24-osios Lietuvos jaunųjų mokslininkų konferencijos „Mokslas – Lietuvos ateitis“ teminė konferencija
Proceedings of the 24th Conference for Junior Researchers "Science – Future of Lithuania"

EKONOMIKA IR VADYBA / ECONOMICS AND MANAGEMENT

2021 m. spalio 21 d., Vilnius, Lietuva
21 October 2021, Vilnius Lithuania

eISSN 2029-7149
eISBN 978-609-476-279-6
Article Number: vvf.2021.063

Finansų valdymas / Financial Management *http://jmk.vvf.vilniustech.lt*

RISK ASSESSMENT RELATED TO FINANCIAL CRIMES IN FINTECH

Jelena STANKEVIČIENĖ, Agata TOMAŠEVIČIŪTĖ*

Business Management Faculty, Vilnius Gediminas Technical University,
Saulėtekio al. 11, LT-10223 Vilnius, Lithuania
*E-mail: *agata.tomaseviciute@stud.vilniustech.lt*

Abstract. Aim of the paper is to investigate risk and financial crimes in financial technology companies, as well as consolidate agenda for future research. Methods to be used analysis of the content of related scientific literature, analysis and summary of risk assessment and management standards.The paper provides definition of FinTech, examines some grow statistics, and reviews the theoretical literature. Risk analysis is critical factor to a successful construction of a project or successful companies' existence, as FinTech companies primary focused to provide fast (efficient) service it tends to forget precautions measure to protect their businesses and their end customer. This paper focused to evaluate literature and researches on FinTech and it facing risks and kick of with the first steps of the research for the future works. Novelty of this paper is connected to the gap where young FinTech, per se Start-ups are not fully prepared for the regulatory/cyber security challenges. Currently there is a limitation for the related data collection, as the limited sample of size is identified there is a risk that not experts to call back. Not publicly available information; Main raised question of the paper is which area of possible risk can cause higer chance of financial crimes between the FinTech companies. Methods which to be used for the reasearch are: Analytic Hierarchy Process (AHP) and Technique for Order Preference by Similarity to Ideal Solution TOPSIS.

Keywords: risk assessment, risk management, FinTech, financial crimes, anti-money laundering directive, AHP.

Introduction

FinTech[1] is contemporary, despite the fact that the exchange between technology innovation and financial services is certainly not a new topic. It has been talked about a considerable amount in the previous few decades. For instance, Berger (2003), examined the profitability and customer welfare assistance implications of data innovation for banking. Also, twenty years prior, in a conversation of combination in financial services, it was concluded with the perception that the progressing consolidation around then was probably going to be followed by specialization-incited discontinuity in the financial services industry. It was guessed that information technologies would support the rise of particular players making an ever-expanding set of market specialties with more better product customization to take into account client preferences (Thakor, 1999).

In a sense the thing that we are noticing today. As Frame, Wall, and White (2018) bring up, technological change that creates financial innovations in banking has implications for improvements in FinTech. Lending, non-intermediated peer-to-peer (P2P), smart contracts, cryptocurrencies are altogether parts of an arising new puzzle of technology helped customized financial services. Maybe one part of this improvement that is fairly exceptional and subsequently surprising is the degree to which these innovations include non-intermediated transactions.

Due to these days fast evolving new technologies which bring together with them easier connections not only for communications or cross-border transfers solutions for people living around the globe but also brings a gap for fraudsters[2] to action their plans once valuable opportunity exists. As a smartphone or a computer with stable internet has gradually become a standard of a minimum wealth being – it gives possibility to use these tools for all

[1] Short for Financial Technology.
[2] A person who commits fraudulent activity, especially in business dealings.

© 2021 Jelena Stankevičienė, Agata Tomaševičiūtė. Leidėjas Vilniaus Gedimino technikos universitetas. Šis straipsnis yra atvirosios prieigos straipsnis, turintis Kūrybinių bendrijų (Creative Commons) licenciją (CC BY 4.0), kuri leidžia neribotą straipsnio ar jo dalių panaudą su privaloma sąlyga nurodyti autorių ir pirminį šaltinį.

possible purposes. One of key issue that can be indicated that not all FinTech companies are not ready to balance the desire to grow new business and provide better customer services in chosen sector, while not having a correctly introduced or adjusted countermeasure of protection. As a part of the novelty of this paper is connected to the gap where young FinTech companies, Start-ups per se as one of the instances are not fully prepared for the regulatory/ cyber security challenges.

Main raised question of the research is: What risk financial crimes causes to FinTech companies?

Purpose of the paper is to investigate risk which would lead to financial crimes in financial technology companies, as well as consolidate agenda for future research. Methods to be used – analysis of the content of related scientific literature, analysis and summary of risk assessments and management standards.

