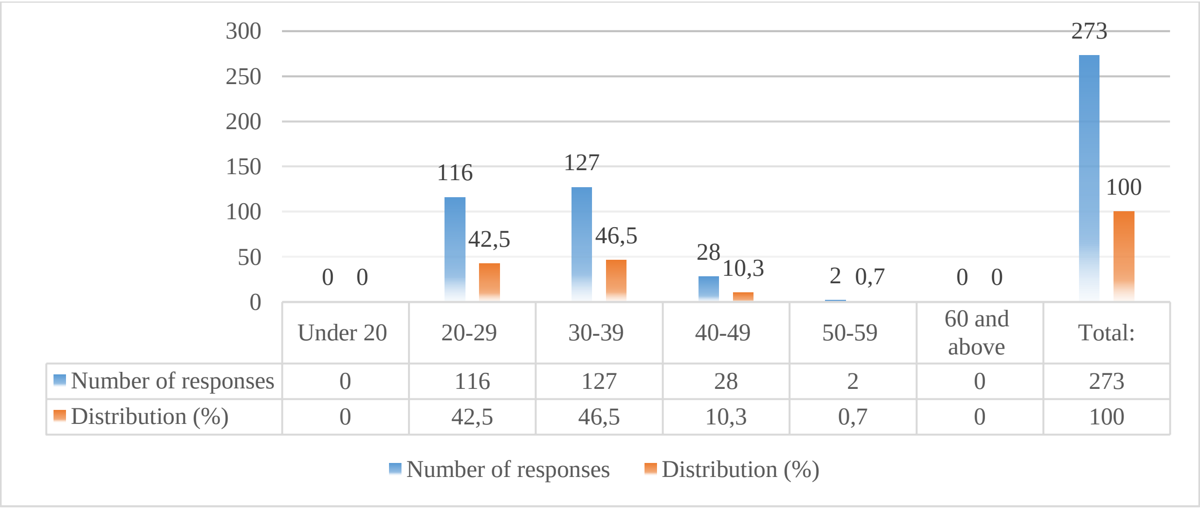
Table 5 presents the percentage distribution to female respondents which are 112 and male 161.

While the status age of the respondents is presented as follows in Table 6 and Figure 5:

Table 6: The Receipt Age of the Respondents

Response choices	Number of responses	Distribution (%)
Under 20	0	0,0
20-29	116	42,5
30-39	127	46,5
40-49	28	10,3
50-59	2	0,7
60 and above	0	0,0
Total	273	100,0

Figure 5: Status Age of the Respondents



From the information on the basis of response choice, it is interesting that on banking sector there is no employee under the age of 20, besides the age 20-29 is the first category with 42.5 present and the most common age of employees in banking sector, as indicated on Table 6, is 30-39 with 46.5 present.

The respondent's development of professional knowledge is presented in Table 8 by frequency and the distribution in percentages.

Table 7: The Receipt Development of Professional Knowledge

Response choices	Number of responses	Distribution (%)
High School Degree	33	12,1
Undergraduate Degree	166	60,8
Graduate Degree	74	27,1
Total	273	100,0

Table 7 shows that bank employees have a higher level of education which means that they can clearly support the implementation of information security policy and banks' management realize that their staff can be prepared in supporting the implementation of the policies if information security policies are developed by the banks.

In the case at hand, from the literature review one can conclude that the information security is dependent on every person included in the security process. It is hard for the banks to involve all employees in an information security training programme due to time consuming and they cannot afford the costs, therefore the education is considered costly at this stage so it is suitable to perform only online trainings. This is particularly significant if the banks demand to adopt a culture of information security.

The status of knowledge about IT and usage of computers of the respondents is presented in Table 8:

Table 8: The Status of Knowledge about IT and Usage of Computers of the Respondents

Response choices	Number of responses	Distribution (%)
Very low	1	0,4
Familiar	20	7,3
Common Understanding	204	74,7
Very high	48	17,6
Total	273	100,0

On implementation and complying with information security policies, the knowledge of staff for internal banks systems and applications should be high and should be considers as a privilege. Based on the literature review, awareness trainings must be delivered to employees when they start working for a bank and this training should be reinforced regularly on annual basis, as well as it should be properly assessed and tested. Therefore, knowledge about IT and usage of computers in this phase can be considered as an important factor for implementing such policies, due to the fact that information security policies include management of systems, user access rights, restrictions on roles towards systems. At this point, banking sector in the Republic of Kosovo can be considered to be prepared and with common understanding on IT knowledge, in our case 204 bank employees, or 74.7 percent stated that their knowledge is in a moderate level. The status of respondents on their job positions is presented as follows in Table 9:

Table 9: The Status of the Respondents about their Job Position

Response choices	Number of responses	Distribution (%)
Senior Managers	11	4,0
Middle Management	34	12,5
Coordinators/Senior Officers	25	9,2
Officers	203	74,4
Total	273	100,0

The status of the respondents about their job position that is presented in Table 9 shall be considered as a proper one due to the fact that banks are well prepared also on managerial level. Four percent of the respondents are senior managers which consist of CEOs and DCEOs, while 34 of the respondents are in middle management positions. The most common job position in banking sector is undoubtedly the officer, and that is where the banks shall organize information security trainings.

5 FINDINGS AND DATA ANALYSIS

The purpose of this section is to present the findings and data analysis based on the information that we have collected form the surveys. This part of the thesis was divided in subsections in order for the data to be more understandable and useful. The survey used in this research was fully analysed to safeguard that the data collected and it was presented clearly with the support of tables, fractions and charts, where necessary. The data are collected and processed based on the hypothesis presented in Chapter 1 of the thesis.

5.1 Hypothesis 1: Is the banking sector in the Republic of Kosovo ready to comply with information security policies?

Regarding this hypothesis, we have developed some questions from which we have collected information to prove the readiness of banks to comply with information security policies. The questions that evaluate subsequently the following hypothesis and the answer to these questions will enable us to narrate the components of the policies with the recommendations made in the literature revision with affection to the content that internal information policy should cover. This evaluation will allow the valuation of the degree to which the policies adopted by banks have been met in order to reflect the recommendations of the literature and identify the most important sets of rules that the employees must comply with.

