**University of Economics, Prague**

**International Business – Central European Business Realities**


# Risk management in financial institutions with a focus on internal processes

Author: Kamran Mamedov

Thesis instructor: doc. Ing. Josef Taušer, Ph.D.

Scholar year: 2016 / 2018

**Declaration:**

I hereby declare that I am the sole author of the thesis entitled “Thesis Title“. I duly marked out all quotations. The used literature and sources are stated in the attached list of references.

In Prague on .....

Signature

Student’s name

**Acknowledgement**

I hereby wish to express my appreciation and gratitude to the supervisor of my thesis, *doc. Ing. Josef Taušer, Ph.D.*

## Content

# Introduction

Financial institutions are rather interesting and complex mechanisms that involve many different spheres – from financial service providing, marketing activities and other internal and external processes. All the processes and procedures must be in accordance with legislation of the country where this financial institution operates its business. To ensure the security and fluidity of customer services it is necessary to create strong and transparent system, which includes risk management and controlling processes.

The topic is very interesting and up-to-date, because in the financial area there are constantly changes in the legal regulations and standards that regulate this area. Continuous emphasis is placed on the transparency, fluidity and integrity of individual financial operations. Banks and other financial institutions are forced to implement increasingly complex and in-depth systems for controlling and managing individual processes, which exerts pressure primarily on risk management, controlling and compliance. New forms of fraudulent operations, which banks have to fight through established mechanisms of control and prevention, take still place.

Legal standards are also constantly updated in order to ensure greater security of internal processes in financial institutions and to ensure the financial security of clients of banking and financial institutions. An example of the current standards for financial institutions is the Basel III, PSD II and FATF regulation against money laundering and terrorism.

The thesis will deal with internal processes taking place in financial institutions, especially with emphasis on processes related to internal control and risk management. The aim of the thesis is to investigate the structure and the role of the internal audit processes in financial institutions; to analyse weaknesses and possible threats in relation to risk management, and to come up with relevant recommendations for increasing the effectiveness of internal audit processes. The partial objective will be to analyse a legal framework governing internal audit and risk management in financial institutions.

The work will be divided into four parts. The first part will define theoretical background, in particular the definition of internal control and audit in financial institutions, characterize the processes in the financial institutions in the risk management and control departments, as well as the functions of the employees of those departments.

The second chapter of the theoretical part will define a legal framework regulating the work of internal auditors, risk managers and controllers in financial institutions, and standards that must be respected and implemented by the financial institution during the provision of financial services. These are the rules of transparency of financial services provided, insurance of deposits of financial institution's clients, but also the observance of measures against the legalization of proceeds from crime and the financing of terrorism.

The practical part is a case study of VersaBank, a Canadaian financial institution. The activity of the risk management department in this financial institution will be characterized and the individual functions and competencies of the staff of this department will be defined. The main question is to find out what processes in the risk management department in the financial institution are the main ones, what are the secondary ones and how these processes are managed in a financial institution. For the purpose of revealing the information of key value to this research, the company will be investigated in detail based on the available documents and also based on the primary data obtained through an interview with its manager. The goal will be to track and reveal the current construction of the company’s risk management procedures, and their effectiveness against the existing risks and threats. Based on the findings of the research, recommendations will be developed for the company to improve its risk management procedures.

The methods of qualitative research will be used for this diploma thesis. Qualitative research will include description, characterization and analysis of processes taking place in the risk management department of the financial institution. Description will be based on the use of secondary data. Such information will include different print and electronic publications, online websites and databases. The data collected from them will be used and interpreted by the author in order to provide a comprehensive picture describing the research topic and revealing its key aspects to fulfil the stated

goals. It will also include the definition of the main functions and subordinate competencies of the staff of this department in the financial institution. The analysis includes an interview with a risk management employee in a selected financial institution to identify the main processes of their management in the risk management department and to identify the major threats to the financial institution arising from its operations.

The interview will be aimed to reveal the financial institution's risk management, and will feature groups of questions touching upon the overall organization of the internal control and monitoring system, how different departments interact for the sake of mitigating risks, the use of external auditors for identifying risks on the initial stage, regularity of checks and particular procedures applied to both internal and external actors, and finally the balance between preventive measures and measures aimed to remedy the situation.

The literature was selected for this research based on the availability of relevant information in it. For instance, the book by Bessis (2015) contains valuable theoretical information on risk management and its particular specificities in the banking sector. The publication by Hull (2015) provides extensive examples of particular financial institutions running their risk management activities, and thus this book can be used for the purpose of designing valuable recommendations for the company analysed within this research. The book by Malek (2014) provides rather more general information, but contains valuable data for understanding how ineffective risk management might affect a company's overall stability, and how this can be mitigated. Other resources to be used are abundant in valuable data as well.

# 1. Internal processes in financial institutions

## 1.1 Financial institutions: definition and specificities

In order to proceed to the analysis of financial institutions' risks and their appropriate risk management activities destined to minimize the level of risks incurred, it is worth providing a clear definition of financial institutions and to understand the specificities of their operation in the financial market.

According to Weber and Marres (2012, p. 16), a financial institution can be defined as a company providing its services in the financial market. Such services include a wide range of monetary transactions, namely deposits, loans, broker's services, investment and asset management, etc. As a results, it can be stated that financial institutions include a wide range of different companies specialized in particular segments of the financial market, namely banking institutions, trust funds, insurance companies, asset management companies, brokerage firms, investment dealers, etc. Financial institutions redistribute funds within a country's national economy, thus ensuring the most effective use of national wealth. Due to being the largest lenders, financial companies are critically important for the effective operation of real economy as a whole. Therefore, the risks incurred by financial companies affect largely the real economic sector as well.

Now, let's investigate more in detail the different types of financial institutions in order to understand the key specificities of their business activities.

Speaking broadly, all financial institutions can be divided into banks and non-bank financial institutions. Alemanno et al. (2012, p. 102) state that a bank is a financial institution which is license to raise deposits from the population and provide loans to companies and individuals. Additionally, banks might perform a range of additional activities and provide a range of additional services such as currency exchange, asset management, and so on. There are different banks responsible for different activities within a country's national economy. Thus, central banks are the issuers of national currency and regulators of the domestic financial market in general. They set the rules

for all licensed banking institutions. Commercial banks are those banks which are involved directly in deposit-and-loan activities with the population and the corporate sector. Commercial banks gain profits on the difference in the rates of interest on deposits paid to customers and on loans paid by customers to banks. Investment banks are specific banks focusing on the provision of services such as underwriting and asset management. All in all, it can be stated that banks play an important role in providing the national economy with growth prospects, as they ensure the redistribution of funds within the economy.

As stated by Kazandziska (2011, p. 16), a non-bank financial institutions is a company running its activities in the financial market, but without having a banking license or without being regulated by financial authorities. Non-bank financial institutions differ from banks by the range of services they offer. For instance, non-bank financial institutions are involved mainly in services such as brokerage, investment and consulting, insurance, risk pooling, and so on. They thus do not act for the purpose of gaining profits on the difference between the interest rates on deposits and loans, but rather earn on the fees drawn from their customers for services. Examples of non-bank financial institutions include insurance companies, currency exchange outlets, brokerage and financial consulting firms, and so on.

Herr and Kazandziska (2011, p. 16) further note that in liberal and democratic countries, the activities of non-bank financial institutions are not regulated as tightly as commercial banks: "*Non-bank financial institutions are – partly, but not only as a result of laxer regulation – more risk- and speculation-oriented than commercial banks. They can use very high leverage to finance their activities.*" The services of non-bank financial institutions are becoming more and more popular as of today, particularly thanks to the development of online and digital technologies, which make the access to such services significantly easier for all persons with Internet access all over the world. However, due to the less strict regulation on the part of central authorities, the risks of transaction with non-bank financial institutions tend to be considerably higher compared to commercial banks.

Madura (2008, p. 16) states that in present time, the global economy cannot function without financial institutions, as they allow maximizing the effectiveness of economic exchange, supporting the entire global infrastructure of cashless payment and

ensuring the multiplier effect for monetary emission on global scale. The services of financial institutions are used virtually by everyone around the globe, from companies and various organizations to households and individuals who use debit cards for paying purchases at stores, transfer money to their friends, buy goods online, and so on. The steady development of technologies contributes to the growing ease of the use of financial institutions' services. At the same time, this also raises the risks of using such services, as the transactions with financial institutions are targeted by fraudsters, and are also vulnerable to a great number of other risks.

Now, having analyzed the main concepts associated with financial institutions and their market activities, in the next chapter of the thesis, the functions of financial institutions will be analyzed in detail.

## 1.2 Functions of financial institutions

The functions of financial institutions describe those key tasks which financial institutions perform within their market activities, and ways in which they serve the interests of communities, thus contributing to the growth of economic wealth. In literature, there can be found different approaches to the classification of financial institutions' functions, and thus different options of describing those functions. However, based on an analysis of available bibliographic sources, we can point out the following most important functions of financial institutions.

1. Preservation of financial wealth

As noted by Taussig (2013, p. 325), by providing deposit services, financial institutions offer their customers to deposit funds with an aim of generating return in the form of interest. Thus, the population gets an opportunity to put its excessive wealth to banks, so as to make the money work and earn income. This type of use of own funds is less risky than investment, provided that the bank is reputable and follows the appropriate standards of safety and risk management. Thanks to the fact that money starts providing interest income, people might reduce significantly or eliminate at all the negative effects associated with inflation. As a result, there is a preservation of wealth against negative external factors and conditions. In the long run, people get greater wealth which they can manage at their own discretion.

2. Redistribution of funds

Booth (204, p. 8) states that as financial institutions accept funds from individual and need to repay interest income in addition to returning deposit principal amount, financial institutions thus need to make this money work and to bring profits, which would not only allow covering all costs, but also procuring a profit margin sufficient for making banks' activities sufficiently effective. The most obvious way to do this is to carry out lending activities and deliver loan facilities to the corporate sector, other individuals, and governments. Banks set their own rates on loans, which are higher than the rates on deposits, and they provide funds to borrowers who thereafter have to repay the principal amount of loan and interest on it. This process leads to the fact that companies which do not have sufficient funds to finance their activities, raise borrowed capital from banks, and therefore get an opportunity to raise the effectiveness of their market activities. The redistribution of funds allows raising the effectiveness of how funds are used in national economy, as financial institutions collect those resources which have been idle lately, and use them for boosting economic growth through lending mechanisms, as borrowers use such funds for their economic growth. In the long run, this leads to overall increased economic output, greater opportunities enjoyed by local manufacturers, and thus overall higher standards of living and opportunities for the entire population of the country.

3. Stimulation of accumulation of funds in national economy

Taussig (2013, p. 325) states that as financial institutions act based on the scheme described above, they provide people with options of how they can manage their funds and how they can operate their income for raising the social standards of their living. This is important not only for individuals who can thus raise their wealth, but also for the national economy as a whole: without financial institutions, people would be incited to spend their funds for different purchases. The use of such funds would lead to the greater monetary mass freely available, and thus to overheating of the economy. As banks and other financial institutions collect a part of such funds from the population, they prevent this money from being spent and from triggering overheating of economy. This helps improving the financial situation for the long-term perspective, thus improving the overall social standards of the population's living, and also minimizing possible expenditures to be borne by the state.

4. Mediation in settlements and payments

According to Alemanno et al. (2012, p. 102), banks ensure the performance of payments by both individuals and companies, which are carried out through bank accounts. Non-bank financial institutions are becoming more and more popular as of today thanks to the opportunities which they offer in terms of convenient money transfers. It is worth noting in particular here transactions involving cryptocurrencies, which have seen major surge in recent years. Electronic payments can be accessed by people from virtually anywhere around the globe, and the quality of such transactions tends to keep steadily rising. As a result, financial institutions ensure the greatest customer convenience in everyday transactions, and at the same time they contribute to the decreasing share of cash payments, which impact positively the global economy.

5. Control and transparency

Alemanno et al. (2012, p. 102) state that all cashless transactions carried out via most financial institutions, either bank or non-bank, can be monitored effectively by public authorities. This lowers the risks of tax evasion by individuals and companies, and provides the tax authorities with more effective levers of control over the operations carried out by business within the state. Furthermore, this also lead to greater transparency in the transactions between different actors, which contributes significantly to organic business growth achieved by economic actors. In the long run, this allows for the most effective target use of funds by both the government and all other economic actors within the state, thanks to which the economy may operate more effectively.