1. Literature review

As in modern society, technology is attracting more and more people's attention – it has become more common to see new products on the market every day, surprising with creativity and innovation. We can see these days we have a bigger tendency of collaboration between the information and communication technology innovations which have triggered big changes in the field of financial services which now being called as a separate unit of financial services – FinTech. FinTech is an international term used as an interdisciplinary subject that combines finance, technology management and innovation management (Leong & Sung, 2018).

As a FinTech is still not fully distinguish term or would say a definition and its usage accelerated with a speed that no one could predict, especially during a bubble and hype period in 2015/2016 (Buckley et al., 2019). As there are many different not fully defined definitions below table indicates most popular defined ones.

Table 1. Definitions of FinTech

Author(s) and year	Main idea(s) of the definition
(Buckley et al., 2019)	FinTech stands for the application of technology in the financial industry. It is not limited to specific model (e.g., wealth management sector) or a specific sector (e.g., lending) it covers majority to finance related services and products.
(Financial Stability Board [FSB], 2019)	It is a technological innovation which can help to boost market access, introduce new product and tools to offer and minimize costs for end customer. Opposite to traditional financial intermediaries, FinTech companies are not regulated.
(Micu & Micu, 2016)	It is a Financial technology which is new to finance an industrial sector covering the full range of technologies used finance to facilitate trade, business interaction and services, provided to the retail consumer.
(Varga, 2017)	FinTech is a modern way of doing different types of transactions that enhance and creates financial industry. FinTech solutions can be offered and not limited by innovative start-ups and mature, establishes FIs.
(Chen et al., 2013)	FinTech is an enterprise that is not being regulated in the legal system or only partially regulated. The main task of FinTech is to provide financial solution services through new technology. They are enterprises which main goal is to provide innovative services by going beyond traditional scope.
(Lietuvos bankas, 2018)	FinTech is a technology-based financial innovation that helps create new business models, business applications, processes, and products. These innovations have a significant impact on financial markets, institutions, and financial services.

All definitions mentioned in Table 1 show an important aspect of subjectiveness of the FinTech, only closer to 2019 we have more broader definition. Presented definitions show a crucial part of FinTech, namely the lack of a clearly defined limit of its activity. As we can notice its activity focuses on two areas: technological and financial services, which makes it difficult to reliably assess its size and identity of the risks related to it. Therefore, evolving a one definition is particularly important as FinTech companies have been pro-active players on financial service market for a good time, and its activities are not so restrictively regulated as much as traditional entities.

Currently FinTech can provide financial services on the basis of subject by subject. It is commonly used in the areas as e-payments, financing, infrastructure provisions by using modern solutions of technologies to provide financial services. If to believe data report from KMPG beginning of 2019 global investment in FinTech companies has reached 37.9 billion USD (Pulse of FinTech H2'19 – Global Trends – KPMG Global, 2019) but the end of the year had pinged a record of investment which ended up with 135.7 billion USD. In comparison with 2018, were investments were reached 118.8 billion shows a slight increase of investment, for some extent Ant Financial raised $14 billion, or Worldpay acquisition by Vantiv valued $12.9 billion. Top stars of that the last year which had targeted a record of investment: acquisition of First Data by Fiserv with 22$ billion USD (US) and the 42.5 billion worth acquisition of WorldPay (UK) by Fidelity National Information Services (Pulse of FinTech H2'19 – Global Trends – KPMG Global, 2019).

Seeing the innovativeness of financial technologies and the value they create countries around the globe strive to create a suitable and sustainable microclimate for the development of financial technology start-ups. Lithuanian created conditions for the development of financial technologies are being welcomed worldwide.

During FinTech Inn World Conference in 2019 which took place in Lithuania a record number of participants (over 3,000) attended this event, such data show that Lithuania is becoming known on the world map of FinTech and gives hope for the growth of the country's economy (FinTech Market Leaders from around the World Gather in Vilnius | Ministry of Finance of the Republic of Lithuania, n.d.).

According to Global FinTech rankings Lithuania is counted as a second Europe's FinTech center and a fourth in the Globe (as a second Baltic state is Estonia – counts in the TOP 10 (Eriksonas, 2018; Invest in Lithuania. 2020).

By reviewing this we can assume that big is not better than small, Lithuania is showing the world that small locations can make a big difference (Invest in Lithuania. 2020; The Global FinTech Index 2020, 2020). By seizing opportunities to make for FinTech enterprises to establish and pairing that with the advantages of rule that give companies based there to trade across the European Union. In Lithuania there are three mostly growing industry type: lending, payments, and banking. Worth to mention that due to increase number of aforementioned industries Compliance and AML analysts becoming one of top needed employees on the Lithuanian market.