In order to answer and evaluate the above hypothesis, some questions have been designed for this issue. The questions are designed to ask about the employee's approaches and awareness on daily tasks, their behaviour to the internal policies and the concept by which they comply. From the respondents we have collected some opinions based on the questions asked through marking questions with 1 to 7 on the Opinion Scale/Lakers scale. The answers of the questions asked that are listed in Table 10 also show the mean value, median, mode and standard deviation, by proceeding for every question raised in order to support the objective of the analysis and clarifications.

Using the information presented in the Table 10 to check the level of banks about information security policies, whether the policies are made available online, most of the employees have stated positive arguments, hence 94 per cent agreed and strongly agreed, while only 6 per cent of them do not have a positive stand about this issue. Having this data collected, it shows that banks are a step forward towards a successful implementation and complying with the information security policies.

Information security policy is a significant element of a management system in a bank nowadays. Basically, the main reason behind the creation of a security policy is to set bank information security foundations, to explain to the bank employees how they are accountable for the protection of the information of the bank.

All the following data have been calculated with Stata application.

Table 10: The Readiness Level of Banks Regarding Implementation of Information Security Policies in the Republic of Kosovo

Questions	**N**	**1 - Strongly Disagree**	**2**	**3**	**4**	**5**	**6**	**7 - Strongly Agree**
10. Information Security Are policies build accessible to employees online within the bank network?	273					16 (5.86%)	36 (13.19%)	221 (80.95%)
11. Information Security Are policies written in a method that is clear and comprehensible?	273				5 (1.85%)	15 (5.49 %)	24 (8.79%)	229 (83.88%)

12. Are you receiving by the IS supporting staff the adequate training before receiving a domain / network account?	273				3 (1.10%)	16 (5.86%)	24 (8.79%)	230 (84.25%)
13. I am conscious of the possible Information Security incidents and their harmful consequences.	273			2 (0.73%)	4 (1.47%)	17 (6.23%)	37 (13.55%)	213 (78.02%)
14. I have adequate understandings about the costs of possible security complications.	273	1 (0.37%)	3 (1.10%)	3 (4.40%)	12 (4.4%)	18 (6.59)	60 (21.9 %)	176 (64.47 %)
15. I recognize the concerns about Information Security and the risks they affect the bank.	273			1 (0.37%)	4 (1.47%)	12 (4.40%)	40 (14.65%)	216 (79.12%)
16. I know the rules and regulations defined in the information security policy in the bank.	273	1 (0.37%)	1 (0.37%)	1 (0.37%)	7 (2.56%)	22 (8.06%)	79 (28.94%)	162 (59.34%)
17. I know my responsibilities as defined in the information security policy to enhance the Information Security in the bank.	273		1 (0.37%)		4 (1.47%)	10 (3.66%)	42 (15.38%)	215 (78.75%)

Variables	**Number**	**Mean**	**Std. Dev**	**Min**	**Max**
Question 10	273	6.750916	0.5526084	5	7
Question 11	273	6.747253	0.6404285	4	7
Question 12	273	6.761905	0.6048937	4	7
Question 13	273	6.666667	0 .7242305	3	7
Question 14	273	6.395604	1.0489421	1	7
Question 15	273	6.706961	0.6546125	3	7
Question 16	273	6.417582	0.8878171	1	7
Question 17	273	6.710623	0.6645963	2	7

Following the literature revision, especially according to Whitman (2004), a tiny defined security policy must consider specific and organizational accountabilities, it should outline the authorized and unapproved uses of the systems and tools, it should provide settings for bank employees on reporting the recognized or suspected threats to the bank infrastructure, it should define consequences for violations, and it should deliver an appliance for revising and updating the security policy on annual basis. In this context, the next question listed on Table 10 demonstrates whether the policies are written in a way that are clear and comprehensible, and 93 per cent of the banking industry employees have agreed and strongly agreed, while 7 percent of them have endured impartial approach about this issue. This shows that the majority of the banks have clear and understandable policies which on the other hand make it easier to implement them.

With regards to question 12 of Table 10, bank employees have stated that 93 per cent received trainings before getting a domain account to support the staff for accessing to banks' systems and this is confirmed by them agreeing and strongly agreeing on this point. As literature has been revised, bank employees must be provided with awareness on training on annual basis when they start working for a bank and this training must be done regularly, and appropriately evaluated. For a bank, it is significant for management to set the model for IT security, by demonstrating the preferred behaviours (Wilson & Hash, 2003). In this respect, we have a strong statement which ensures that banks in the Republic of Kosovo deliver training to new-comers. And it is recommended for these steps to be defined in the information security policy and trainings must be mandatory to all employees and contractors.

Discussing question 13 of the table 8, 92 per cent of bank employees are conscious of the potential information security incidents and their undesirable significances (they agreed and strongly agreed). Therefore, by implementing security policies, banks can conduct their business electronically. Moreover, only for 8 per cent, banks must be aware. This low percentage may be considered as human error. Therefore, following the literature, banks' information security officers show a critical part in safeguarding banks information or financial data and its information assets that are properly protected, handling weaknesses within the banks infrastructure, managing incidents in impacting bank assets and educating bank employees about their responsibilities on privacy protection.

Question 14 reflects the costs if the bank employees are informed by supporting staff for the costs of security problems that may occur, while 86 per cent of employees stated that they agree and strongly agree that they have the knowledge when information incidents occur within the banks. Whereas 11 per cent have had a neutral opinion. However, 3 per cent have specified a negative opinion on this question that is considered as a disagreement. Therefore, as long as an organization has information that has value, the organization will be subject to risk, (Charl van der Walt, 2001). The function of any information security control mechanism (technical or policies) is to minimize that risk to a tolerable level. Information security policies are a risk-control tool and there is a need to be designed and established to respond to particular risks, to create an internal culture so that employees are informed regarding the inside or outside incidents.

All the above figures show that banking sector in the Republic of Kosovo is well positioned regarding the compliance of the information security policy with a mean score which presents a high level. Basically, banking sector is investing in providing understandable information security policies. It also is adopting trainings to employees to make sure that it is in compliance with the internal information security policy, and international standards on information security which can be considered as guideline of information security.