6. Consultancy and spreading of information

Lone (2016, p. 23) states that as financial institutions' services include the provision of information, one of their functions is the increase in the level of the population's financial literacy, and the provision of opportunities for companies to plan and perform better their market activities. As financial institutions have the access to the freshest and most relevant financial information, they are able not only to anticipate the trends to prevail in the financial market, but also affect to a large extent the expectations of their customers, and thus the activities which the customers would undertake in the light of the existing conditions and factors. The spreading of information by banks thus

has direct effects on the overall behavior of the population, and on the circulation of funds within the national economy.

Therefore, based on the information states above, it can be concluded unequivocally that financial institutions perform a wide range of functions, which are of essential importance to the effective operation of the economy. Without financial institutions, the real economic sector would not have enough funds to boost its growth, and thus this would have major adverse conditions for the population, the corporate sector, and the government. However, despite the positive effects which financial institutions bring to the economy, it should also be borne in mind that such institutions collect funds from the population and operate such large amounts, this inadvertently entails significant risks, which should be taken into account. In the next chapter of the thesis, such risks will be analyzed more in detail.

## 1.3 Definition and types of risks incurred by financial institutions

Due to the specificities of their activities, financial companies incur a great number of risks in the course of their business operations. Such risks are created from both the external and the internal environment, and in aggregate, they represent a considerable threat to financial institution's effective performance. Below, the main risks incurred by financial institutions will be analysed.

1. Credit risk

According to Joseph (2006, p. 31), credit risk can be defined as "*the probability of loss (due to non-recovery) emanating from the credit extended, as a result of the non-fulfilment of contractual obligations arising from unwillingness or inability of the counter-party or for any other reason.*" Therefore, to put it briefly, credit risk stands for the risk that the borrower might not repay a loan, and that the financial institution as the lender might lose the principal amount of the loan and the interest due on the loan, thus suffering financial losses. Credit risk arises in those situations when borrowers plan to repay their current loans at the expect of future proceeds. Due to the fact that the economic market is undergoing constant and often adverse changes, the financial institution can never be fully confident in the customer's repayment of the loan. As a result, it bears credit risk. The compensation for incurring this type of risk is the amount

of interest to be received by the financial institution as an income. Wise policies ensure a situation in which expected profits from interest are sufficient for covering possible non-repayments of loans on the part of customers.

Koulafetis (2017, p. 2) states that credit risk is most often connected with the borrower's insolvency or bankruptcy. Insolvency describes a situation in which the borrower's liabilities are greater than its assets, and it thus doesn't have source sufficient for covering its liabilities. Bankruptcy refers to a situation in which the borrower's insolvency is recognized legally, and external administration is established to govern the borrower's business activities. Upon bankruptcy, the value of the borrower's assets goes further down, which only worsens the financial institution's credit risk. The actual repayment of the loan in this situation is thus preconditioned by the priority of the repayment of loans set by the borrower's external administration.

Christoffersen (2011, p. 277) states that the assessment of credit risk a hard task for companies, as it involves many different factors which precondition the risks that the borrower would not repay the loan raised from the financial institution. Most often, a necessary procedure for financial institutions includes the assessment of the customer's credit history, current loans taken either from this particular financial institution or from any other in the market, detailed analysis of financial statements in order to reveal the availability of sources to cover the liabilities to the creditor and the borrower's equity and its historical dynamics.

Finally, according to Koulafetis (2017, p. 2), it should be noted that credit risk is interconnected tightly with the interest rate set for the particular loan facility. Thus, the higher credit risk, the higher the interest rate set by the financial institution on the loans it delivers to customers. This is due to the fact that the level of perceived risk preconditions directly the lender's desire to protect itself against possible losses due to the non-repayment of the loan by the borrower. At the same time, each loan facility's actual credit risk is often evaluated by financial institutions against the borrower's credit rating, and therefore this process may be quite individual and customized for each particular borrower.

2. Market risk

According to Scandizzo (2016, p. 109), market risk can be defined as *"the risk of an increase or decrease in the market price of a financial instrument or portfolio, due to changes in stock prices, interest rates, credit spreads, foreign exchange rates, commodity prices, implied volatilities."* Therefore, based on this definition, it can be stated that in contrast to credit risk which is incurred by financial institutions in association with possible non-repayment on the part of the borrower, market risk isn't associated with possible issues of any borrower, but is connected with the overall dynamics of the financial market and possible unfavourable conditions formed for the financial institution in the external environment. The degree of control over such external dynamics on the part of the financial institution is even smaller compared to credit risk.

As market risk is associated with negative financial market dynamics, there might be different underlying factors preconditioning the aforesaid negative situations. Thus, market risk comprises a great number of smaller risks. Interest rate risk is associated with growing volatility due to unfavourable changes in interest rates. As interest on loans might be the main source of revenue for financial institutions, any negative scenarios affect directly the level of expected profits. Another component of market risk is equity price risk. Negative changes in the price of securities or portfolio affect significantly the financial institution's market position and financial stability. Moreover, negative equity price dynamics can be either systematic or unsystematic, the former being caused by global market factors, and the latter being caused by situational factors which can be mitigated through diversification.

Next, market risk also includes foreign exchange risk. This also commonly referred to as currency risk. According to Levi (2007, p. 191), foreign exchange risk is "*related to the variability of domestic-currency values of assets or liabilities due to unanticipated changes in exchange rates, whereas foreign exchange exposure is the amount that is at risk.*" Negative dynamics of the national currency's exchange rate can be preconditioned by the vector of economic policies chosen by the government, insufficient economic power to maintain the currency's rate, negative external shocks, and a great number of other factors beyond the financial institution's control. Such negative dynamics affect directly the level of profits generated by the financial institution, and also make it review and re-consider its policies.

Scandizzo (2016, p. 109) emphasizes that the prevision of market risk is harder compared to credit risk, as it implies the need to take into account a great number of factors. Forecasting and planning associated with market risk requires the financial institution to run thorough market analysis, so as to reveal the abundance of factors which might have negative impact on the financial institution's performance in the periods to come. The mitigation of risks against negative external dynamics is particularly important for financial organizations due to the very limited scope of control over such scenarios on the part of companies.

3. Operational risk

As defined by Chaudhuri and Ghosh (2015, p. 2) based on the Basel Committee, operational risk is "*the risk of direct or indirect loss resulting from inadequate or failed internal processes, people or systems or from external events.*" This definition of operational risk comprises legal risk, but doesn't include strategic and reputational risk. In financial institutions, a major source of operational risk is most often errors in human-led operations. For instance, this might include incorrectly stated amounts of funds, improper information processing, leaking of information to any third parties, as well as various system failures and programming errors. Therefore, it can be stated that in contrast to previous risks, operational risk is associated rather with the organization and its internal flaws than with any external factors. As a result, the financial institution can have quite a significant degree of influence on operational risk, and the effectiveness of the construction of all internal processes preconditions directly its possible outcomes.

Grinsven (2009, p. 6) states that operation risk does not necessarily mean the company's failure, even though it might entail financial losses. However, operational risk contributes directly to the firm's growing internal costs. The assessment of operational risk within financial institutions is based first of all on thorough audit and control, so as to reveal the organization's weaker part and so as to reveal in which aspects of its activities the most urgent corrective measures are required for avoiding further negative consequences for its business.

4. Liquidity risk

According to Vento and La Torre (2006, p. 76), liquidity risk can be defined as "*the risk arising from changes in cash flow… as the risk of not having enough cash to meet obligations, as well as the price or the opportunity cost or loss to bear in order to obtain cash.*" The risk of liquidity thus arises when the financial institution is unable to convert its current assets quickly into cash so as to cover its current liabilities. There might be different reasons for this situation, but quite often, this is due to mismanagement and ineffective planning. When planning its expectations regarding future periods, the financial institution needs to evaluate effective not only the expected income might get, but also the expected costs, taking into consideration effectively all deadlines and maturity periods. The most effective option for financial institution is to ensure an effective management of their cash flows, so as to avoid major losses in cases when they need to cover their liabilities.

5. Reputational risk

As noted by Chesini (2017, p. 114), reputational risk can be defined as "*the risk of economic losses associated with a negative image of the bank by the clients, supervisors, regulators, and the public.*" Reputational risk is thus a hidden danger. It doesn't exist per se, and is provoked by ineffective market activities led by the financial institution, which in the long run cause dissatisfaction on the part of its customers. Reputational risks can be cause by virtually any actions. For instance, they can be caused by insufficient prudence in market operations, customers' dissatisfaction with the quality of customer support, or even by ineffective or improper market activities led by partners. As a result of this, reputational risk is hard to forecast and also often hard to control. Most often, companies wishing to minimize its possible negative impact need to fulfil due damage control procedures and establish effective communication with target customers, so as to ensure an effective bilateral exchange of information.

6. Systemic risk

Fouque and Langsam (2013, p. 20) define systemic risk as "*the risk that financial instability becomes so widespread that it impairs the functioning of the financial system to the point where economic growth and welfare suffer materially*." Systemic risk can be provoked by either endogenous or exogenous factors. A classic example of systemic risk is the 2008 global financial and economic crisis where

systemic risk was one of the main factors contributing to the development of the crisis events. Some financial corporations are so large that their failure represents significant risks for the entire global financial sector. The failure of any such company inadvertently leads to the consequent cascade-like failure of other financial institutions, and this brings major damage not only to the financial sector itself, but also to the real economic sector.

7. Business risk

According to Huang and Kahraman (2013, p. 505), business risk can be defined as "*the level of exposure to uncertainties that the enterprise must understand and effectively manage as it executes its strategies to achieve its business objectives and create value*." In the context of financial institutions, the business risk is the risk that the losses of such companies will be greater than their revenues, and the risk that the financial institution's forecasting in the course of business planning would in the long run be ineffective or insufficient for covering the possible effects of dangers.

Therefore, based on the information presented above, it can be stated that financial institutions incur a great number of different risks in the course of their activities. This entails the need for them to take into account all those risks effectively in their business policies and to respond to them correspondingly and adequately with particular measures. In the next chapter of the thesis, the main specificities of risk management in financial institutions will be considered more in detail.

## 1.4 Specificities of risk management in financial institutions

According to Broder and Tucker (2011, p. 91), risk management can be defined as *"the process by which an entity identifies its potential losses and then decides what is the best way to manage these potential losses."* Risk management thus stands for the identification and elimination of risks which a company incurs in the course of its activities for the purpose of ensuring its effective business performance and guaranteeing the achievement of the desired business results.

The specificities of risk management in financial institutions are preconditioned by the specificities of financial institutions' business outlined earlier in this thesis.

Banks and non-bank financial institutions operate large amounts of funds, and have strict time delays to be met in the course of their interaction with customers. Furthermore, banks use different forms and methods of money relationships with their customers, and this entails appropriate risks which financial institutions have to comply with.

Mok and Saha (2017, p. 3) state that after the 2008 global financial and economic crisis *"Regulators have been pushing institutions to formalize capital-planning and stress-testing procedures for many years to help ensure their ability to weather future events."* After the global crisis which had brought to light the deficiencies and vulnerabilities of the global financial sector, large financial institutions started using a strategic approach to risk management, within which the risk management procedures are implemented in an integrated manner throughout all business departments and business processes, and more conservative strategies are implemented for the sake of achieving the desired results in the market, instead of pursuing high short-term profits which imply greater risks. Against the background of globalization, the role of strategic risk management in financial institutions should only be expected to keep growing in the future, and therefore the effectiveness of companies' risk management procedures will be of major importance to the construction of internal processes for the years to come.

Mok and Saha (2017, pp. 5-9) note that the procedures of risk management in financial institutions as of today are implemented in a cyclical manner, where all stages are intertwined and add to each other's importance. The initial stage is the review of strategic risks and planning in the course of development of the financial company's market strategy. The failure to take into account the impending risks on the preliminary stage of the financial institution's market activities is a considerable shortcoming which might have major negative effects for the company in the future. Therefore, risk review is set to reveal the main risks which the financial institution might face, and planning is set to foresee the most effective ways to respond to such risks and to minimize their potential negative impact on the company, thus adapting the company to the conditions of the external environment.