1.1. FinTech facing risks

FinTech sector has unique combination of exposures that are not contemplated by traditional financial institutions products. Although numerous researchers and practitioners have a believe that FinTech can reshape the longer term of the financial industry, the adoption of FinTech adoption is still unclear. Most adoption barriers are risk issues such as regulation (e.g., legal uncertainty for adoption), financial (e.g., loss of monetary outcome and extra fee), operational (e.g., inadequate processes or systems of FinTech companies), security and privacy (e.g., vulnerability of security technologies) concerns. Clients would like to determine the arithmetic mean of FinTech adoption considering its benefits also as risks at an equivalent time, and accordingly make an adoption decision when its benefits are greater than its risks. Therefore, FinTech companies are challenged particularly to increase the potential benefits and reduce the potential risks once they offer FinTech to customers (Crouhy et al., 2008; Financial Inclusion Centre, 2018; Liu et al., 2020).

Beyond all the risk that exists that are being seen – in some areas they are overlapping or brings a suggestion for potential new areas of risk to for organisations to be associated with. To narrow more trending risk Table 2 was created which seems to be most relevant this year (2020) despite all traditional risks which are meant to be permanent for foreseeable future.

Table 2. Risk to FinTech of 2020 (source: Crated by the author of analysed works of (Chenyakov & Chernyakova, 2018; Christoffersen, 2011; Crouhy et al., 2008; European Banking Authority [EBA], 2020; Jorion, 2011; Thakor, 2020; Zhu & Chen, 2016)

Type	Description
Professional liability	Failing to take proper care over negligent advice and failing to provide to the customer are quite common risks for companies that provide financial services, to great extend FinTech that offers new financial solutions through new distribution models.
Embezzlement[3]	As a sector (FinTech) is dealing with a vast frequency of money movement. Big amounts of payments being processed, transaction and client accounts, and fast growth and automation or new technology implementation gives vulnerable space for theft. Theft can be external individuals or an employee.
Regulatory environment	New products, new solutions, new technology, new distribution gives not only a wealth opportunity, but a regulatory exposure. FinTech enterprises must ensure that they are on an ongoing basis implementing and enhancing risk management systems.

[3] The act of withholding assets for the purpose of conversion / Robbery of Funds.

End of Table 2

Type	Description
Technology failures	New methods of technology are essential for FinTech enterprises – it is a secret key how they have disrupted traditional financial sector. As these types of companies have huge reliance of technology infrastructure it means that they can be vulnerable. As of one consequences of technological failure we can count an error when customer cannot access services resulting in loss of customer and income.

The uncontrolled spread of the shadow economy, which has a negative impact on the country's economic and political life, poses a serious threat to the state and society. Financial crime is on the rise, it is becoming more and more international, and the ways in which it is committed are becoming increasingly difficult. The "shadow economy" is defined as a process that adversely affects the state's tax revenue and involves acts contrary to the law, which evade tax obligations or seek other illegal tax benefits. The most damaging components, according by Prosecutor General's Office of the Republic of Lithuania (Lietuvos Respublikos generalinė prokuratūra, 2013) the shadow economy:

- smuggling and illegal circulation of excisable goods.
- carrying out unregistered economic activities and / or avoiding income accounting and illegal work.

Lithuania's unstable economic situation and high unemployment create preconditions for the growth of the shadow economy and the increase in the number of criminal acts and other violations of the law of the financial system. Economic and financial criminal acts cause significant damage to the property, property rights and interests of individuals, as well as to the state economy, business order, and financial system. Economic and financial crimes include money laundering, fraud, embezzlement or waste, production and sale of counterfeit money, smuggling, and infringements of intellectual property rights. Economic-financial crimes can be divided into:

- crimes and criminal offenses against property, property rights and property interests;
- crimes against intellectual and industrial property;
- crimes and criminal offenses against the economy and business order;
- crimes and criminal offenses against the financial system (European Parliament and the Council of the European Union, 2015); International Business Machines [IBM], 2020; Muhtaseb, 2020).

In current transactions and payments environment of developing security risk, regulation, customer expectation, approaches based on data science, Artificial Intelligence, machine learning, big data computing have possible new, real threats. All potential financial crimes can occur both in standard FI or FinTech's as each of the sector companies trying to follow and enhance their systems and procedures to attract new and keep existing customers.

2. Risk assessment methods

The risk management process is critical for any enterprise. Risk measurement includes determining the level of risk for each objective and assessing the risk analysis using a variety of methods and technologies (Zavadskas et al., 2010). Risk management methods depends on the risk environment and the context of the business. Risk management in organizations level is one of the components of strategic management.