Table 10 shows also the mean score, standard deviations of each question which of course represents the values that can be considered too high, and by supporting the hypothesis that the banks in Kosovo are ready to comply with information security policies. From these figures, we can conclude that internal information policies are available to most of the employees, they are written in a manner that are clear, and address the most critical issues when staff are exposed to incidents. It is worth to mention that standard deviation of each question is highly related to each issue raised and it is considered that the level of strong agreement in most of the questions is higher.

5.2 Hypothesis 2: Are bank employees ready to comply with information security policies in the Republic of Kosovo?

In fact, to find out what the banks situation is and to go through the direction of answering this hypothesis, the following set of questions have been prepared which describe the situation.

Results show that bank employees are well informed about security issues and are supported, trained by bank supporting staff regarding the information security policies. They declare a strong agreement about training. A strong mean point is done for these questions as well.
Besides, the employees admitted that the banks treat the security policies at a higher standard, and each of them must comply with it. Therefore, bank employees comply with internal information security policy at a higher level.

Table 11: Compliance with Bank Information Security Policies

Questions	**N**	**1 - Strongly Disagree**	**2**	**3**	**4**	**5**	**6**	**7 - Strongly Agree**
18. I do comply with the information security policy in my daily job.	273			1 **(0.37%)**	1 **(0.37%)**	6 **(2.2%)**	21 **(7.69%)**	244 **(89.38%)**
19. I recommend my co-workers to support the enforced information security policy.	273	4 **(1.47%)**	2 **(0.73%)**	2 **(0.73%)**	6 **(2.2%)**	8 **(2.93%)**	27 **(9.89%)**	224 **(82.06%)**
20. Bank management considers that I must according to the information security policy of the bank	273	4 **(1.47%)**	2 **(0.73%)**	2 **(0.73%)**	6 **(2.2%)**	8 **(2.93%)**	29 **(10.62%)**	222 **(81.32%)**
21. The direct manager thinks that I should comply according to information security policy effective in the bank.	273	4 **(1.47%)**	3 **(1.10%)**	3 **(1.10%)**	8 **(2.93%)**	14 **(5.13%)**	26 **(9.52%)**	215 **(78.75%)**

22. IS supporting staff in the bank think that I should comply with enforced information security policy.	273	4 **(1.47%)**	1 **(0.37%)**	5 **(1.83%)**	7 **(2.56%)**	8 **(2.93%)**	4 **(1.47%)**	244 **(89.38%)**

(Scale from 1 to 7)

Variables	**Number**	**Mean**	**Std. Dev**	**Min**	**Max**
Question 18	273	6.85348	0.48561	3	7
Question 19	273	6.62271	1.05045	1	7
Question 20	273	6.61539	1.05129	1	7
Question 21	273	6.52747	1.15052	1	7
Question 22	273	6.67033	1.08182	1	7

As described in Table 11, the employees mostly strongly agreed on complying with information security policy. There seems to be a low number of bank employees that disagree regarding this issue. Further, 92 per cent of the respondents (who agreed and strongly agreed) have stated on complying with the information security policy in daily job, meanwhile only 7 per cent of them declared a neutral opinion.

An effort has been made through this research on seeing if the employees, bank management, supporting staff responsible for implementing information security policies endorse others to act in accordance with information security policy and as a conclusion we may say that 91 per cent of the respondents have stated a strong agreement on this direction. Further, a low percentage of the respondents (9 per cent), may be considered as disagreeing with it.

Besides this, as an overview we may conclude that banking sector employees are acting in accordance with information security policies, and the banks are considered as well prepared on this issue, which is an important factor. As literature revision has been performed in the respective paragraphs, we can summarize that information security policy is very important part and plays and critical role on banking sector and therefore it needs to be treated and covered form the beginning and also in different organizational internal forms such as: standards, procedures, baselines, guidelines and instructions.

Based on the above hypothesis, the bank employees were requested to give their opinion on the following set of questions in order to understand their perception for this issue on their daily jobs, hence if they respect/comply with information security policy. This is the core aspect of this research related to the bank employees. This set of questions will briefly determine the complying issues.

From the results of the Table 11, we can see the mean score, standard deviations of each question which of course represent the values that can be considered too high and satisfied, by supporting the hypothesis that the employees of the banks in Kosovo are ready to comply with information security policies. From these figures, we can conclude that bank employees on daily basis comply with internal policies. Further it is considered that employees are aware to comply with information security policies and that their management and supervisors are informed. It is worth to mention that standard deviation of each question is highly related to each of the issue raised and it is considered that the level of strong agreement in most of the questions is higher.

As indicated above, Table 12 presents figures that the employees are complying with information security policies implemented and enforced by the banks. Bank employees are aware by the requirements that policies set these requirements as necessary. For all questions the employees have nearly the same answers regarding compliance. Further, employees were asked regarding the complying with the information security policy which would improve protection of the resources and systems at work, and they have a feeling that the systems will be protected and misuses will be avoided. Also they have shown a strong agreement on complying with the information security policy that would minimize and eliminate the risk of damage of the used resources at work. The measures reflected through the standard deviation calculation from a high range that cover the presented arguments defined above, and which rely that the results of the responses on these questions are very strong.

Table 12: Employees Following/Respecting the Internal Information Security Policies

Questions	**N**	**1 - Strongly Disagree**	**2**	**3**	**4**	**5**	**6**	**7 - Strongly Agree**
23. I will be punished if I don't comply with the IS policy.	273	5 **(1.83%)**	7 **(2.56%)**	1 **(0.37%)**	18 **(6.59%)**	16 **(5.86%)**	43 **(15.73%)**	183 **(67.03%)**
24. For me, complying with the requirements of the IS policy is necessary.	273			1 **(0.37%)**	1 **(0.37%)**	7 **(2.56%)**	14 **(5.13%)**	250 **(91.56%)**
25. Complying with the IS policy would improve protection of my systems at work.	273	2 **(0.73%)**		5 **(1.83%)**	8 **(2.93%)**	15 **(5.49%)**	38 **(13.92%)**	205 **(75.09%)**
26. Complying with the IS policy would minimize the risk to my resources at work.	273	3 **(1.10%)**	3 **(1.10%)**	4 **(1.47%)**	7 **(2.56%)**	15 **(5.49%)**	28 **(10.26%)**	213 **(78.02%)**
27. Complying with the IS policy would lead to less security related problems associated with my systems and resources at work.	273	4 **(1.47%)**	4 **(1.47%)**	5 **(1.83%)**	9 **(3.30%)**	9 **(3.30%)**	37 **(13.55%)**	205 **(75.09%)**
28. If I don't comply with the IS policy, my resources and systems will be at risk.	273	5 **(1.83%)**	5 **(1.83%)**	5 **(1.83%)**	7 **(2.56%)**	12 **(4.40%)**	22 **(8.06%)**	217 **(79.49%)**