In the course of business activities, the financial institution needs to keep investigating the current dynamics of all risk factors in the market, and the possible

impact of such dynamics on the company's activities. Mok and Saha (2017, p. 8) note that trend analysis, scenario planning and assumptions testing constitute an important part of risk management activities on this stage. This can often be performed with the involvement of third-party experts and specialists. The ultimate goal of such ongoing risk management activities is to understand how risks are changing on a particular time interval, and thus develop responsive operational measures which would allow responding effectively to the impending threats. On the last stage, when the financial institution evaluates its financial performance, the results should be tested against the initial assumptions done by the responsible risk managers, and the follow-up procedures are set to reveal to which extent the company was able to foresee and react effectively to the threats endangering its business success.

According to Bock (2010, p. 10), financial institutions' risk management policies encompass a broad range of actors which need to be taken into consideration. Thus, first of all, financial institutions need to evaluate the amount of funds available to them and the expected liabilities to be borne in relation to third parties. Thereafter, appropriate provisions are made for covering possible losses, and schedules are designed for meeting the liabilities to depositors of funds against the repayment of loans on the part of borrowers. Such liabilities are partially imposed on financial institutions by central banks, but specific criteria are also designed individually by financial institutions' managers in order to avoid excessive risks.

Next, Lam (2014, p. 281) states that financial institutions need to evaluate the reliability of their hardware and software systems in order make sure that possible external attacks would not affect customers' security above an appropriate degree. Specialists in the field of security test banks' shortcomings and flaws in the existing protection, and thus have to propose measures which would allow covering those shortcomings and removing system vulnerabilities. A great number of attacks are carried out today in the online environment or using online tools. As a result, technical security is to a large extent dependent on the technical measures undertaken for ensuring their highest degree of protection on the web. Leakages of financial data are among the highest risks together with the theft of funds, and thus they should be paid particular attention as well.

Also, Mok and Saha (2017, p. 8) state that—— staff training plays an important role too. Financial companies using a strategic approach to their risk management procedures need to make their employees fully aware of the actions which they should do in case of any threats to the financial institution's security arising either from within the company or from its external environment. Employees need to be able to interact effectively with each other and with their managers on all levels, thus contributing to the best possible reaction to the existing or potential risk events. Financial companies' management is also interested in carrying out regular audits so as to reveal internal flaws and inconsistencies. Risks might be caused not only by third-party agents, but also by the company's own employees and associated parties, and therefore time and effective monitoring and control are among the key preconditions for the effective implementation of risk management.

Therefore, based on the information stated above, it can be said that risk management in financial companies is a complex process based on a number of different procedures and processes. In most large financial institutions, the risk management procedures are carried out broadly within a strategic approach. However, the existence of a body responsible for the results of such procedures is important for their ultimate results. In the next chapter, the role and competencies of the risk management department of the financial institution will be analysed.

## 1.5 Role and competencies of the risk management department in financial institutions

The risk management department of a financial institution is its internal unit responsible for performing effective risk management procedures, and thus for ensuring the minimization of risks incurred by the company. Thus, the functions of the risk management department embrace all of the risk management tasks to be fulfilled within the financial institution. The risk management department is a unit which ensures the strategic coordination of all risk management activities within the corporation, and which is destined to ensure a systemic approach to the resolution of the arising issues and to the prevention of the occurrence of new possible threats which might damage the company's security and thus its performance in the long run.

Fraser et al. (2014, p. 434) state that the risk management department of a financial institution is responsible for the identification, measurement, monitoring and control of the entirety of risks incurred by the financial institution throughout the course of its business activitie. One of the main tasks of the risk management unit is to evaluate and review in a timely manner the risks which hinder the company's financial performance and which might affect its long-term business performance. The review of risks is carried out together with the company's top management, so as to integrate appropriate risks measurement measures in the company's appropriate business strategies and policies. However, thereafter such activities are also carried out in order to make appropriate adjustments to the company's strategies, but also to make effective amendments to its policies. Ongoing monitoring is equally important for companies in order to make timely changes to the business policies they carry out, and thus in order to avoid excessive threats to their business. The information on the results of ongoing monitoring are transmitted regularly to the board of directors.

Louisot and Ketcham (2014, p. 216) note that another important task of the risk management department is to perform the training of the financial institution's staff, so as to ensure that the staff complies with the company's chosen strategic direction in terms of risk management, and so as to make the staff follow the rules established for all procedures carried out throughout the company, thus reducing the aggregate amount of risks incurred by the financial institution.

According to Fraser et al. (2014, p. 434), the risk management department cooperates closely with the financial institution's credit committee, analysing the risks associated with loans delivered to particular customers and customer groups and discussing the opportunity to meet the company's liabilities effectively on maturity. The risk management department might also be entitled to carry out audits in order to reveal the existing threats in the company's security systems, and thus can cooperate closely with the security department.

Therefore, in overall terms, it can be stated that the risk management department of a financial institution is one of its key business units ensuring its stability in the long-term perspective by guaranteeing a strategic approach to risk management throughout all business processes.

# 2. Legislation related to risks in financial sphere and their management

## 2.1 Financial Action task force – FATF

As stated by Young (2013, pp. 51-52), the Financial Action Task Force (on Money Laundering), commonly referred to simply as FATF, is an intergovernmental body founded in the 1989 G7 Paris Summit, with the main aim of combatting money laundering. As of today, the organization includes 37 member states, most of which are developed countries. As of today, the main goal of the FATF, as declared by the organization, is to set effective legislative standards and to promote the implementation of legal, regulatory and operational measures for combating money laundering, the financing of terrorism and other major threats affecting the steady operation of the global financial system. In addition to this, as can be found in the Financial Action Task Force (2018), "*The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally. In collaboration with other international stakeholders, the FATF works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.*" A number of reputable international organizations participate in the FATF as associate members, with the main goal of contributing to the mitigation of risks in the financial sector and their effective management. Namely, such organizations include Interpol, the International Monetary Fund (IMF), the Organization for Economic Cooperation and Development (OECD), and the World Bank.

The legislative framework elaborated by the FATF for ensuring effective policies against money laundering and the financing of terrorism includes the organization's forty recommendations against money laundering and special recommendations on terrorism financing. The 40 recommendations provided by the fact are subdivided into particular specific groups, namely legal systems, measures to be

taken by financial institutions and non-financial businesses and professions to prevent money laundering and terrorist financing, institutions and other measures necessary in systems for combating money laundering and terrorist financing, and international cooperation. Let's consider more in detail the recommendations provided by the FATF for combatting money laundering.

The Financial Action Task Force (2018) recommends its member states to adopt a risk-based approach in the financial sector. Countries are advised to designate a responsible authority and to develop explicit mechanisms of action to evaluate the degree of risks incurred in the financial sector, which is indispensable for effective ongoing control and struggle against money laundering and terrorist financing. This is also a basic precondition for an effective mechanism of resource allocation of anti-money laundering and anti-terrorist activities. Also, the member states of the FATF are recommended to coordinate their policies in the fields of AML and CFT for the sake of coordinating effectively their activities and thus for approaching the problem on the international level. They are recommended to exchange relevant information between responsible authorities and to design effective mutual measures in the sector.

Next, the Financial Action Task Force (2018) recommends that "*Countries should criminalise money laundering on the basis of the Vienna Convention and the Palermo Convention. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences.*" Under the abovementioned conventions, the FATF member states are recommended to adopt appropriate legislation and to enable their responsible authorities to freeze, seize and confiscate the money and material goods of the persons or organizations involved in the aforesaid processes of money laundering and terrorist financing.

The Financial Action Task Force (2018) stipulates in its recommendations that countries should penalize the activities of both terrorist organizations and individual terrorists, for which sake money laundering should be prevented effectively. The FATF promotes targeted financial sanctions related to terrorism and terrorist financial. Also, targeted financial sanctions are recommended to be applied in relation to any actors involved in the proliferation of weapons. Also, the Financial Action Task Force (2018) states that "*Countries should review the adequacy of laws and regulations that relate to*

*non-profit organisations which the country has identified as being vulnerable to terrorist financing abuse.*"

Also, within the forty recommendations of the FATF, it is recommended for countries to ensure that financial institution secrecy laws do not affect the implementation of the FATF recommendations. Financial institutions should be prohibited from keeping any anonymous accounts, and should be required to keep all information on their customers and all transactions during five years. Appropriate risk management procedures should be applied to politically exposed persons and to correspondent banking. Particular attention is paid to the operation of money and value transfer services, new technologies in the financial sector, and wire transfers. For financial institutions, it is recommended to pay attention to internal controls with subsidiaries and branches, third parties and operations in higher-risk countries.

Next, as can be found in the Financial Action Task Force (2018), financial institutions are recommended to report any suspicious transactions to the financial intelligence unit, and it is recommended to free such organizations and their employees from any possible responsibility for the disclosure of confidential data when they disclose such data in good faith, due to grounded suspicions regarding potentially unlawful transactions.

Also, of particular attention in the forty recommendations of the FATF are the guidelines related to the transparency of ownership and legal arrangements, for which sake the FATF recommends timely, full and accurate disclosure on the part of appropriate entities. The Financial Action Task Force (2018) recommends that "*Supervisors should have adequate powers to supervise or monitor, and ensure compliance by, financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections.*" In addition to this, the FATF recommends the structure of the provision of powers and responsibilities to financial intelligence units, law enforcement and investigative authorities for the purpose of ensuring transparency in anti-money laundering activities. Also, the Financial Action Task Force (2018) states that "*The competent authorities, supervisors and SRBs should establish guidelines, and provide feedback, which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing…*"

The FATF recommends that countries should adopt effective sanctions in relation to those organizations and entities which have violated appropriate laws. The FATF also outlines recommendations for mutual international cooperation and assistance, namely in terms of freezing and confiscations of assets, extradition of violators, and other forms of international cooperation.

According to Nance (2017), as of today, the FATF is playing an essential role in the development of a common international legal framework to provide guidelines for countries to combat money laundering and terrorist financing. The main shortcoming of the FATF as an organization destined to combat money laundering and the financing of terrorism is the fact that this international organization has a limited scope of legal capacities and has limited practical powers to be directed to the implementation of its recommendations. At the same time, the effectiveness in the implementation of the FATF recommendations vary from state to state, which is due to the specificities of every country's local legislation and its approach to the regulation of the financial sphere.

## 2.2 Basel III and its application in the financial sphere

Basel III can be seen as a global regulatory framework stipulating the standards of capital adequacy, stress testing and market liquidity risks. Basel III is a voluntary framework, which provides guidelines for member states to minimize the risks in the financial sector and raise its long-term stability. Basel III standards were adopted by the Basel Committee on Banking Supervision in 2010-2011. Historically, they are a continuation of Basel II standards, which further enhance the requirements to capital adequacy and stress testing, thus aiming to ensure even greater financial stability for financial institutions through more effective risk management. According to the Hong Kong Institute of Bankers (2013, p. 203), "*The aim of Basel III is to further strengthen global capital and liquidity rules "with the goals of promoting a more resilient banking sector."*" The reforms offered by the Basel Committee within Basel III standards were based on the lessons learned from the 2008 global financial and economic crisis, and namely from the major negative consequences which banks had suffered due to the lack of effective risk management.

Now, let's consider more in detail the requirements imposed by Basel III.

In terms of minimum capital requirements, Basel III imposed stricter standards compared to Basel I and Basel II. According to the standards of Basel III, the regulatory capital of banks is divided into Tier 1 and Tier 2. In its turn, Tier 1 is divided into common equity Tier 1 and additional Tier 1 capital. Tier 2 capital includes unsecured subordinated debt. The main capital requirements imposed by Basel III are the following according to IBM (2017):

1. Capital conservation buffer. This buffer is destined to allow financial institutions absorbing losses in times of economic crises and recession. According to IBM (2017), "*Financial institutions will be required to hold a capital conservation buffer of 2.5% to withstand future periods of stress, bringing the total common equity requirement to 7% (4.5% common equity requirement and the 2.5% capital conservation buffer). The capital conservation buffer must be met exclusively with common equity. Financial institutions that do not maintain the capital conservation buffer faces restrictions on payouts of dividends, share buybacks, and bonuses.*"

2. Countercyclical capital buffer. This buffer is designed to serve as an extension of the capital conservation buffer. Its amount ranges between 0 and 2.5% of common equity, according to national specificities.