The FinTech sector is characterized by dynamism, faced with different situations, because each project, industry type of FinTech is unique, so the creation of a model is an important aspect. The models are easily adapted to the industry type of companies. By harmonizing the life cycle process, a smooth planning process and project management can be ensured. Risk is the probability that, under certain circumstances, a negative event may occur (Gegužienė et al., 2019). The risk analysis assesses the significance of each risk (Figure 3). Risk management methods depends on the risk environment and the context of the business (Figure 1).

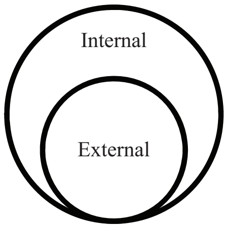


Figure 1. Type of risks

Internal risk is controlled, and its management and control depend on the organization ongoing strategies. External risk is uncontrollable, it depends on external factors, such as economic situation, politics, and so on. Accidents at work are classified as internal enforcement and management risk. The goal of risk management is value creation and protection. The principles set out in this Regulation are the basis for risk management and should be considered in the determination the organization's risk management system and (ISO, 31000: 2018).

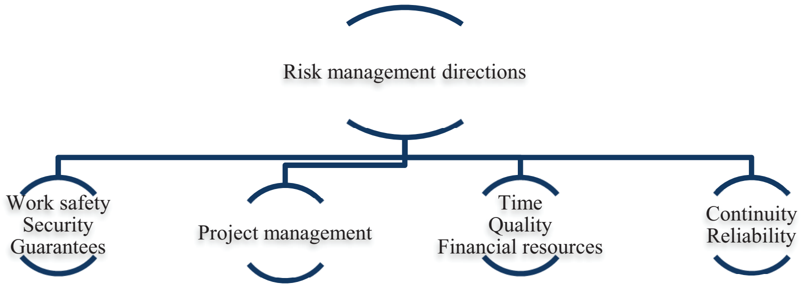


Figure 2. Risk management directions

Risk is an indefinite effect that affects an organization's goals, and therefore it is beneficial for the organization to integrate risk management into its activities and functions. Risk management effectiveness depended on its integration into the management of the organization, including decisions adoption (Figure 2). The organization should evaluate its existing risk management practices and processes, assess any gaps, and address those gaps in the system. Risk assessment consists of risk identification, risk analysis and risk assessment. In the first stage of risk assessment, the risk is identified, in the second stage, the nature of the risk is determined. In the third stage, a comparison process is carried out between the analysis results and the risk criteria obtained and the acceptability of the risk is determined. Risk assessment assistance shall address what action needs to be taken to prevent threats. The decision is made to avoid, transfer, maintain or reduce the risk.

Risk identification identifies risk factors and their characteristics. Risk can be identified in two directions, when it is determined what can happen and what the consequences of that event will be, and when it is predicted what consequences can be and investigate what caused it (Faraji Sabokbar et al., 2016). Risk identification is one of the most important parts of risk assessment. The more potential risk factors are identified, the greater the likelihood of reducing the risk or its to avoid. Risk analysis can be qualitative and quantitative. According to Zwikael (2009), quantitative the task of the analysis is to quantify the impact of changes in risk factors on project effectiveness evaluation. The risk is assessed during the qualitative analysis the probability that each risk factor may or may not occur is determined risk factor influence, risk factors are ranked by probability or influence on the project. Quantitative risk analysis is numerically analyzed the likelihood of each risk factor or its consequences for the objectives of the project, the degree of impact for the entire construction project. Quantitative analysis is performed with those factors that have been sorted according to priorities in the qualitative risk analysis as potential and able to do the greatest impact on the project.

Multiplying the risk probability score by the impact score gives a comprehensive assessment and determines the significance of the risk. The assessed risk factors can be set out in a matrix according to which risk management measures are selected. An example of a risk matrix is shown in Figure 3. Green indicates low risk, yellow indicates medium risk, red indicates high risk.

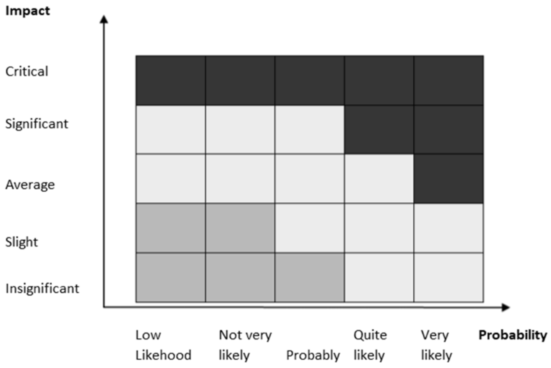


Figure 3. Matrix of risk

All in all, researches had been focusing on many areas related to FinTech's although there is not align approach how the companies can be evaluated to existing outrages – especially

3. Methodology

In the process of the review theoretical research was applied to investigate the literature. As for the future research one of Multiple-criteria decision methods to be chosen.