29. If I don’t comply with the effective IS policy, my resources/system can be misused.	273	9 **(3.30%)**	6 **(2.20%)**	5 **(1.83%)**	9 **(3.30%)**	14 **(5.13%)**	25 **(9.16%)**	205 **(75.09%)**
30. I intend and implicate to act in accordance with IS policies in the future.	273	11 **(4.03%)**			1 **(0.37%)**	2 **(0.73%)**	17 **(6.23%)**	242 **(88.64%)**
31. I intend to assist my colleagues in accordance with IS policies in the future.	273	10 **(3.66%)**	3 **(1.10%)**	1 **(0.37%)**	12 **(4.40%)**	10 **(3.66%)**	40 **(14.65%)**	197 **(72.16%)**
32. I think it is the right choice to continue working on my duties, even if I do not follow the effective IS policy.	273	239 **(87.55%)**	20 **(7.33%)**	1 **(0.37%)**	6 **(2.20%)**	5 **(1.83%)**	2 **(0.73%)**	
33. There are no risks and punishments if I break the rules of the IS policy during my work.	273	234 **(85.71%)**	21 **(7.69%)**	4 **(1.47%)**	1 **(0.37%)**	2 **(0.73%)**	4 **(1.47%)**	7 **(2.56%)**

The bank employee’s sentiment regarding the problems associated with the bank systems and resources when not acting in accordance with the information security policies is considered as a strong agreement.

(Scale from 1 to 7)

Variables	**Number**	**Mean**	**Std. Dev**	**Min**	**Max**
Question 23	273	6.27473	1.35092	1	7
Question 24	273	6.87186	0.47941	3	7
Question 25	273	6.54579	0.98831	1	7
Question 26	273	6.53114	1.11472	1	7
Question 27	273	6.46526	1.04894	1	7
Question 28	273	6.47985	1.21256	1	7
Question 29	273	6.32601	1.27784	1	7
Question 30	273	6.67033	1.47527	1	7
Question 31	273	6.35897	1.39171	1	7
Question 32	273	1.24542	0.81022	1	7
Question 33	273	1.37363	1.20032	1	7

Complying with the information security policy would lead to less security related problems associated with my systems and resources at work. The bank employees answered in very positive way for this issue by rating it with 89 per cent in agreeing with this concern. This means that bank employees understand that complying with policies will bring less security breaches in banks due to the nature of sensitivity. While for 11 per cent of bank employees, we can summarize that they have not stated a positive opinion.

Additionally, bank employees have usually specified that the aspect of not acting in accordance with the information security policy would lead for the resources and systems to be at risk. Bank employees are familiar with the risks and their opinion is very strong, the opinion concerning this issue, therefore they have rated it with 88 per cent, while the remaining points were collected from the bank employees with an opinion that is not considered as positive. Overall, this question was posed in order to see if the employees are informed about the risk associated with systems at work.

From another perspective, the respondents were asked also about the misuses of resources and systems in cases of not complying with information security policies. The respondents have a clear positive opinion by rating these issues with 85 per cent and the remaining respondents (15 per cent) can be considered as having neutral opinion.

As seen from the above table, the bank employees have mostly agreed on the question of intending to act in accordance with information security policies in the future, which can be considered as a long run fact. While, a small number (13 per cent) of bank employees have stated a negative opinion on this issue which can be considered as an indication of disagreement.

On the other hand, bank employees have been asked the following question in order to see their opinion on not complying with information security policies:

- Do you think it is the right choice to continue working on your duties, even if you do not follow the effective information security policy?

In relation to the above question, around 95 per cent of the bank employees have stated a strong disagreement or that it is not the right choice not to comply with information security policy. Further, this finding gives a strong correlation about employees complying with information security policies.

Results of Table 12 show that the average mean points on all above questions is strong, which tests the compliance with information security policies and is considered as very stable mean and can confirm the hypothesis based on the most important issues that bank employees can comply with the information security policy and that it will improve protection of the resources and systems or that complying with the information security policy would minimize and eliminate the risk of damage to employee’s resources at work.

It is worth to mention that standard deviation of each question is highly related to each issue raised and it is considered that the level of strong agreement in most of the questions is higher.

5.3 General research objectives

The research has addressed three general objectives and it can be considered that these objectives have been achieved:

- The evaluation of banks' ability to invest in information security policies. The literature and research shows that these systems may cost too much sometimes. Based on the opinions of the employees that we have been collecting, banks in Kosovo have invested a lot of effort in order for the staff to comply with policies.
- Notwithstanding, security consultants might be able to recognize the employees that are more motivated to participate themselves in escalating behaviour. Accordingly, security specialists can identify these employees particularly in order to restrict them from working in an incompliance way with the banks' information security policies. To understand the readiness of bank employees in complying with the information security policies.
- This point has shown us that bank employees are ready to support the implementation of these policies and comply with them.

Literature review has evaluated that the general objectives for information security policy are as follow, thus to:

- Safeguard compliance with existing laws, principles and rules;
- Fulfil the requirements established for confidentiality, integrity and availability;
- Create controls for protecting the information and information systems against theft, misuse and other forms of frauds;
- Encourage managers and staff to uphold the obligation for, ownership of and awareness about information security, in order to reduce the risk of security incidents;
- Safeguard the protection of personal data (privacy);
- Safeguard the availability and reliability of the system infrastructure and the services supplied;
- Meet the terms and methods of international standards for information security, i.e. ISO 27001 and 27002;
- Safeguard flexibility and an adequate level of security for gaining access to information systems.