3. Basel III introduced a higher common equity Tier 1 (CET 1) indicator, with an increase from 2% to 4.5%.

4. In addition to the capital requirements outlined above, according to IBM (2017), "*Minimum Total Capital Ratio remains at 8%. The addition of the capital conservation buffer increases the total amount of capital a financial institution must hold to 10.5% of risk-weighted assets, of which 8.5% must be tier 1 capital. Tier 2 capital instruments are harmonized and tier 3 capital is abolished.*"

In addition to the capital requirements outlined above, Basel III introduced a minimum leverage ratio for banking institutions calculated by dividing Tier 1 capital by average total consolidated assets. The minimum leverage ratio for financial institutions was set at a level of 3% by Basel III. As stated by IBM (2017), "*In July 2013, the US Federal Reserve Bank announced that the minimum Basel III leverage ratio would be 6% for 8 SIFI banks and 5% for their bank holding companies.*"

In terms of liquidity requirements, Basel III introduced two obligatory liquidity ratios, namely the liquidity coverage ratio (LCR) and the net stable funding ratio (NSFR). As explained by IBM (2017), LCR is calculated as high-quality liquid assets divided by total net liquidity outflows over 30 days, and it should be greater than 100%. In fact, this indicator shows a financial institution's ability to endure 30 days in stress market conditions. As IBM (2017) notes, the "*Net Stable Funding Ratio (NSFR) promotes resilience over long-term time horizons by creating more incentives for financial institutions to fund their activities with more stable sources of funding on an ongoing structural basis.*"

Ramirez (2017, p.13) states that the main advantage of Basel III is that it provides a more robust and sound system of requirements for financial institutions to achieve a better quality of their assets and their business activities. These standards make banks create greater reserves for the cases of crisis events, and thus ensure greater reliability in banks' activities, contributing to their more effective risk management and long-term financial planning.

One of the main inconveniences of Basel III for financial institutions, according to Ramirez (2017, p.13), is the fact that Basel III regulations are widely seen as very conservative and might be negative in terms of financial institutions' opportunity to attract investors for attractive return. However, this is explained by the fact that Basel III promotes financial institutions to adopt a strategic approach in their risk-taking, so as to ensure the best opportunity for them to improve the quality of their assets and to minimize the impact of risks in their risk profiles. This emphasizes the main goals of Basel III, and namely the refusal from pursuing higher returns through excessive risks in favor of lowering the risks of failures and thus maximizing long-term financial stability.

## 2.3 Payment services (PSD 2) - Directive (EU) 2015/2366

The Payment Services Directive (PSD, Directive 2007/64/EC) was launched by the European Commission in 2007 in order to ensure proper regulation of payment services and the operations of payment service providers in the European Union and the European Economic Area. The main aim of the Payment Services Directive was to

enhance competition among service providers and to ensure the harmonization of consumer protection rules in the sector of payment services. On October 8, 2015, the European Parliament ratified the European Commission's proposal for updating the Payment Services Directive for ensuring safer and more innovative payments in the EU and the EEA. This new Directive 2015/2366 is commonly referred to as PSD2. The PSD2 Directive came into force on January 13, 2018.

As noted by the European Commission (2017), "*PSD2 empowers the Commission to adopt regulatory technical standards (RTS) on the basis of the draft submitted by the European Banking Authority (EBA). The security measures outlined in the RTS stem from two key objectives of PSD2: ensuring consumer protection and enhancing competition and level playing field in a rapidly changing market environment.*" The PSD2 Directive introduces significantly stronger security requirements compared to its predecessor, which is seen as a key requirement in the light of the growing threats in the financial sector. PSD2 makes strong customer authentication (SCA) the basis for accessing one's payment account. It becomes obligatory for payment systems to provide simultaneously at least 2 of the 3 following authentication methods: a password or PIN code, a card or a mobile phone; and a fingerprint or an iris scan. Banks and other financial institutions are required to implement the necessary infrastructure for supporting the functionalities of SCA. At the same time, the Directive requires such financial institutions to improve their fraud management through better training of the staff and implementation of appropriate protection measures. As the European Commisison (2018) notes further, "*All payment service providers will need to prove the implementation, testing and auditing of the security measures. In case of a fraudulent payment, consumers will be entitled to a full reimbursement. For online payments, security will be further enhanced by linking, via a one-time password, the online transaction to its amount and to the beneficiary of the payment. This practice ensures that in case of hacking, the information obtained by a potential fraudster cannot be re-used by for initiating another transaction.*"

A revolutionary aspect of PSD2 compared to its predecessor is the fact that the Directive allows third-party applications with a trusted license to access customers' bank account data and data in payment systems. Thus, in fact it forces customers to reveal their data to third parties, which, according to Chishti and Puschmann (2018, p.

117), allows "*rebalancing client data in favour of the clients themselves, increasing competition by forcing incumbent banks to innovate faster and providing more choices and seamless experiences to clients.*" For banks, this aspect might represent a threat that third-party institutions could take over their clients through the provision of better infrastructure and access to complementary services. Therefore, the European Commission believes that PSD2 should drive the banking institutions' desire to maximize the quality of their services in the light of growing competition.

Another important legislative innovation set out in PSD2 is the way how corporate batch payments should be treated. According to the European Commission (2017), the PSD2 Directive sets out specifically the requirements applicable to host-to-host machine communication which occurs in the case of batch payments used by corporations.

Teigland et al. (2018, p. 16) believe that the application of the PSD2 Directive should be expected to bring considerable changes to the structure of the industry of payment services in the near future. Namely, it should be expected to contribute to the development of actors such as third-party providers (TPPs), account information service providers (AISPs), and payment initiation service providers (PISPs). The emergence of these new actors should be expected to enhance the intensity of competition in the industry of financial technologies and financial services, and should incite the existing actors to improve their business models based on the implementation of innovations, adoption of greater transparency and soundness and orientation on the maximization of positive customer experiences.

The application of the rules set out in PSD2 improve the quality of customer services and allows customers using more conveniently the opportunities of online payments. It also promotes the development of small payment service providers, which contributes to customers' opportunities of choice. However, as Teigland et al. (2018, p. 16) note, there are several important shortcoming in the application of PSD2. Thus, first of all. It applies only in the European Economic Area, however it doesn't affect the transactions associated with third countries. Users might also be considered unprotected due to the exemptions stipulate in the Payment Services Directive. Finally, there are discrepancies in terms of the opportunities for companies to choose the regulations

applicable to merchants, which might bring unequal application of the Directive throughout the European Union.

As the European Commission (2017) itself states, while PSD2 is aimed to boost e-commerce by promoting consumer trust, it at the same time focuses on minimizing the level of frauds through higher security. This requires payment systems to adapt their security measures to the new requirements, which requires additional resource expenditures on their part, which might be a negative temporary effect, yet to be compensated in the long-term perspective.

Another important aspect of the PSD2 Directive is the fact that it establishes requirements applicable to banks and other financial institutions in terms of the creation and operation of their communication interfaces with customers. According to the European Commission (2017), "*Payment service providers, including banks, will have to define transparent key performance indicators and service level targets for the dedicated communication interfaces, if they decided to set them up. These performance indicators should be at least as stringent as those set for the online payment and banking platforms used by the customers.*" Banks can be exempted from setting up a fall-back mechanisms, if they set up a fully functional communication interface.

PSD2 also pays specific attention to customers' personal data. As the European Commission (2017) explains, no data transmission can be carried out without the express consent of the customer. Customers can control the transmission of their person data under PSD2 and the Data Protection Directive. Payment service providers are required to inform customers of all ways in which they data will be processed, which is done in order to minimize the risks of loss or maltreatment of customers' personal data, and thus to improve the level of security for protecting customers from possible external or internal perpetrations. As the European Commission (2017) notes, "*PSD2 prohibits TPPs from accessing any other data from the customer payment account beyond those explicitly authorised by the customer. Customers will have to agree on the access, use and processing of these data. With these new rules, it will no longer be allowed to access the customer's data through the use of the techniques of "screen scraping"*." Screen scraping stands for customers' personal data being literally 'scraped' from the customer interface. Banking institutions are required to provide the interface to allow third-party service providers accessing such personal data of customers in compliance

with the requirements of PSD2. In this way, PSD2 prevents third-party service providers from accessing customers' personal data without notifying the banks thereof. This is set to guarantee the maximum level of customers' protection in the course of interaction with payment service providers and other kinds of financial intermediaries.

According to Deloitte (2016), the application of PSD2 will have both strategic and operational impact on financial institutions, and operational impact on customers. Thus, in terms of strategic impact, banks will have to set up themselves an AISP or PISP, review their payment strategy and consider potential loss of revenues on payment cards business. TPSPs will have to identify the optimal country to be registered in, ensure the availability of professional indemnity insurance, and to monitor developments of service offerings by market competitors. Merchants should consider developing applications for improving customer service. In terms of operational impact, banks are required to ensure compliance with reporting standards and to consider the need for IT developments. TPSPs are required to further develop technology infrastructure and to ensure compliance with reporting requirements. For merchants, it is required to ensure connections with PISPs to support the new payments workflow. For consumers, operational impact will consists in a decreasing number of card transactions, and the opportunity to use a single AISP to manage all own accounts.

Therefore, in overall terms, it can be stated that the FATF, Basel III, PSD2 and other measures noted in this chapter are aimed first of all to enhance the level of security of financial institutions and their customers. This proves that one of the main scopes of focus of developed states in the financial market as of today is the minimization of inherent risks for the sake of ensuring the maximum level of security for customers' interaction with payment services providers. Taking into account these facts, it is now worth proceeding to the practical analysis of a financial institution to reveal the specificities of its risks management and associated processes in the light of the existing security threats.

# 3. Case study – risk management and internal processes in the chosen financial institution

## 3.1 Evidence and small cases from the history

The main focus in this chapter of the thesis is going to be put on the evaluation of the risks associated with banks' cybernetic security. The main reason for the choice to focus on this specific category of risks is the fact that issues of cybernetic security are currently among the main risk factors affecting banks' overall financial conditions. As noted earlier in this research, hackers' attacks against banks tend to become more and more intensive in line with the development of technological progress and the growing versatility of up-to-date online and digital technologies. Banks are suffering from such attacks in association with two main factors: on the one hand, their customers are losing their funds deposited in the bank as a result of such attacks, and on the other hand, such attacks might also be directed to stealing personal data. In the long run, not only the banks' financial funds are stolen, but also its image is getting impaired. As noted by Campbell (2017), "*Hacking software is becoming more sufficient, increasing the impact that hackers can have on a business. Cyber hackers are moving to more sophisticated agendas such as espionage, disinformation, market manipulation and disruption of infrastructure, on top of previous threats such as data theft, extortion and vandalism. Being able to mitigate these threats requires businesses to not only think of cyber security as a business risk, but to act on this too.*" Therefore, we need to evaluate this issue more in detail in order to understand better how the current situation with growing cybersecurity risks might affect banking institutions and which responsive actions banks might implement in order to achieve the desired business results.

In order to emphasize further the importance of this research focus, we should consider several of the recent cases of cybernetic attacks against banks in order to understand their scope and the underlying threats they imposed on banks.

In 2017, a group of hackers was able to steel USD 60 million from the Far Eastern International Bank in Taiwan by infiltrating its computer system. As noted by

Thomson (2017), "*The malware's masterminds, we're told, managed to harvest the credentials needed to commandeer the terminal and drain money out of the bank. By the time staff noticed the weird transactions, $60m had already been wired to banks in the US, Cambodia, and Sri Lanka.*" The perpetrators acted through the deficiencies in the bank's system of processing of SWIFT payments, and were able to steel credentials using which they subsequently appropriated clients' funds. An investigation run by the bank and the financial authorities of Taiwan after the incident proved that the bank's security system was not completely sound, and account management had major drawbacks, which impaired substantially the overall security of the SWIFT system. According to Reuters (2017), the banks was able to recover only USD 500,000 of the funds stolen, and was additionally fined by the regulatory bodies of Taiwan for USD 160,000.