In the Qualitative risk assessment strategies include programs which would include "consider the possibility" checklist, task analyses, safety audits, the sequentially timed event plotting (STEP) strategy and Hazard and Operability study (HAZOP). Quantitative evaluation methods incorporate the relative proportional risk assessment (PRAT), the decision matrix risk assessment (DMRA) procedure, and weighted risk assessment (WRA). Half and half procedures incorporate Fault-tree Analysis, Human Error Analysis Techniques, Event Tree Analysis and so on (Kokangül et al., 2017). Likewise, the Analytic Hierarchy Process (AHP) strategy is another strategy usually utilized as a risk appraisal procedure practically speaking (Padma & Balasubramanie, 2007; Yulong et al., 2008). Albeit a portion of these methods, (for example, AHP) yield just a risk score, different techniques, (for example, Fine Kinney) yield risk scores and risk classes of each risk. For examined topic one of Multi Criteria Decision Making methods was chosen – AHP. The AHP (Beaumont, 1984; Saaty, 1977, 1990, 2003) is approach to deal with quantifiable as well as theoretical criteria in the decision-making process. It is a multi-objective multicriteria dynamic methodology that depends on the possibility of pairwise examinations of options as for a rule (e.g., which alternative, An A or B, is liked and by the amount more is it liked) or regarding a goal (e.g., which is more significant, A or B, and how much more significant is it). By utilizing pairwise examinations, the general significance of one model over another can be easily assessed. This idea was developed by Thomas Saaty in the 1970's.

By utilizing a hierarchical structure, AHP encourages one settle on choices when an unpredictability of objectives and criteria are included (Dyer, 1990). When the chain of command is set up, the rules within the hierarchy order are assessed dependent on combined correlations. The components are compared in relative terms to it similarly as with their significance or commitment to a given standard that possesses the level promptly over the components being compared. The last weights of the components at the lower level of the hierarchy of command are acquired by adding all the contributions of the components in a level concerning all the components in the level above. This is known as the standard of hierarchic (Saaty, 2003; Vargas, 1990).

An AHP-based risk assessment instrument to introduced in upcoming research for a proficient methodology for overseeing risks in FinTech. This methodology will coordinate preventing income losses and guaranteeing wellbeing into venture risk evaluation utilizing a maldistributed decision-making technique. The proposed structure will utilize the AHP method for making the pairwise examination of the risk criteria introducing a dependable ranking of these risk by analyzing solid decisions. A questionnaire to be created for the criteria to be reviewed and ranked by the experts afterwards questionnaire to be checked for the reliability by using Cronbach's alpha. Received answers from the experts to be reviewed and rank as per indication. Afterwards new tool to be created for enterprises to utilize by evaluating their position and readiness in terms of security and exposure to financial crimes risk.

Sampling size for the experts to be calculated using finite population formula:

$$n = \frac{z^2 N_p^2}{\left(N-1\right)e^2 + z^2 o_p^2}, \tag{1}$$

N – size of population, n – size of sample, e – acceptable error, o_p – standard deviation of population, z – number relating to the degree of confidence.

As the population is small the sample size can be reduced by utilizing the formula:

$$n = \frac{n_0}{1+\frac{\left(n_0-1\right)}{N}}. \tag{2}$$

To assess the criteria's' and their effect multiple criteria decision analysis (MCDA) methods (or multicriteria methods) are widely used. TOPSIS methods was analyzed and applied to evaluate the financials of a popular approach to multiple criteria decision analysis (MCDA) developed by Hwang and Yoon.

TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) it's a multi-criteria decision analysis method, which was originally developed by (Hwang & Yoon, 1981) with further developments. TOPSIS is based on the concept that the chosen alternative should have the shortest geometric distance from the positive ideal solution and the longest geometric distance from the negative ideal solution. Compensatory methods such as TOPSIS allow trade-offs between criteria, where a poor result in one criterion can be negated by a good result in another criterion.

TOPSIS is carried out in 7 steps:

1. Creating normalized decision-making matrix which consist of m alternatives and n criteria, with the intersection of each alternative and criteria given as *xij*, with the matrix $(x_{ij})m \times n$.

$$\underset{ij}{\overline{x}_{\cdot\cdot}} = \frac{x_i}{\sqrt{\Sigma_i^n - x_{ij}^z}}. \tag{3}$$

2. Calculation of weighted with normalized decision matrix:

$$\hat{x}_{ij} = \overline{x}_{yij}. \tag{4}$$

3. Determine the best and the worst alternative from all alternatives:

$x\_pj = \left[\max\right]\_ix_{\left(ij_,\right)}$ when the best indicator has the maximum value;

$x\_pj = \left[\min\right]\_ix\_\left(ij_,\right)$ when the best indicator has the maximum value;

and

$x\_bj = \left[\max\right]\_ix\_\left(ij_,\right)$ when the best indicator has the maximum value;

$x\_bj = \left[\min\right]\_ix\_\left(ij_,\right)$ when the best indicator has the maximum value.