These steps must be taken into consideration in order to have a proper information security policy. In our case, these recommendations can be taken into account by the banks in order to produce and implement and enforce information security policies.

To evaluate the role of human factor in our case, the bank employees manage restricted and confidential information within banks. Therefore, it is reasonable that if the employees comply with information security policies then the management process of classification of information meaning confidential or restricted is at a high priority. Beside this, results provide strong support that bank employees are responsive of potential information security incidents and their negative consequences that might happen due to noncompliance.

6 LIMITATIONS OF THE RESEARCH

Before concluding this research and examination, the following limitations were identified:

- The questionnaire was unable to be filled online by the banks due to the sensitivity that this research was for all banks;
- The respondents were chosen by the supporting staff of the banks that are responsible to implement the information security policies. Consequently, the data might not be one hundred percent true because the employees might feel afraid on giving or describing the real situation through the questionnaire;
- It was not acceptable from the banks to see a sample of their defined and effective information security policies due to its confidentiality;
- We are not sure if bank employees have understood and responded to the questionnaire in a fair way because they might be convinced differently by supporting staff, responsible for implementation of information security policy.

7 FINAL RESULTS AND RECOMMENDATIONS

In a digital world, as it is nowadays, especially for institutions that process and generate financial data, information has become a very important component. In this context, banks need to have a good culture and to be safe that they have implemented the internal information security policies and that bank employees comply with it.

Following the literature, information security has become an important factor in any bank, especially dealing with client data. Literature revision of this research provides fundamental understandings that the banks need an information security policy, which must be applied to all bank employees, distributed to them, and available to all employees. Policies bring many advantages to banks by protecting information from unauthorized persons and ensure that employees have appropriate access levels to the information.

In other context, if the information security policies are implemented in banks, they can be measured or mitigated by growing employees’ awareness, offering professional trainings for security tools, implementing information security tools with a level of usability that can be considered as high which can be controlled by professional experts or outsourced, adjusting time pressure, and finally by increasing awareness among all employees and bank management.

From the data collected, we can conclude that banking sector has a positive approach regarding implementing information security policies and it can be considered in a good position. The data tabularized in previous section show that bank employees have a general agreement also in complying with information security policies which is considered as the primary matter on supporting the implementation process.

As stipulated on the purpose part of this thesis, the first objective was to evaluate the ability of the banks to invest in the information security policies. In general banks in the Republic of Kosovo were ready to invest in information security due to the advantages by supporting staff with trainings, whereas the employees were ready to comply with the current policies. However, banks cannot be considered that they have accomplished to have the proper information security policies without taking into consideration the minimum criteria described below and the international security standards described in Table 1 of this paper.

Form the data collected, we can conclude that the bank employees are able to support the implementation of the information security policies which was the second objective of this thesis, because complying with it can be considered as an essential part. Additionally, it is recommended that banks' management should support the implementation of the policies, especially in cases when someone was found violating them.

Moreover a critical success factor in managing information in banking sector is the human factor. Employees must be trained about the principles of information security before getting access on any systems or resources and these trainings must be annually offered to them by being a mandatory trainings, which on the other hand can be considered as refreshment trainings. By doing this, supporting staff for implementing information security policies have the opportunity to identify bank employees that are more disposed on escalating the policies, while these employees can be found on time in order to control and monitor them.

Bank employees must be informed that in case different employees were found on misusing banks confidential information, such as employee's data, client data, internal communication documents, banks financial data etc. and in order to increase the awareness, it is recommended that banks shall ensure to regulate a process of reporting the violations of breaches of information security to the staff that is responsible for implementing information security policies.

CONCLUSION

To conclude this research and to try to answer the research question, we may conclude that banking sector in the Republic of Kosovo is ready to implement the information security policies, as the overall percentage of agreement by bank employees is considered more than 85 per cent, which can be considered as a high rate. Moreover, these empirical results suggest that the information security affects the banks in various manners therefore it is needed to undertake a careful information security management.

To further elaborate on the level of information security policies implementation in the Republic of Kosovo, it is highly suggested to conduct further studies on various aspects on this topic which were not covered in this research. Some of the questions that need to ask oneself to understand the entire picture of the information security policy in the banking sector, are:

- What are the difficulties on complying with the information security policies in banking sector?
- Does complying with information security affect the bank business operations?
- Are banks in the Republic of Kosovo ready to invest in IT infrastructures to support the implementation of information security policy?
- What are the failures of information security policy implementation, do the banks have a plan B or a recovery plan?

Consequently, we recommend that banks should focus on defining the policies by taking into consideration the commitment of the staff, which we see as a practical clarification to also enforce the readiness of complying with information security policy. On this behalf, banks can successfully redefine their information security polices by concentrating on notifying the staff that the violating of the policy is crestfallen.

The results shows that bank staff who are involved in performing sensitive tasks or dealing will sensitive information are more exposed to risks and data, therefore bank staff responsible for managing information security should take these pools as an important factor to redefine and update the information security policies. Moreover, we consider that banks should define strict sanctions when any violation is identified.

Finally, this work will contribute to the increasing knowledge on information security policy compliance in banks in the Republic of Kosovo. It has affected the problems and advantages of information security policies from a different perspective. This work will also contribute as a guideline to serve as information to security management for bank employees, and also will help them to realize the important factors of the security awareness and policy implementations.

The results and the literature revision obtained in this thesis might make some improvements in the practice of using information security policies.

To conclude, the literature revision and results of the thesis will contribute and will deliver a provision to the banks that implementing an information security is a significant way to reduce risk and to avoid any data leakage.

REFERENCES

1. Al-Awadi, M., & Renaud, K. (2010). *Success factors in information security implementation.* University of Glasgow.

2. Anderson, B. (2002). *Information security management process: Part 1 - An introduction*. Nami Trust.

3. Brecht, M., & Nowey, T. (2012). *A closer look at information security costs.* University of Regensburg.

4. British Standard ISO/IEC 27001. (2005). *Information technology — Security techniques — Code of practice for information security management.* Retrieved September 7, 2013, from http://www.bsigroup.com/en-GB/iso-27001-information-security/

5. British Standard, BS 7799-2. (2002). *Information security management systems specification with guidance for use.* Retrieved September 7, 2013, from http://www.aitel.hist.no/fag/dsh-m/lukket/lek03/fagstoff/BS-7799.pdf

6. BSI – Standard 100-1. (2008). *Information security management system (ISMS).* Retrieved September 2, 2013, from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile

7. Bulgurcu, B. (2008). *The antecedents of information security policy compliance*. University Of British Columbia.

8. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). *Information security policy compliance: An empirical study of rationality - Based beliefs and information security awareness.* MIS Quarterly.