Another example of a hacker attack aimed at a bank's SWIFT system is the 2017 attack against the Russain state bank Globex. According to the Japan Times (2017), "*Unknown hackers stole 339.5 million roubles ($6 million) from a Russian bank last year in an attack using the SWIFT international payments messaging system, the Russian central bank said on Friday. The disclosure, buried at the bottom of a central bank report on digital thefts in the Russian banking sector, is the latest in a string of attempted and successful cyberheists using fraudulent wire-transfer requests.*" The investigation run by the Russian authorities did not lead to any tangible results, and the bank was fined by the Central Bank of Russia for undue attention to security issues and the lack of effective protection mechanisms to guarantee the security of clients' funds in the light of growing third-party attacks.

In addition to this, as noted by the Seddon (2018), "*Most vulnerable, however, are Russia's banks. Hackers used the Cobalt Strike security-testing tool to steal more than $17m from more than 240 Russian banks in 2017, according to the central bank.*" Therefore, the threat of cyber-attacks is of a mass nature, and it affects not only individual banks, but also whole bank systems, even of large countries such as Russia.

Another bright case of the growing sophistication of criminals' activities with cyberattacks against banks is the activities of the hacker group MoneyTaker. According to Osborne (2017), "*The first attack was detected in 2016 when money was stolen from a US bank by compromising First Data's network operator portal. Since then,*

*companies in California, Utah, Oklahoma, Colorado, Illinois, Missouri, South Carolina, North Carolina, Virginia, and Florida have also been targeted. Group-IB connected the dots between attacks conducted by MoneyTaker through the tools used, attack infrastructure, and withdrawal schemes which had a particular signature -- the use of unique accounts for each transaction.*" The key specificity of the attacks run by this groups is that they focus on steeling funds from ATMs without having any physical access to the machines. Modular software is used by the hackers in order to reveal payment orders of customers and modify them, replace payment detail and erase logs. A special concealment module allows the hackers erasing the traces of their attacks, and therefore they cannot be tracked by the authorities.

Another important case study worth being mentioned is the 2014 data breach case of JPMorgan Chase. According to Roman (2014), the cyberattack led against JPMorgan Chase compromised approximately 83 million accounts and was one of the greatest data breaches in the history of the global financial sector. The attack occurred in September 2014, but was revealed by the bank's security department only in July 2014 and remedied in August. The bank's management denied customers' personal data being compromised, but thereafter acknowledged it, namely stating: "*We uncovered an attack by an outside adversary recently where the firm's technology environment was compromised… We are confident we have closed any known access points and prevented any future access in the same way.*" The perpetrators got access to the login information of customers for their personal accounts, and to their phone numbers, physical and electronic addresses. The main reason for the effective performance of the perpetrators consisted in a considerable vulnerability in the bank's cybersecurity system. Namely, the perpetrators, allegedly from Russia, used a vulnerability of an employee's computer. This computer was connected with the employees' home computer through a virtual private network. Through this, the perpetrators accessed the corporate computer. To remedy the situation, the bank closed employees' accounts and cleaned up the system, until all leakages were eliminated. However, despite this, the situation brought considerable damages to the bank, as it impaired its reputation as a reliable and secure financial institution in the eyes of customers.

It is also worth noting the case of Société Générale which underwent a fraud on the part of its employee Jérôme Kerviel in 2007, and thus endured considerable

financial losses. As Iskyan (2016) notes, Kerviel was an employee who worked as a trader for the French bank Société Générale. In 2007, Kerviel started engaging in unauthorized trades, anticipating the falling stock prices in the market. He opened trade positions for almost EUR 50 billion, 1.5 times greater than the bank's own capitalization. He hid these transactions from the bank, and Kerviel's unauthorized trading was revealed by the bank's security service in January 2018. The bank had to close his positions, and as a result lost almost EUR 5 billion. This situation illustrates clearly that banks' cybersecurity system is compromised not only by external perpetrators, but also by internal stakeholders who have access either to confidential information or to levers of decision-making.

This case is somehow similar to the one of Nick Leeson. According to Rodrigues (2015), Nick Leeson was a rogue trader whose illegal trading operations led to the collapse of Barings Bank in 1995. Leeson gambled away as much as GDP 827 million in the bank's name. As a result of his fraudulent operations, the bank was acquired by ING Bank, and many of Leeson's colleagues lost their job.

Also, it is worth recalling the role of ineffective internal audits in elevated risks of frauds in banks. Thus, according to Roy and Ghosh (2018), the Punjab National Bank in India lost over 8 million dollars as a result of its ineffective internal audit system. Despite the fact that the auditor reported directly to the directors, he was unable to monitor effectively those operations which were not effected through the bank's core banking system. The fraud can be caught in this case, but it requires thorough monitoring, and this was not done by the bank's internal audit department.

Another illustrative case in this context is the one of Wells Fargo. According to Marks (2016), the bank opened an estimated USD 2-million deposit accounts and applied for 565,000 credit card accounts to meet sales goals. The banks was fined for USD 185 million. Makrs (2016) describes that "*Spurred by sales targets and compensation incentives, employees boosted sales figures by covertly opening accounts and funding them by transferring funds from consumers' authorized accounts without their knowledge or consent, often racking up fees or other charges.*" This was possible only due to the incompetent monitoring and weak risk assessment of the bank's internal auditors. Moreover, internal auditors didn't pay sufficient attention to monitoring

customer satisfaction claims, which prevented them from revealing the existing fraudulent activities on the part of employees.

Thus, as can be seen from the brief overview of recent cyberattacks against banks presented above, the threats of cybersecurity are indeed among the most important risk factors which affect the activities of banking institutions as of today. In order to overcome this, banks need to develop powerful cybersecurity systems, and should have thorough protocols for the elimination of such risks.

## 3.2 In-depth case study

Within the case study in this part of the research, we are going to focus on the analysis of the cybersecurity system of VersaBank, a Canadian financial institution in the banking sector which acts only as a digital bank and has lately been involved in the development of specific functionalities for cryptocurrencies. As the bank operates only in the online environment, the threats of cybersecurity are the most important ones which might affect its long-term financial stability. In an interview held with the company's risk manager, we tried to reveal the main types of cybersecurity threats incurred by the bank, and to identify those protection measures and mechanisms which the institution uses in order to minimize their impact. The conversation with the manager was held by phone and lasted for approximately one hour. The interview was semi-structured. Its questions were developed by the thesis author in line with the goals of this part of the research. The structure of the interview can be found in Annex 1 to this thesis. Below, we are going to highlight the main findings derived from the interview with VersaBank's manager, and we are going to analyse them.

**On the threats incurred by the bank in terms of cybersecurity**

Answering this question of the interview, the manager of VersaBank stated that the risks of cybersecurity are indeed high, and the bank is vulnerable to them. He stated that this relates not only to theft of funds or customers' personal data, but also to DDOS attacks which are directed to block the bank's activities. In the long run, in either case, the bank loses its funds, its reputation gets impaired, and significant investment should be done to restore the previous positive image. Therefore, the bank adopts a proactive position toward the identification of potential threats, and tries to maximize the

effectiveness of the security mechanisms implemented within the structure of its security system. Nevertheless, despite this, the threats in the field of cybersecurity still exist and cannot be eliminated at all, as perpetrators always improve the tools they use for hacker attack, and put the benefits of technological progress to use for their illegal purposes.

**On the differences in terms of cybersecurity between traditional and digital-only banks**

The manager of VersaBank answered that the differences in terms of cybersecurity are minimal as regards how traditional and digital-only banks are affected. For perpetrators, in both cases, the same tools are used and the same goals are pursued. The only reason is that traditional banks are generally larger compared to digital-only banks, and they have an opportunity to invest more in their cybersecurity systems, as well as to diversify their risks through the operation in different environments. In digital banks, all risks are concentrated in the field of cybersecurity, hence the potential effects of any possible cyberattacks can be expected to bring greater damages to the financial institution. This emphasizes again the need for such banks to pay particular attention to their cybersecurity and protection.

The manager of VersaBank also stated: "*However, despite the fact that our risks are rather greater compared to traditional banks in terms of cybersecurity, it should still be noted that we have greater expertise in this field as well, as we are a digital-only bank. We always work on cybersecurity, and therefore we are able to adapt our activities better to the existing threats in the field of security.*" According to the manager of VersaBank, digital banks are able to build greater expertise in the field of cybersecurity, and this allows them meeting the existing threats with subsequent development of their dedicated staff's skills in the domain of cybersecurity. However, digital-only banks are smaller compared to traditional banking institutions, and they have smaller financial resources as well, due to which their capacities in the development of own technologies in cybersecurity are smaller, and they have to base their security on the use of third-party technologies, namely ones borrowed from traditional banks. As a result, they have smaller competitive advantages in terms of the technologies available and applied in cybersecurity.

**On potential negative effects of different types of cybersecurity threats**

Here, the manager stated that the range of attack schemes, tools and methods currently used by perpetrators is very large, and therefore there are many different cybersecurity threats, all of which should never be neglected.

First of all, we should speak here of hacker attacks destined to hack the access to customers' bank accounts or e-wallets in electronic payment systems. This can be done in several ways. On the one hand, perpetrators are seeking vulnerabilities in the bank's security system: they search for ways to steel confidential data such as encryption codes and passwords, find ways to reroute transactions to different recipients, use automatic tools to generate possible passwords to customer accounts. The main task of the bank here is to guarantee that no leakages of confidential data exist, that all security mechanisms are duly protected, and finally to identify the existence of attempts to breach banking security, so as to react quickly. Perpetrators can use malware which is installed on the PCs of the banking institution or ordinary customers and thereafter collects data such as logins and passwords, records them and transmits them to the hackers, which can thereafter use such information for steeling customers' funds.

In this context, a particularly widespread method is phishing e-mails. Perpetrators often send messages to their victims stating that they need to undertake particular actions in association with their bank accounts for the purpose of avoiding freezing, accepting fund transfers, and so on. Phishing links are sent in such e-mails. As soon as the customer follow the link, he goes to a website similar to the one of the bank, and when he enters his credentials, the perpetrators steel them, and thereafter have all means required for steeling funds from the customer's account. The bank's actual opportunities to do anything here are very limited, and perpetrators have significantly greater opportunities to complete their illegal acts successfully. Similarly, perpetrators can often use forums, chats, online boards, social networks, and all other possible channels of online communication to coax confidential data out of customers.

The so-called Nigerian letters, where customers are offered a great compensation if they transfer some funds or provide the data on their account to the perpetrator, are another important method of gaining illegal and unauthorized access to customers' bank accounts.

Therefore, generally, all cybersecurity threats can be divided broadly into two categories: those based on the use of deficiencies and vulnerabilities in the bank's security system and those based on the deception of customers.

In addition to this, the manager stated that method such as DDoS attacks, even though they do not allow perpetrators stealing funds or confidential data, might block the operation of online banking, which in the long run leads to considerable damages and losses to be incurred by the bank.

**On attacks against banks and attacks against their customers**

According to the opinion of VersaBank's manager, both types of attacks are equally dangerous and can have potentially similar consequences in terms of losses to be incurred by the bank. However, in the case of own vulnerabilities, all responsibility is on the bank, and the financial institution's cybersecurity experts can foresee the activities of perpetrators and implement measures to counteract possible illegal steps on their part. In the case of attacks directed at customers, the bank cannot act effectively, as they can be unaware of such situations. Unfortunately, customers often fail to take into account the recommendations delivered by banks in terms of security of their transactions, and thus they undertake measures to protect their accounts too late. In these terms, the attacks against customers are more dangerous. However, in terms of aggregate amounts which are stolen and overall consequences for the bank, attacks based on the use of the bank's vulnerabilities are more harmful, as they are done in a centralized manner, and the range of victims is significantly broader.

**On whether VersaBank has been subject to any considerable attacks**

The manager of VersaBank stated that fortunately, the bank has never been a target to large-scale hacker attacks. Minor accidents occur periodically, but their impact is insignificant, and the bank is able to deal with them quite effectively thanks to the robust organization of its cybersecurity system. Most often, perpetrators are able to complete successfully their attacks when they target the bank's customers directly, and coax confidential data from them. The banks can remedy the situation only if customers react instantly and require the bank to block their account. Otherwise, such attacks are hard to monitor and counteract, and therefore they are often successful. To avoid them,

the bank tries to constantly remind the customers of the existing threats and of how they can be minimized.