4. Calculate the distance between the alternative ί and best condition:

$$d_P i = \sqrt{\sum_{j=1}^{n}\left(\underset{ij}{x_{\ddot{y}}} - \underset{\beta pj}{x}\right)^2}. \tag{5}$$

5. Calculate the distance between the target alternative ί and the worst condition.

6. Calculate for each alternative relative distance from the ideal alternative to worst:

$$K_i = \frac{\mathrm{d}_{bi}}{d_{pi}\mathrm{i} + \mathrm{d}_{bi}} \tag{6}$$

7. Rank the alternatives according to gathered results.

For the this paper research these methodologies to be chosen in order to change qualitative data into the quotative which can mean measured at the same point if to follow this methods.

4. Results and discussion

After the calculation it was revealed that 9 experts to be interviewed for the data collection in the upcoming research (the calculations were made in Eqs. (7) and (8). Experts were chosen to be questioned although only 8 were capable to answer. Experts were questioned to evaluate risks that effect the company. The questionnaire was structured to collect data where experts indicates most risky areas in the company that can lead to financial crimes. 10 criteria determined as factors influencing a business performance were used in applying TOPSIS method (Table 3 in Section 4 with the received results). All factors were set as criteria because usually a firm would concentrate on maximization the efforts to keep most efficient and save way to keep business running. The higher the result of the factor, the higher importance of a factor. In order to have a fair and not subjective view, the weights to the criteria were equally set by calculating the average of all received score for each factor separately by calculating averages of each factor collected scores. From all collected factors the biggest attribute weight was given to Operational Risk right after goes Regulatory Risk with Credit Risk meaning they cost bigger exposure to the financial crimes. Lowest scores were given to Market and Liquidity risks.

After the calculations it was determined that 15 experts to be taken as a sampling (formula number 2).

$$n = \frac{2.57^2 \times 17 \times 2_p^2}{\left(17-1\right)0.5^2 + 2.57^2 \times 2_p^2} = 14.765. \tag{7}$$

At last it was calculated to have 9 special mater experts (formula 4)

$$n = \frac{14.765}{1 + \frac{\left(14.765-1\right)}{17}} = 8.15. \tag{8}$$

After the literature review there were barely found any previously made research that would fully analyze factor/risks that lead to financial crimes. One of the biggest limitations was a statistical data collection for previous year as nor data base is storing such information.

Using TOPSIS method below results were collected from the experts (Table 3). Attribute weights have been calculated for each of the factors.

Table 3. Initial decision matrix (compiled by author)

Factor number	Factor	min./max.	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5	Expert 6	Expert 7	Expert 8	Attribute weights
x1	Market Risk	1 5	1	4	3	2	2	3	2	1	2,250
x2	Environmental, Social, Governmental Risk	1 5	4	5	3	5	4	3	4	4	4,000
x3	Business Risk	1 5	2	3	2	3	5	3	5	3	3,250
x4	Financial Risk	1 5	4	3	2	3	3	3	2	4	3,000
x5	Operational Risk	1 5	5	5	5	5	5	5	5	5	5,000
x6	Liquidity Risk	1 5	1	2	2	3	3	2	2	3	2,250
x7	Regulatory Risk	1 5	4	5	5	5	5	5	5	5	4,875
x8	Reputational Risk	1 5	4	3	2	3	4	3	2	3	3,000
x9	Counterparty Risk	1 5	4	5	4	4	5	4	3	4	4,125
x10	Credit Risk	1 5	5	4	5	5	3	5	5	5	4,625

After the calculations (Table 3 and 4, 5) it was determined that from all questioned experts the best alternative/highest risk is given by the third (rating score 0,53) and very close to it was alternative number one (rating score 0,52) and alternative number 7. As per best alterative (Expert #3) highest risk is caused by Operations, Regulatory environment and Credit factors.