9. Cavusoglu, H., Cavusoglu, H. & Raghunathan, S. (2004). *Economics of IT Security Management: Four improvements to current security practices, communications of the ACM.* Communications of the Association for Information Systems.

10. Charl van der Walt (2001). *Introduction to Security Policies, Part Four: A Sample Policy. Part Four.* Security Focus.

11. Central Bank of Republic of Kosovo. Retrieved December 11, 2012, from http://www.bqk-kos.org/?cid=2,1

12. Cobit Security Baseline, IT Governance Institute. (2007). *An information security survival KIT.* IT Governance Institute.

13. Dancho, D. (2003). *Building and implementing a successful information security policy. Microsoft Security.*

14. Dhillon, G. (2007). *Principles of information systems security: Text and cases.* John Wiley & Sons.

15. Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal.*

16. Doherty, N., F., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: An exploratory analysis? *Loughborough University, UK and Heather Fulford.*

17. Ed Tittel, Mike Ch., James M. S, (2003). *CISSP: Certified Information Systems Security Professional*. Symex.

18. ENISA European Network and Information Security Agency, (2006). A u*sers' guide: How to raise information security awareness*. Retrieved March 11, 2012, from http://www.enisa.europa.eu/activities/awareness-raising

19. ENISA European Network and Information Security Agency. (2007). *Information security awareness initiatives: Current practice and the measurement of success*. Retrieved March 11, 2012, from http://www.enisa.europa.eu/activities/awareness-raising

20. ENISA European Network and Information Security Agency, (2008). *The new users' guide: How to raise information security awareness*. Retrieved March 11, 2012, from http://www.enisa.europa.eu/activities/awareness-raising

21. ENISA European Network and Information Security Agency. (2009). *Information security awareness in financial organizations, guidelines and case studies.* Retrieved March 11, 2012, from http://www.enisa.europa.eu/activities/awareness-raising

22. ENISA European Network and Information Security Agency. (2009). *The growing requirement for information security awareness.* Retrieved March 11, 2012, from http://www.enisa.europa.eu/activities/awareness-raising/

23. Eric Moore, (2001). *Network Security: A beginner's guide Osborne.* McGraw-Hill.

24. Etsebeth, V. (2003). *Legal implication of information security governance*. *University of Johannesburg*. Retrieved April 12, 2012 form http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=125

25. European Central Bank, (2007). *Information security requirements*. Retrieved September 8, 2013, from http://www.ecb.int/paym/t2s/pdf/T2S_AG_meet4_requirements2.pdf

26. Gartner Inc. (2009). *Cost categories for information security.*

27. Garry D., (1999). *The Second Annual Global* Information Security *Survey*. Information Management & Computer Security

28. Gurpreet D., (1999). *Managing and controlling computer misuse*. Information Management & Computer Security.

29. Gonzalez, J., J, & Agata, S. (2002). *A framework for human factors in information security*. Department of Information and Communication Technology. *Agder University College.*

30. GTAG, (n.d). Global technology audit guide: Information technology controls. Retrieved April 12, 2012, http://www.theiia.org/bookstore/product/global-technology-audit-guide-1-information-technology-controls-1064.cfm

31. Hone, K., & Eloff, J., H., P. (2002). *What makes an effective information security policy network security.* Computers and Security. *University of Glasgow*

32. ISACA, (2012). *CISA review manual.* Retrieved April 14, 2013, from http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Prepare-for-the-Exam/Study-Materials/Pages/default.aspx

33. ISO 27002 (2013). *Information technology — Security techniques — Code of practice for information security controls.* Retrieved April 13, from http://www.iso.org/iso/catalogue_detail?csnumber=54533

34. IT Governance Institute. (2006). *Information security governance: Guidance for boards of directors and executive management*, (2nd ed). IT Governance Institute.

35. IT Standards, guidelines, and tools and techniques for audit and assurance and control professionals current (2009). Retrieved March, 13, 2013, from http://www.isaca.org

36. Kajava,J. (2006). *Exploring the use of an E-learning Environment to Enhance Information Security Awareness in a Small Company.* CIS2006

37. Killmeyer, J. (2006). *Information security architecture: An integrative approach to security in the organization*. Auerbach Publications.

38. King, C., M, Dalton, C., E., & Osmanoglu, T., E. (2001). S*ecurity architecture: Design, deployment and operations*. McGraw-Hill.

39. Kissel, K. (2009). *Small business information security: The fundamentals.* Retrieved October 1, 2012 from http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf

40. Laudon K.C. and Laudon J.P. (2002). *Management information systems*. Prentice-Hall.

41. Law on Protection of Personal Data, Official Gazette of the RKS, 03-L-172, (2010). Retrieved August 7, 2012 from http://www.kuvendikosoves.org/?cid=3,191,465

42. Layton, T. (2005). *Information security awareness: The psychology behind the technology.* Author House.

43. Li, Y., & Siponen, M. (2011). *Call for research on home users' information security behavior.* PACIS.

44. Lockstep, C. (2004). *A Guide for government agencies calculating return on security investment.* Lockstep Consulting.

45. M. Al-Humaigani and D. Dunn (2004). *A model of return on investment for information systems security.* Department of Electronics and Computer Technology,

46. MacKay (2003). *Information Theory, Inference, and Learning Algorithms.* Cambridge University Press

47. Madigan, E., M., Petrulich, C., & Motuk, K. (2004). *The cost of non-compliance when policies fail*. Proceedings of the 32nd Annual ACM SIGUCCS Conference on User Services.

48. Matthias, B., & Thomas, N. (2012). *A closer look at information security costs-working paper.* University of Regensburg.