**On the organization of cybersecurity at VersaBank**

Answering this question of the interview, the risk manager of VersaBank stated that the company's cybersecurity system is based on a constant re-evaluation of risks and threats and the implementation of measures destined to minimize the potential negative impact of any activities undertaken by perpetrators. Any attacks which are identified by the company's specialists are counteracted immediately, and the entire team works on remedying their effects. The company uses the most up-to-date software for preventing illegal access of third parties to its confidential data. It uses powerful encryption mechanisms for all transactions and prevents any possible leakage of data due to the bank's internal vulnerabilities. In addition to this, periodically, the bank resorts to the use of third-party companies which imitate hacker attacks on the bank's servers, and real-life situations are simulated, in which the bank's staff responsible for cybersecurity needs to react very quickly in order to avoid major negative consequences for the bank.

The company's risk management department is responsible for 24/7 monitoring of all actions on the part of third parties destined to breach the security of the company's system. The risk management department cooperates closely with VersaBank's IT department. The IT department is responsible for the development, maintenance, implementation and updated of software and hardware used in the bank's systems of cybersecurity. The IT department is also involved in the identification of vulnerabilities and threats in terms of the operation of the bank's information system and associated technologies. In addition to the risk management department and the IT department, it is also worth noting the importance of the top managers' role in the maintenance of the company's cybersecurity. Namely, the top management of the bank develops frameworks and guidelines within which the entire system of cybersecurity operates, and thus sets the rules and standards for the cooperation of all other stakeholders and for the most effective implementation of the bank's security mechanisms. Also, the bank provides trainings for all its employees, as every employee is believed to play a decisive role in the effective operation of the whole system of cybersecurity. Thus, employees' role consists in the prevention of possible data

leakages and unauthorized attacks on the part of third parties, and in ongoing communication with the bank's risk management department. As employees only operate on a remote basis and do not see their clients in person, they should have particular skills in the identification and prevention of potential threats. It is also important for employees to understand well all the procedures applied by the company, and thus to operate within the framework of the applicable regulations so as to ensure consistency in the integration of the bank's security system with all its components.

The bank builds up its internal communication in terms of cybersecurity in a way to ensure the maximization of effectiveness of the measures applied against the existing and possible future perpetrations. Namely, meetings are held with the involvement of the main stakeholders on a weekly basis. On such meetings, the achievements in the field of security are discussed, as well as the existing threats. Communication is aimed at revealing where the bank faces the greatest threats in terms of cybersecurity, where its vulnerabilities contribute most to the existence of such threats, and which measures should be undertaken for preventing perpetrators from running effective attacks against the bank. In terms of employees' risk management skills, the banks organizes security trainings for employees on a quarterly basis. At the same time, new employees are provided with an extensive training on cybersecurity when they are first hired. It is important for the bank to ensure that every business unit and every single manager and employee contribute effectively to the bank's business security, so as to guarantee the most stable situation with security in the long-term perspective.

As for the use of third-party services when modelling potential external attacks against the bank, the manager of VersaBank stated the following: "*It is always important to get a fresh look from apart. Some threats might be out of our sight, and we might be unaware of their existence, or of the existence of vulnerabilities in our security system. When we hire experts which simulate attacks against the bank, we get professional assistance, as such specialists emphasize our problems, and thus indicate where we should undertake measures to improve our cybersecurity*". Upon termination of such mutual campaigns, all corporate stakeholders and managers in the bank discuss their results, and design countermeasures for remedying the existing threats and for eliminating the existing vulnerabilities.

Of great importance for the bank is also the follow-up of the measures implemented. Often, they require additional work and improvement, and the banks' cybersecurity specialists focus on ensuring steady improvement and regular updated of all such tools, processes and frameworks.

In addition to this, the bank is a pioneer on the global scale in the use of blockchain technologies for protecting its confidential data and thus for minimizing the inherent risks of theft of confidential data and their subsequent use for illegal purposes. According to the information provided by the London Free Press (2018), "*VersaBank says the blockchain-based vault works like a safety deposit box, where only the user has access or knows what is inside but its contents are protected from hackers and other risks… The VersaVault, when launched, will also hold other digital valuables such as sensitive photographs or contracts, he added.*" The company's risk manager confirmed that the use of a blockchain-based vault is seen by the company as a new word in the field of cybersecurity. The management of VersaBank believes that the use of this technology will allow reducing significantly the risks of successful hacker attacks, particularly those based on theft of unduly protected customer records and documents. As noted by FX Street (2018), "*This is a breath of fresh air especially for the huge players in the cryptocurrency market. Hacking and theft have been frequent reports in the market in the recent months. A secure vault could be the answer to such woes in the market. Investors are hopeful that this decision will take root and materialize as planned.*"

According to the information provided by the manager of VersaBank, the company's security department always monitors all new information in the market. This relates to new cyberattacks held by hackers against the world's banks, innovations in the field of cybersecurity, various new practices which banks all over the globe apply with the aim of raising the overall level of their security, the current trends in the development of new technologies, and so on. Without being aware of the latest development in the sector, the bank would be unable to respond appropriately to the existing and possible new threats with its own measures. The main task of the bank's staff is to analyse the entirety of information available, and to generate new ideas which might help improve the situation. The bank is rather small, and its opportunities to develop new own technologies are limited. As for the development of own technologies

in the field of cybersecurity, the manager of VersaBank stated that this is the responsibility of the bank's research and development department. The specialists of the department are responsible for developing and implementing new technologies in the field of cybersecurity to raise the bank's overall protection against the existing threats. The bank's management invests funds in the development of own security technologies, as the bank has a unique expertise in the domain of online transactions, and thus can put them to use for the sake of maximizing its own security.

However, the bank draws on the best practices of other financial institutions and improves the whole range of technologies available in the field of cybersecurity. General meetings of the staff are held where brainstorming is used as a method to generate new creative ideas and subsequently implement them in the bank's practice. Also, the bank's own inconveniences and faults in the field of cybersecurity are analysed thoroughly, and appropriate measures are undertaken to avoid the re-occurrence of such events in the future.

The bank is also one of the pioneers in the domain of cybersecurity, where it acts effectively in terms of the adaptation of blockchain technologies, as noted above. The bank focuses on the development of own technologies in cybersecurity as one of the top-priority vectors of its business activities for the near future.

The risk manager of VersaBank stated that there is a commonly recognized and accepted protocol of customer activities which allows minimizing the risk of their data being stolen or hacked. First of all, customer should keep their passwords and other confidential data secret and protected. A common mistake is to hold them in a file on the desktop on your PC, or to write them down on a sheet of paper left on the table. You should make sure that no third person has access to such information. Second, personal data should never be transmitted to any third parties.

The manager stated that in the case of their particular bank, previous thefts were done due to customers' inattention. The variety of methods used by perpetrators were quite large, but most often this is don't through phishing e-mail. The web interface of any website is quite easy to imitate, and customers who are easily confident in such e-mail are persuaded they operate through the ban's interface. Thus, they provide their own confidential data deliberately to the perpetrators, and this cannot be detected by the

bank. Sometimes, perpetrators can call the customers and inform them of some information required on their account, such as the PIN code. Even though the bank always emphasizes that its employees never ask any personal details of their customers in phone conversations, people still often believe in such calls and provide their data to perpetrators. However, there have been cases when perpetrators hacked the mail servers of customers, and thus stole the confidential data of VersaBank's customers from their mailboxes.

As for internal security**, t**he bank's employees never ask the customer's passwords, PIN codes or any other confidential data in conversations; such data are never required by shops, public authorities, and so on. Therefore, when any third party asks for such data, it is quite likely to be a perpetrator. Next, the antivirus and anti-malware software on your PC should be always kept updated. Often, data are stolen from customers' PCs by automated malware, and this can even remain unnoticed. Therefore, the use of effective anti-malware software is of key importance for minimizing the risk of being hacked.

When operating with Internet banking, customers should always check the website address in the address bar, and should make sure that the secure https protocol is used. This is a guarantee that you wouldn't be redirected to a malicious third-party website where your confidential data can be stolen, thereafter leading to possible theft of your personal funds. Moreover, customers should refrain from publishing anywhere the phone number or e-mail address tied to their account at the bank. The bank in its turn guarantees that no third parties have access to such information. This allows minimizing the risks of perpetrators gaining access to your accounts by hacking your webmail server or using phishing calls. If such data are kept confidential, the overall level of your bank account's security will be significantly higher. Finally, the manager of VersaBank recommended to avoid installing and using various apps such as bonus collectors, checkers and so on, as they raise the risks of loss of confidential personal data.

If customers follow the recommendations outlined above and pay sufficient attention to the security of their bank accounts, this will lower significantly the risks associated with possible theft of their personal data and/or funds through the banking institution.

The manager of VersaBank stated that the main trends which can be expected in the banking industry is the growing sophistication of perpetrators' attacks, and as a result the growing effectiveness of banks' protection technologies, as banking institutions are learning new ways to proceed with illegal perpetrations as well. Artificial intelligence and machine learning can be expected to be the predominant technologies predefining subsequent vectors in the development of banks' cybersecurity. Banks can also be expected to strengthen their specific regulations associated with internal leakages and breach of confidentiality. A common global cybersecurity network can be expected to keep developing in the years to come, as the risks incurred by banking institutions are virtually the same all over the world, and therefore all financial institutions are interested in seeking mutual solutions in order to minimize their possible losses associated with hacker attacks.

Analysing additional secondary data, we can recall some more trends which can be expected to rule cybersecurity in the banking sector in the years to come. Thus, according to Drolet (2017), in the spring of 2018, the General Data Protection Regulation (GDPR) is expected to enter into force: "*If your preparations for the European Union's new GDPR, explaining how companies should process, store, and secure the personal data of EU citizens are not complete, or at least well underway, then you better get moving. The GDPR will be enforced from May 25, and infringements can provoke fines of up to 20 million euros ($23.6 million at the time of writing) or 4% of the total worldwide annual turnover of the preceding financial year.*" This regulation should thus contribute to the common rules of play in the field of cybersecurity and should formalize the framework of banking institutions operations in the field of cybersecurity in the European Union. The author notes additionally that another common trend which can be expected in the fight against ransomware such as WannaCry which brought major damages to companies around the globe in 2017.

Panetta (2017) notes that another main focus of banks in terms of cybersecurity in the years to come will be the security of cloud-based services: "*As the cloud environment reaches maturity, it's becoming a security target and it will start having security problems. It's possible cloud will fall victim to a tragedy of the commons wherein a shared cloud service becomes unstable and unsecure based on increased demands by companies. When it comes to cloud, security experts will need to decide*

*who they can trust and who they can't.*" Therefore, we can expect that the efforts of banks' cybersecurity specialists can be expected to focus largely on the resolution of issues associated with cloud services.

Regarding the risks incurred, the manager of VersaBank stated that the institution is going to focus its blockchain-based vault, which the company believes to be one of the most up-to-date technologies in the field of cybersecurity and which it sees as a key competitive advantages which might allow for the bank's market growth in the years to come. At the same time, the company will continue monitoring the current trends in cybersecurity in the banking sector, and will try to maintain steadily high standards of security of its customers' accounts.

So, based on the findings revealed through the interview with the manager of VersaBank, we can state that in terms of cybersecurity there are two main groups of risks for banking institutions: on the one hand, those are the risks associated with the vulnerabilities of the banks themselves. The second group of risks include those risks which customers incur due to the lack of sufficient attention: such risks are particularly threatening, as banks cannot monitor the situation effectively. In the first case, the responsibility lies totally on banks, as they need to implement effective protection measures and keep their cybersecurity systems always updated in order to minimize the risks incurred. In the second case, banks need to provide information to customers on how their confidential data should be kept secret, but it is the responsibility of customers to ensure that such data are not disclosed to any third parties.

It can be stated that the findings from the interview with the manager of VersaBank correlate with the previous findings of the thesis. They confirm that the range of tools available to perpetrators tends to keep evolving thanks to steady technological progress, and banks need to be able to withstand threats from different sources in order to maximize their effectiveness in the field of cybersecurity. Cases of frauds in large financial institutions such as Société Générale, JPMorgan Chase, and Wells Fargo prove that any defects or shortcomings might compromise the banks' entire security system. VersaBank seeks addressing these issues by adopting an integrated approach to cybersecurity and by using innovative technologies.

Based on the information outlined above, we can now proceed to the assessment of the actual amount of risks associated with cybersecurity as incurred by banks, and can develop a risk map which would reflect such risks graphically.