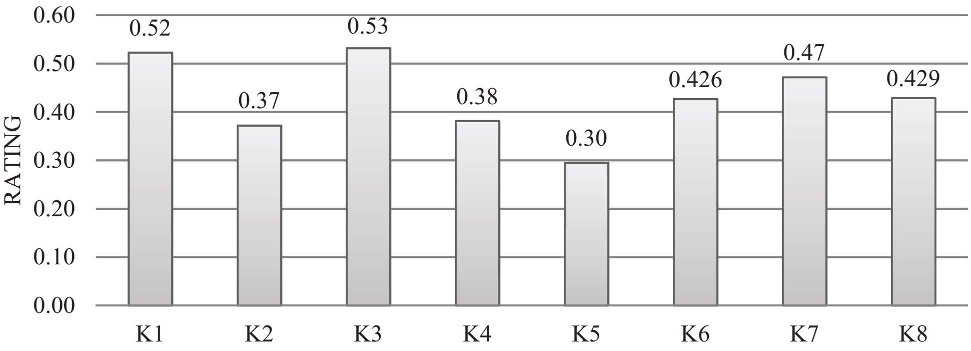
Table 4. Best alternative from all collected (consolidate by the author from collected data)

Rank	Expert Nr	Rating weights
1	3	0.53
2	1	0.52

End of Table 4

Rank	Expert Nr	Rating weights
3	7	0.47
4	8	0.429
5	6	0.426
6	4	0.38
7	2	0.37
8	5	0.30

Table 5. Alternative ratings weights received from the calculations (consolidate by the author from collected data)



Note: K letter – corresponding to the number of the expert.

Operational Risk was chosen to be evaluated more in depth as a research was conducted in back office. 4 subcategories were evaluated: Process, Technology, People, External Risks. After the calculation of separation from negative ideal solution – the rating of Operations Risk criteria was distributed as follows: first is Technology criteria (most risky), second is Process risk together with Human risk and lastly is External Events Risk. Data of Selected Criteria and best alternatives indicating the highest risk are showed in the Table 6 till 9. For the Technology Risk *cybersecurity* was indicated at the higher exposure were *hardware* at the lowest. For the People Risk *lack of adequate product knowledge and skill set* together with Unauthorized Activity and Employee Fraud had scored as the most exposed factors. Looking at the External Events Risk it is noticeable to notice that *outsourcing service* and *external fraud activities* are most harmful according to the experts. As for the Process Risk many inside criteria were ranked very closed to each other: *ineffective procedures, internal data, external data, client services and interactions* were most rank at the highest scores by the experts. Surprisingly, cost saving due to negligence of the management was ranked as the lowest risk alternative from all given.