49. May, J., & Dhillon, G. (2010). *A holistic approach for enriching information security analysis and security policy formation.* Research Paper: 18th European Conference on Information Systems.

50. Meyrick, J. (2006). *What is good qualitative research? A first step towards a comprehensive approach to judging rigor/quality*. Public Health Specialist and Research Consultant, UK.

51. Michael, A. (1996). *The underground guide to computer security*. Addison-Wesley Publishing Company Certified Information Systems Security Professional.

52. Michael, E., W., & Herbert, J., M. (2008). *Principles of information security*. Thomson Course Technology. Cengage Learning.

53. Michelle, B. (2011). *Information security: Lessons from behavioral economics.* Gonville and Caius College, University of Cambridge.

54. Niekerk, J. F. (2010). *Fostering information security culture through integrating theory and technology.* Nelson Mandela Metropolitan University.

55. NIST (2011). Information Security Continuous Monitoring (ISCM). Special Publication 800-137.

56. NIST (2006). *Information security handbook: A guide for managers*. Special Publication 800-100.

57. Puhakainen, P., & Siponen, M. (2010). *Improving employees' compliance through information systems security training: An action research study*. MIS Quarterly.

58. Puhakainen, P., & Siponen, M. (2010). *Improving employees' compliance through.* MIS Quarterly.

59. Photopoulos. C. (2008). *Managing Catastrophic Loss of Sensitive Data*. Syngress.

60. RUSecure (n.d). *Information security policies plus glossary and reference manual, securing information in the digital age*. Retrieved August 21, 2013 from http://www.eon-commerce.com/rusecure

61. Shon, H. (2010). *CISSP all-in-one exam guide.* McGraw-Hill Osborne Media.

62. Sonnenreich, W., Albanese, J. & Stout, B. (2006), *Return on security investment* (ROSI). A Practical Quantitative Model.

63. Sorcha, C. (2003). *An information security policy development guide for large companies.* SANS Institute.

64. Stewart, J, Chapple, M, & Gibson, D. (2012). *CISSP certified information systems security professional study guide*. Sybex Study Guide.

65. Straub, (1990). *Effective IS Security: An Empirical Study.* Information Systems Research.

66. Swanson, D. (n.d). *Information security, practical guidance on how to prepare successful audits.* Retrieved October 27, 2013 from http://www.itcinstitute.com

67. Tom, C. (2001). Information security management: Understanding ISO 27002. *Lucent Technologies Worldwide Services.*

68. Trustwave, SpiderLabs (2012). *WP Global Security Report*. Retrieved September 1, 2012 from http://www.trustwave.com/global-security-report

69. Tryfonas, T., Kiountouzis, E., & Poulymenakou, A. (2001). *Embedding security practices in contemporary information systems development approaches*. Information Management & Computer Security.

70. Thiagarajan, V. (2002). *Information security management, audit check list.* SANS Institute, British Standard 7799.2.

71. Verizon, Risk Team (2012). *Data breach investigations report*. Retrieved January 11, 2013, from http://securityblog.verizonbusiness.com

72. Ying Li & Mikko Siponen (2011). *A Call for research on home users' Information Security Behaviour*.

73. Whitman, M. E. (2004). In defense of the realm: Understanding the threats to Information security. *International Journal of Information Management.*

74. Wood, C. (1995) Whitening InfoSec Pollicises. *Computers and Security.*

75. Wilson, M., & Hash, J. (2003). *Computer security: Building information technology security awareness and training program. Information technology laboratory national institute of standards and technology*. Gaithersburg, MD 20899-8933.

76. Wylder, J. (2003). *Strategic information security*. Auer Bach Publications.

77. Xiaomeng, S. (2006). An overview of economic approaches to information security management. Journal of Magnetism and Magnetic Materials.

APPENDICES

LIST OF APPENDICES

APPENDIX A: LIST OF ACRONYMS

BS ISO/IEC	British Standard International Organization for Standardization/International Electro-technical Commission
IS	Information Security
ISO	Information Security Officer
ISMS	Information Security Management System
CIO	Chief Information Officer
CBK	Central Bank of Kosovo
KFOR	Kosovo Force
OSCE	Organization for Security and Cooperation in Europe's
UNMIK	United Nations Mission in Kosovo
USAID	United States Agency for International Development
UNDP	United Nations Development Programme
UNICEF	United Nations Children's Fund
UNHCR	United Nations High Commissioner for Refugees
SANS	System Administration, Networking, and Security Institute
CIA	Confidentiality, Integrity and Availability
ISACA	Information Systems Audit and Control Association
SSL	Secure Sockets Layer
IT	Information Technology
ENISA	European Network and Information Security Agency
NIST	National Institute of Standards and Technology
ITIL	Information Technology Infrastructure Library

APPENDIX B: QUESTIONNAIRE

Questionnaire: (this questionnaire was prepared to be anonymous).

Respondent's details:

1. Gender:
   a) Female;
   b) Male.
2. Age:
   a) Under 20;
   b) 20-29;
   c) 30-39;
   d) 40-49;
   e) 50-59;
   f) 60 and above.
3. Development of knowledge:
   a) High school;
   b) Undergraduate degree;
   c) Graduate degree.
4. Knowledge about IT and usage of computers:
   a) Very low;
   b) Familiar;
   c) Common understanding;
   d) Very high.
5. Usage of computers in years:
   a) 1;2;3;4;5;6;7;8;9;10;11;12;13;14;15.
   b) if other specify:________.
6. Division in Bank:
   a) Head office;
   b) Branches.
7. Actual Job Position:
   a) Senior managers;
   b) Middle management;
   c) Coordinator/seniors/specialists;
   d) Offices.
8. Work experience in years:
   c) 1;2;3;4;5;6;7;8;9;10;11;12;13;14;15.
   a) if other specify:________.
9. Work experience in current Job:

a) 1 to 10;
b) 1;2;3;4;5;6;7;8;9;10;11;12;13;14;15
c) if other specify:_________.