## 3.3 Lessons learned and recommendations

**Table 1: Assessment of banks‘ risks based on the findings of the interview and previous research**

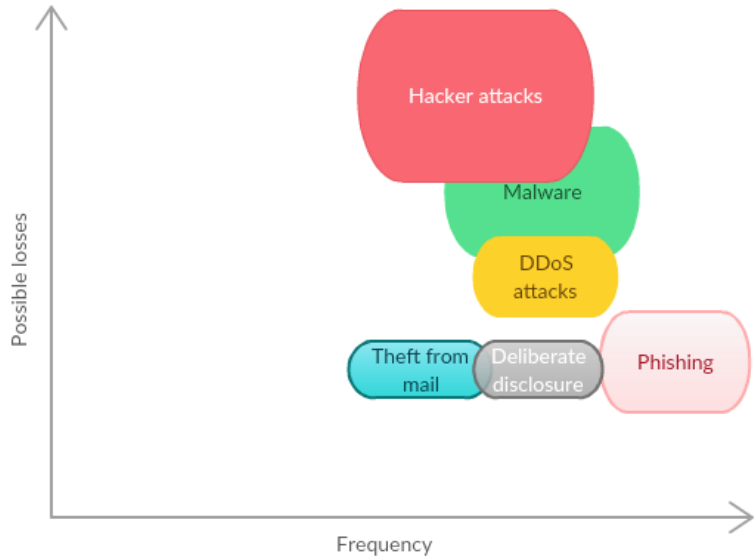
| | Frequency (1 to 5) | Possible losses (1 to 5) | *Sum* | Weight coefficient (sum = 1) | ***Total*** |
|---|---|---|---|---|---|
| Hacker attacks against banks | 3 | 5 | *8* | 0.3 | ***2.4*** |
| Use of malware | 4 | 4 | *8* | 0.22 | ***1.76*** |
| DDoS attacks | 4 | 3 | *7* | 0.12 | ***0.84*** |
| Phishing e-mails and phone calls | 5 | 2 | *7* | 0.14 | ***0.98*** |
| Theft of data from customers' mail servers | 3 | 2 | *5* | 0.12 | ***0.6*** |
| Customers' deliberate disclosure of their personal data | 4 | 2 | *6* | 0.1 | ***0.6*** |

**Source: Own research based on the findings of the interview**

In order to compile the table presented above, we took two major characteristics associated with risk: the frequency of their occurrence and possible aggregate losses (both financial and reputation losses) which banks might incur as a result of the occurrence of such events. All such risks were then assigned points from 1 to 10. The amounts obtained were summed. Then weight coefficients were assigned to each risk factor based on the interpretation of the results obtained through the interview and previous research. The amount of weight coefficient was assigned by the thesis author based on the own understanding of the findings derived through the interview. By multiplying the sum of points by the weight coefficient, the total aggregate amount of risks was obtained. Thus, the total score is evaluated based on the frequency and

expected losses from each type of fraud multiplied by the weight risks, i.e. the general importance which risk managers pay to particular types of risks.

**Figure 1: Risk map based on the evaluation of banks' risks**




**Source: Own research based on the findings of the interview**

As can be seen from the risk map illustrated above and the previous calculations, the most important risk in terms of the possible negative outcomes for the banks in terms of the combined impact of frequency and the expected amount of losses is hacker attacks, which is followed by the use of malware by perpetrators. These two risks impose major threats on banks, and precondition the need for the banking institutions to implement a robust system of cybersecurity and to adapt their measures for risk prevention steadily to the existing market realities in the changing external environment. The third major risk is phishing. Despite the fact that individual acts of phishing are not expected to bring major losses to banks, due to the high frequency of their occurrence, their aggregate possible outcome is very large, and hence they represent major threats to banks in the performance of their market activities. The main problem for banking institutions in this context is that they cannot deal directly with situations when phishing is directed by perpetrators on customers, and it is the responsibility of customers to make appropriate actions to protect themselves from such cases. The actual weight of DDoS attacks is slightly lower than the one of phishing, but it should not be neglected. If such attacks are well-organized and are of a mass nature, they can lead to major interruptions in the bank's operation in terms of not only online banking, but also the entire bank infrastructure. Finally, the smallest aggregate weight

belongs to the risks of customers' deliberate disclosure of their personal data on forums, in online social networks, etc., and to theft of data from customers' mail servers. The latter risk has a smaller frequency due to the fact that to perform such actions, perpetrators need to hack the servers of webmail providers, which requires significant expenses on their part and is associated with greater risks.

Now, based on the findings outlined above, what recommendations and suggestions can we develop for banks to improve the overall level of their cybersecurity and to avoid excessive risks in this domain?

First of all, we can recommend banks to adopt a systemic approach to the recognition and evaluation of risks. Without such a systemic approach which would allow covering all of the bank's business departments and business units, and in which all of the bank's stakeholders would be involved, it is virtually impossible to guarantee any high standards of cybersecurity. The operation of a dedicated cybersecurity department is a key prerequisite for the normal mitigation of risks. However, it is insufficient. All of the bank's departments should provide information on the risks incurred by them in the course of the bank's operation and the loopholes found in the bank's internal regulation associated with cybersecurity. This is required in order to develop and implement all countermeasures quickly, so as to restore the desired level of security.

One of effective approaches in this context might be to find the weakest link. As revealed by the interview with the manager of VersaBank, the company regularly resorts to the services of third-party professionals which imitate have attacks on the bank, thus providing opportunities for their cybersecurity department to respond to such threats and find the best solutions to eliminate them. This approach can be very effective. A proof can be found in RSM (2016) who states that "*The most common and effective form of cyberattack is through social engineering-that is, through contacting personnel by email or phone and duping them into disclosing confidential information that can subsequently be used to gain access to systems and data. Alternatively, emails can be opened by employees who unwittingly release customized and often quite sophisticated malware (the software used by hackers to infiltrate IT systems).*" When such activities are performed in a simulated environment, the bank's security services have the best opportunity to try different approaches to their resolution and to reveal the

weaknesses which exist in their current approaches to cybersecurity management, thereafter improving them for the sake of better security of the institution.

Regular trainings are thus required for all employees, including those who work at the cybersecurity department and all other whose activities need to take into account the bank's current approach to risk management. Such trainings are also required to prevent possible cases of internal leakages of confidential data and the implementation of unlawful activities on the part of the bank's own employees. In this context, effective managerial controls grounded in a risk-based approach are another key prerequisite for maximizing the effectiveness of the bank's corporate cybersecurity management.

Legal compliance is another critical factor for raising the overall quality of banks' protection measures in the field of cybersecurity. As noted by the Financial Stability Institute (2017), "*Recent high-profile cyber-attacks on financial institutions have focused attention on the need to strengthen cyber-security, leading to various official sector initiatives to address cyber-risk. At the international level, the G7 finance ministers and central bank governors issued a set of Fundamental elements of cybersecurity for the financial sector, with the aim of helping banks tailor their cyber-security approaches to their operational and regulatory environment.*" Thus, the efforts of the international community in the banking sector are directed largely to the improvement of the overall situation with cybersecurity risks for all actors in the market. Such efforts cover not only developed states, but also developing countries. The compliance with such national and international guidelines is an important step on the way toward the harmonization of international efforts in combatting international cybercrime. By complying with the legislative acts governing the field of cybersecurity, banking institutions can achieve an overall higher level of financial soundness, and thus can approach their audit more effectively, which is an essential step on the way to the optimization of banks' procedures associated with cybersecurity.

Of particular importance to banks is also the work with their customers. As a significant portion of risks is associated with the perpetrators' activities directed specifically at customers, banks need to provide information to their customers which would allow them being aware of all existing risks, and which would minimize the chances of perpetrators' success when targeting customers directly. Thus, banks should keep reminding their customers that they never ask any personal information of such

customers by phone or by e-mail, that customers should always watch the addresses in their browser's address bar, that they should never provide any confidential data in conversations to third parties, how they should preserve their PIN codes and passwords, and so on. The use of such basic and elementary approaches to personal security on the part of customers is one of the main prerequisites for the implementation of effective cybersecurity activities by banks in general, and for the maximization of the overall level of the bank's security.

If banks are able to implement effectively the recommendations provided above, they will be likely to improve their cybersecurity. At the same time, we can recommend banks to constantly monitor the innovative technologies in the market which are destined to improve the overall level of cybersecurity in financial institutions. Banks also need to invest funds in research and development for the purpose of creating own technologies. Such innovations can be important not only for raising their level of cybersecurity, but can also serve as a source of important competitive advantages for the financial institution to hold leading positions in its target market.

# Conclusion

The findings of this thesis prove that as of today, the financial sector on the international scale is vulnerable to a number of considerable threats. Namely, it is subject to the impact of the risk of fraudulent activities, which can be performed by a number of different external and internal perpetrators. The growing technological progress and steady advancement of technologies on the international level contribute to the expanding scope of services financial institutions are able to provide to their customers. This favors the quality of customer service. However, at the same time, advanced technologies can be put to use by perpetrators more effectively for achieving an unauthorized access to customers' funds or personal data.

In the light of these threats, banks and other financial institutions are required to pay particular attention to the organization of their security system and risk management activities. Given the fact that most operations are run in cashless form, and are driving toward the online environment, financial institutions should focus specifically on raising the quality of their security in this online environment. Such actions require effective cooperation on the part of all units and appropriate stakeholders, ongoing control and revision of the effectiveness of the risk management measures being implemented.

In the practical part of the thesis, a case study of the Canadian bank VersaBank was analyzed. The bank does not have physical branches and runs its business activities in the online environment.

The findings of the interview held with the manager of VersaBank allow stating that the bank believes cybersecurity to be one of the most important fields for ensuring the long-term stability of its commercial operations. The bank has to protect itself against a great number of cybersecurity threats, particularly in the light of the fact that it operates only in the digital environment. Among the most important threats, the bank's manager stated hacker attacks, use of malware, but also internal data leakages and cases when customers share their confidential data deliberately or as a result of being misled by perpetrators. Also, banks might undergo DDoS attacks which are not aimed at

stealing customer funds, but might breach the uninterrupted nature of the bank's operations.

The manager of VersaBank stated that the bank's security system is built on constant re-evaluation of threats and risks. The bank has a separate risk management department responsible for ongoing monitoring and response to threats. The bank resorts to third parties for modeling stress situations of real attacks. Other stakeholders are involved as well in the process of development of countermeasures for preventing fraudulent activities as well. The bank is also the world's pioneer in terms of the use of blockchain technologies for building a robust system of cybersecurity. The management monitors innovations in the market and seeks building its security system on the use of such innovations.

Based on the evaluation of the bank's risks in terms of cybersecurity, VersaBank can be advised to focus more on trainings for its employees to raise their skills of risk management and security, improved legal compliance procedures, and a greater emphasis on the work with customers for informing them of how excessive risks and threats can be avoided.

# Literature

ALEMANNO, Alberto, DEN BUTTER, Frank, NIJSEN, André, and TORRITI, Jacopo. *Better Business Regulation in a Risk Society*. London: Springer Science & Business Media, 2012. 328 p. ISBN 978-14-614-4405-3.

BESSIS, Joël. *Risk management in banking*. Fourth edition. Chichester: Wiley, 2015. ISBN 978-1-118-66021-8.

BOCK, Michael. *Governance Risk Management and Financial Product Development in Islamic Financial Institutions*. Munich: GRIN Verlag, 2010. 136 p. ISBN 978-36-407-1279-3.

BOOTH, Philip. *Modern Actuarial Theory and Practice, Second Edition*. London: CRC Press, 2004. 840 p. ISBN 978-15-848-8368-5.

BRODER, James F., and TUCKER, Eugene. *Risk Analysis and the Security Survey*. Amsterdam: Elsevier, 2011. 368 p. ISBN 978-01-238-2234-5.

FOUQUE, Jean-Pierre, and LANGSAM, Joseph A. *Handbook on Systemic Risk*. Cambridge: Cambridge University Press, 2013. 389 p. ISBN 978-11-072-7657-4.

FRASER, John, SIMKINS, Betty, and NARVAEZ, Kristina. *Implementing Enterprise Risk Management: Case Studies and Best Practices*. Hoboken, NJ: John Wiley & Sons, 2014. 688 p. ISBN 978-11-186-9196-0.

GRINSVEN, Jost H.M. *Improving Operational Risk Management*. Amsterdam: IOS Press, 2009. 240 p. ISBN 978-16-075-0420-7.

HERR, Hansjörg, and KAZANDZISKA, Milka. *Macroeconomic Policy Regimes in Western Industrial Countries*. London: Routledge, 2011. 296 p. ISBN 978-11-368-2167-7.

HONG KONG INSTITUTE OF BANKERS. *Operational Risk Management*. Hoboken, NJ: John Wiley & Sons, 2013. 256 p. ISBN 9780470827680.

HULL, John. *Risk management and financial institutions*. Fourth edition. Hoboken, New Jersey: Wiley, 2015. Wiley finance series. ISBN 978-1-118-95594-9.

CHAUDHURI, Arindam, and GHOSH, Soumya K. *Quantitative Modeling of Operational Risk in Finance and Banking Using Possibility Theory*. London: Springer, 2015. 16 p. ISBN 978-33-192-6039-6.

CHESINI, Giusy, GIARETTA, Elisa, and PALTRINIERI, Andrea. *The Business of Banking: Models, Risk and Regulation*. London: Springer, 2017. 239 p. ISBN 978-33-195-4894-4.

CHONGFU, Huang, and KAHRAMAN, Cengiz. *Intelligent Systems and Decision Making for Risk Analysis and Crisis Response: Proceedings of the 4th International Conference on Risk Analysis and Crisis Response, Istanbul, Turkey, 27-29 August 2013*. London: CRC Press, 2013. 950 p. ISBN 978-02-037-7147-1.

CHRISTOFFERSEN, Peter. *Elements of Financial Risk Management*. London: Academic Press, 2011. 344 p. ISBN 978-00-809-2243-0.

CHISHTI, Susanne, and PUSCHMANN, Thomas. *The WEALTHTECH Book: The FinTech Handbook for Investors, Entrepreneurs and Finance Visionaries*. Hoboken, NJ: John Wiley & Sons, 2018. 336 p. ISBN 9781119362180.

JOSEPH, Ciby. *Credit Risk Analysis: A Tryst with Strategic Prudence*. Delhi: Tata McGraw-Hill Education, 2006. 339 p. ISBN 978-00-705-8136-4.

KOULAFETIS, Panayiota. *Modern Credit Risk Management: Theory and Practice*. London: Springer, 2017. 234 p. ISBN 978-11-375-2407-2.

LAM, James. *Enterprise Risk Management: From Incentives to Controls*. Hoboken, NJ: John Wiley & Sons, 2014. 496 p. ISBN 978-11-188-3443-5.

LEVI, Maurice D. *International Finance: Contemporary Issues*. London: Routledge, 2007. 656 p. ISBN 978-11-343-9295-7.

LONE, Fayaz Ahmad. *Islamic Banks and Financial Institutions: A Study of their Objectives and Achievements*. London: Springer, 2016. 201 p. ISBN 978-11-375-1566-7.

LOUISOT, Jean-Paul, and KETCHAM, Christopher H. *ERM - Enterprise Risk Management: Issues and Cases*. Hoboken, NJ: John Wiley & Sons, 2014. 280 p. ISBN 978-11-185-3951-4.

MADURA, Jeff. *Financial Institutions and Markets*. London: Cengage Learning EMEA, 2008. 742 p. ISBN 978-03-246-5561-2.

MÁLEK, Jiří, ed. *Risk management 2014*. Praha: Oeconomica, 2014. ISBN 978-80-245-2062-9.

RAMIREZ, Juan. *Handbook of Basel III Capital: Enhancing Bank Capital in Practice*. Hoboken, NJ: John Wiley & Sons, 2014. ISBN 9781119330820.

SCANDIZZO, Sete. *The Validation of Risk Models: A Handbook for Practitioners*. London: Springer, 2017. 242 p. ISBN 978-11-374-3696-2.

TAUSSIG, Frank W. *Principles of Economics, Volume 1*. London: Cosimo, Inc., 2013. 572 p. ISBN 978-16-020-6342-6.

TEIGLAND, Robin, SIRI, Shahryar, LARSSON, Anthony, PUERTAS, Alejandro Moreno, and BOGUSZ, Claire Ingram. *The Rise and Development of FinTech: Accounts of Disruption from Sweden and Beyond*. London: Routledge, 2018. 444 p. ISBN 9781351183604.

VENTO, Gainfranco A., and LA TORRE, Mario. *Microfinance*. London: Springer, 2006. 175 p. ISBN 978-02-306-2758-1.

VIT, Gregory B. *The risk in risk management: financial organizations & the problem of conformity*. New York, NY: Routledge, 2013. 160 p. ISBN 978-0-415-50984-8.

WEBER, Dennis, and MARRES, Otto. *Taxing the Financial Sector*. Amsterdam: IBFD, 2012. 214 p. ISBN 978-90-872-2141-6.

YOUNG, Mary Alice. *Banking Secrecy and Offshore Financial Centers: Money Laundering and Offshore Banking*. London: Routledge, 2013. 190 p. ISBN 9780415526326.

## Internet sources

*BASEL III* [online]. [cit. 2018-04-11]. Available from: http://www.bis.org/bcbs/basel3.htm

*CAMPBELL, Neil. Cyber Security Is A Business Risk, Not Just An IT Problem.: Forbes* [online]. 2017 [cit. 2018-04-11]. Available from: https://www.forbes.com/sites/edelmantechnology/2017/10/11/cyber-security-is-a-business-risk-not-just-an-it-problem/#6d69f55d7832

*DELOTTE. PSD2 – Payment Services Directive 2* [online]. 2016 [cit. 2018-04-11]. Available from: https://www2.deloitte.com/lu/en/pages/banking-and-securities/articles/psd2-revised-payment-services-directive.html

*DROLET, Michelle. 8 cybersecurity trends to watch for 2018.: Financial Stability Institute* [online]. 2017 [cit. 2018-04-11]. Available from: https://www.csoonline.com/article/3241242/data-protection/8-cybersecurity-trends-to-watch-for-2018.html

*EUROPEAN COMMISSION. Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments* [online]. 2017 [cit. 2018-05-14]. Available from: http://europa.eu/rapid/press-release_MEMO-17-4961_en.htm

*FINANCIAL ACTION TASK FORCE. About* [online]. 2017 [cit. 2018-05-14]. Available from: http://www.fatf-gafi.org/

*Financial stability institute. Regulatory approaches to enhance banks' cyber-security frameworks* [online]. 2017 [cit. 2018-04-11]. Available from: https://www.bis.org/fsi/publ/insights2.pdf

*FX STREET. Cryptocurrency market overview: VersaBank Inc., will offer secure vault for digital assets.*[online]. 2018 [cit. 2018-04-11]. Available from: https://www.fxstreet.com/news/cryptocurrency-market-overview-VersaBank-inc-will-offer-secure-vault-for-digital-assets-201802191057

*IBM. Basel III Summary* [online]. 2017 [cit. 2018-05-14]. Available from: https://www.ibm.com/support/knowledgecenter/en/SSN364_8.8.0/com.ibm.ima.tut/tut/bas_imp/bas3_sum.html

*ISKYAN, Kim. Here's the story of how a guy making $66,000 a year lost $7.2 billion for one of Europe's biggest banks* [online]. 2016 [cit. 2018-05-28]. Available from: http://www.businessinsider.com/how-jerome-kerviel-lost-72-billion-2016-5

*MARKS, Norman. The Wells Fargo Fraud: Where Was Internal Audit?* [online]. 2016 [cit. 2018-05-28]. Available from: https://www.cmswire.com/information-management/the-wells-fargo-fraud-where-was-internal-audit/

*MOK, Anna, and SAHA, Ronnie. Strategic Risk Management in Banking.: Inside Magazine* [online]. 2017 [cit. 2018-04-11]. Available from: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/Banking/lu_inside_issue14_strategic_risk_management.pdf. 16 p.

*NANCE, Mark T. The regime that FATF built: an introduction to the Financial Action Task Force* [online]. 2017 [cit. 2018-05-14]. Available from: https://link.springer.com/article/10.1007/s10611-017-9747-6

*OSBORNE, Charlie. MoneyTaker hacking group steals millions from US, UK, Russian banks.* [online]. 2017 [cit. 2018-04-11]. Available from: http://www.zdnet.com/article/moneytaker-apt-steals-millions-from-us-uk-russian-banks/

*PANETTA, Kasey. 5 Trends in Cybersecurity for 2017 and 2018.: Financial Stability Institute* [online]. 2017 [cit. 2018-04-11]. Available from: https://www.bis.org/fsi/publ/insights2.pdf

*PSD II.* [online]. 2017 [cit. 2018-04-11]. Available from: https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

*REUTERS. Taiwan's Far Eastern International fined T$8 million over SWIFT hacking incident.: Reuters* [online]. 2017 [cit. 2018-04-11]. Available from: https://www.reuters.com/article/us-far-eastern-fine/taiwans-far-eastern-international-fined-t8-million-over-swift-hacking-incident-idUSKBN1E60Y3

*RODRIGUES, Jason. Barings collapse at 20: How rogue trader Nick Leeson broke the bank.: The Guardian* [online]. 2018 [cit. 2018-05-28]. Available from: https://www.theguardian.com/business/from-the-archive-blog/2015/feb/24/nick-leeson-barings-bank-1995-20-archive

*ROMAN, Jeffrey. Chase Breach Affects 76 Million Households.: BIS* [online]. 2018 [cit. 2018-04-11]. Available from: https://www.bankinfosecurity.com/chase-breach-affects-76-million-households-a-7395

*ROY, Anup, and GHOSH, Joydeep. Nirav Modi PNB fraud: How bank auditors failed to detect scam in 6 years.* [online]. [cit. 2018-04-11]. Available from: http://www.business-standard.com/article/finance/pnb-fraud-how-bank-auditors-failed-to-detect-the-scam-in-six-years-118021901425_1.html

*RSM. How banks can increase cybersecurity risk management.* [online]. [cit. 2018-04-11]. Available from: http://rsmus.com/our-insights/newsletters/financial-institutions-insights/how-banks-can-increase-cybersecurity-risk-management.html

*SEDDON, Max. The hacker, hacked: national criminals attack Russian banks.: Financial Times* [online]. 2018 [cit. 2018-04-11]. Available from: https://www.ft.com/content/b813ab48-1b04-11e8-aaca-4574d7dabfb6

*THE JAPAN TIMES. Hackers stole $6 million from Russian bank via SWIFT system, central bank says.* [online]. 2018. [cit. 2018-04-11]. Available from: https://www.japantimes.co.jp/news/2018/02/16/business/financial-markets/hackers-stole-6-million-russian-bank-via-swift-system-central-bank-says/#.WrNh8C5uZjE

*THE LONDON FREE PRESS. VersaBank takes steps towards launching blockchain-based cryptocurrency vault.* [online]. 2018 [cit. 2018-04-11]. Available from: http://lfpress.com/pmn/news-pmn/canada-news-pmn/VersaBank-takes-steps-towards-launching-blockchain-based-cryptocurrency-vault/wcm/8686563e-5a54-40b5-a673-72beafbe53f4

*THOMSON, Ian. Hackers nick $60m from Taiwanese bank in tailored SWIFT attack.: The Register* [online]. 2017 [cit. 2018-04-11]. Available from: https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/

# Annexes

## Annex 1. Structure of the Interview with VersaBank's Manager

1. Do you feel your bank is threatened considerably by perpetrators in terms of cybersecurity?
2. Do you believe there are any major differences in terms of cybersecurity between traditional and digital-only banks?
3. What types of cybersecurity threats do you believe to be the most dangerous?
4. What kinds of attacks are more dangerous in your opinion: those directed against the vulnerabilities in the bank's protection system or those which are directed to steal information from customers?
5. Have there been any major attacks against your bank?
6. How is your security system built in terms of organization and in technical terms?
7. How can you monitor the innovations in the field of cybersecurity and implement them?
8. What are the most common ways using which perpetrators steel data and/or funds from your bank's customers?
9. What could you recommend to customers in order to save their funds against possible attacks on the part of perpetrators?
10. In your opinion, what will be the main trends in the banking industry in the years to come in terms of hacker attacks and banks' response to them?
11. What risks would you believe as the most important for your bank in particular?