No.	Questions raised	1 - Strongly Disagree	2	3	4 - Neither Agree nor Disagree	5	6	7 - Strongly Agree
10	Information Security Policies are made available to employees online within the bank network?							
11	Information Security Policies are written in a manner that is clear and understandable?							
12	Are you receiving by the Information security supporting staff the adequate training before getting a domain/network account?							
13	I am aware of the potential information security incidents and their negative consequences.							
14	I have sufficient knowledge about the cost of potential security problems.							
15	I understand the concerns regarding information security and the risks they pose in the bank.							
16	I know the rules and regulations defined in the information security policy in the bank.							
17	I know my responsibilities as defined in the information security policy to enhance the information security in the bank.							
18	I do comply with the information security policy in daily job							

No.	Questions raised	1 - Strongly Disagree	2	3	4 - Neither Agree nor Disagree	5	6	7 - Strongly Agree
19	I recommend my co-workers to comply with the enforced information security policy.							
20	Bank management thinks I should comply with the information security policy of the bank.							
21	The direct manager thinks that I should comply with the information security policy effective in the bank.							
22	Information security Supporting staff in the bank thinks that I should comply with enforced information security policy.							
23	I will be punished or demoted if I don't comply with the information security policy.							
24	For me, complying with the requirements of the information security policy is necessary.							
25	Complying with the information security policy would improve protection of my resources and systems at work.							
26	Complying with the information security policy would minimize and eliminate the risk of damage to my resources at work							

No.	Questions raised	1 - Strongly Disagree	2	3	4 - Neither Agree nor Disagree	5	6	7 - Strongly Agree
27	Complying with the information security policy would lead to less security related problems associated with my systems and resources at work.							
28	If I don’t comply with the information security policy, my resources and systems will be at risk.							
29	If I don’t comply with the effective information security policy, my resources/system can be misused.							
30	I intend and implicate to comply with information security policies in the future.							
31	I intend to assist my colleagues in complying with information security policies in the future.							
32	I think it is the right choice to continue working on my duties, even if I do not follow the effective information security policy.							
33	There are no risks and punishments if I break the rules of the information security policy during my work.							

APPENDIX C: SUMMARY OF RESULTS

Question	Answers							N	Mean	Percentage distribution							Std. Dev.
	1	2	3	4	5	6	7			1	2	3	4	5	6	7	
Q10	0	0	0	0	16	36	221	**273**	**6.75**	0.00%	0.00%	0.00%	0.00%	5.86%	13.19%	80.95%	**0.55**
Q11	0	0	0	5	15	24	229	**273**	**6.75**	0.00%	0.00%	0.00%	1.83%	5.49%	8.79%	83.88%	**0.64**
Q12	0	0	0	3	16	24	230	**273**	**6.76**	0.00%	0.00%	0.00%	1.10%	5.86%	8.79%	84.25%	**0.60**
Q13	0	0	2	4	17	37	213	**273**	**6.67**	0.00%	0.00%	0.73%	1.47%	6.23%	13.55%	78.02%	**0.72**
Q14	1	3	3	12	18	60	176	**273**	**6.40**	0.37%	1.10%	1.10%	4.40%	6.59%	21.98%	64.47%	**1.05**
Q15	0	0	1	4	12	40	216	**273**	**6.71**	0.00%	0.00%	0.37%	1.47%	4.40%	14.65%	79.12%	**0.65**
Q16	1	1	1	7	22	79	162	**273**	**6.42**	0.37%	0.37%	0.37%	2.56%	8.06%	28.94%	59.34%	**0.89**
Q17	0	2	0	4	10	42	215	**273**	**6.71**	0.00%	0.73%	0.00%	1.47%	3.66%	15.38%	78.75%	**0.66**
Q18	0	0	1	1	6	21	244	**273**	**6.85**	0.00%	0.00%	0.37%	0.37%	2.20%	7.69%	89.38%	**0.49**
Q19	4	2	2	6	8	27	224	**273**	**6.62**	1.47%	0.73%	0.73%	2.20%	2.93%	9.89%	82.05%	**1.05**
Q20	4	2	2	6	8	29	222	**273**	**6.62**	1.47%	0.73%	0.73%	2.20%	2.93%	10.62%	81.32%	**1.05**
Q21	4	3	3	8	4	26	225	**273**	**6.53**	1.47%	1.10%	1.10%	2.93%	1.47%	9.52%	82.42%	**1.15**
Q22	4	1	5	7	8	4	244	**273**	**6.67**	1.47%	0.37%	1.83%	2.56%	2.93%	1.47%	89.38%	**1.08**
Q23	5	7	1	18	16	43	183	**273**	**6.27**	1.83%	2.56%	0.37%	6.59%	5.86%	15.75%	89.38%	**1.35**
Q24	0	0	1	1	7	14	250	**273**	**6.87**	0.00%	0.00%	0.37%	0.37%	2.56%	5.13%	67.03%	**0.48**
Q25	2	0	5	8	15	38	205	**273**	**6.55**	0.73%	0.00%	1.83%	2.93%	5.49%	13.92%	91.58%	**0.99**
Q26	3	3	4	7	15	28	213	**273**	**6.53**	1.10%	1.10%	1.47%	2.56%	5.49%	10.26%	75.09%	**1.11**
Q27	4	4	5	9	9	37	205	**273**	**6.47**	1.47%	1.47%	1.83%	3.30%	3.30%	13.55%	78.02%	**1.05**
Q28	5	5	5	7	12	22	217	**273**	**6.48**	1.83%	1.83%	1.83%	2.56%	4.40%	8.06%	75.09%	**1.21**
Q29	9	6	5	9	14	25	205	**273**	**6.33**	3.30%	2.20%	1.83%	3.30%	5.13%	9.16%	79.49%	**1.28**
Q30	11	0	0	1	2	17	242	**273**	**6.67**	4.03%	0.00%	0.00%	0.37%	0.73%	6.23%	75.09%	**1.48**
Q31	10	3	1	12	10	40	197	**273**	**6.36**	3.66%	1.10%	0.37%	4.40%	3.66%	14.65%	88.64%	**1.39**
Q32	239	20	1	6	5	2	0	**273**	**1.25**	87.55%	7.33%	0.37%	2.20%	1.83%	0.73%	72.16%	**0.81**
Q33	234	21	4	1	2	4	7	**273**	**1.37**	85.71%	7.69%	1.47%	0.37%	0.73%	1.47%	0.00%	**1.20**