Table 6. Technology Risk

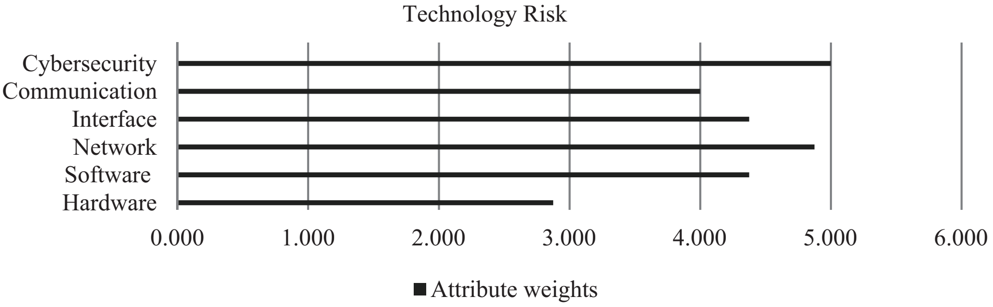


Table 7. People Risk

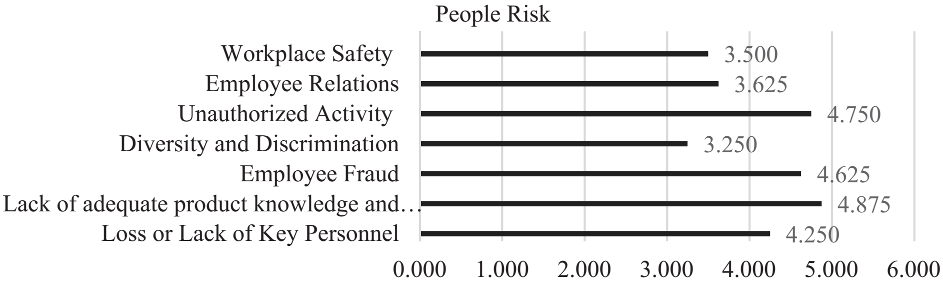


Table 8. External Events Risk

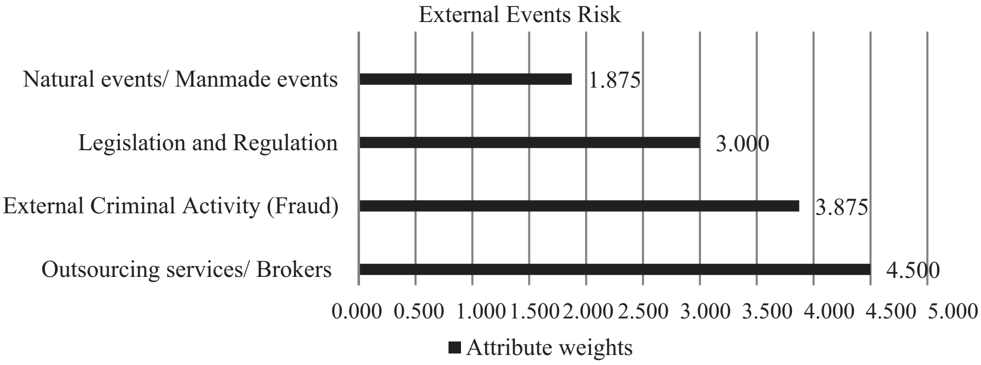
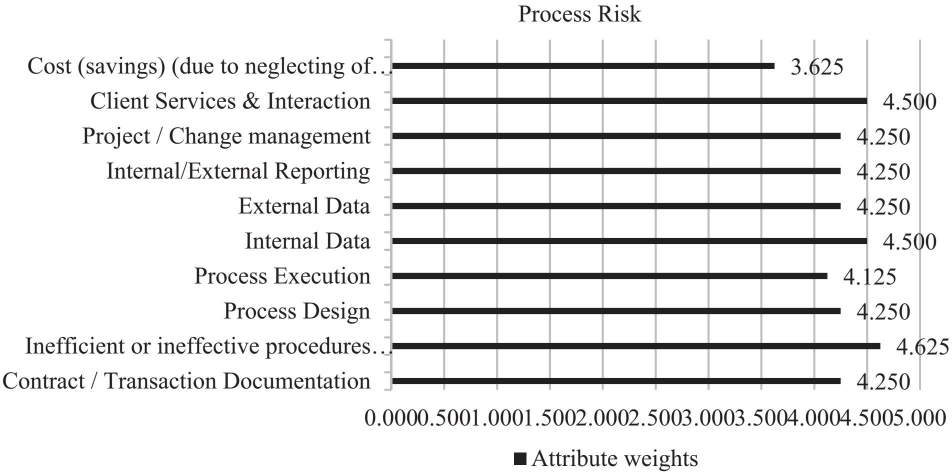


Table 9. Process Risk



From all the experts it was calculated that the riskiest factors were indicated by the expert number 3 (K3) and 1 (K1) as in the table below.

Below chart indicate from the highest to lowest bets alternatives (dark grey color indicates the highest risk, white the lowest of all (Table 10).

Table 10. Determine relative closeness to ideal solution

K1	K2	K3	K4	K5	K6	K7	K8
0.52	0.37	0.53	0.38	0.30	0.426	0.47	0.429

Conclusions

FinTech is quite recent development, there is still a vast amount of studies to be carried out on the social, regulatory, technological, and managerial aspects of FinTech. This makes it very challenging for financial firms to make informed decisions regarding the investment in FinTech projects. Most used term of FinTech – technology-based financial innovation that helps create new business models, business applications, processes, and products. These innovations have a significant impact on financial markets, institutions, and financial services.

FinTech sector has unique combination of exposures that are not contemplated by traditional financial institutions products. Although numerous researchers and practitioners have a believe that FinTech can reshape the longer term of the financial industry, the adoption of FinTech adoption is still unclear. Most adoption barriers are risk issues such as regulation (e.g., legal uncertainty for adoption), financial (e.g., loss of monetary outcome and extra fee), operational (e.g., inadequate processes or systems of FinTech companies), security and privacy (e.g., vulnerability of security technologies) concerns. Additionally, to these risks we should add all traditional (commonly used risk).

Financial crimes typically refer to any crime or misconduct including bribery & corruption; fraud or dishonesty; economic and trade sanctions; cybercrime; market abuse (insider trading, market rigging/ collusion); market abuse (insider trading, market rigging/ collusion); money laundering; handling the proceeds of crime; and conducting breaches. The importance of regulatory supervision regarding innovative services and merchandise was emphasized by the introduction of the 5th EU AML Directive where FinTech solutions where included under the scope. In current transactions and payments environment of developing security risk, regulation, customer expectation, approaches based on data science, Artificial Intelligence, machine learning, big data computing have possible new, real threats. All potential financial crimes can occur both in standard Financial Institutions or FinTech's as each of the sector companies trying to follow and enhance their systems and procedures to attract new and keep existing customers.

Most of the previous studies imply that FinTech industry is booming and more and more regulatory supervision to be given. As sector is not fully regulable it gives a big exposure to the customer who are utilizing their (FinTech) services and gives a big room for scammers to take advantage on the industry and their clientele. During recent 10 years regulators put more structural supervision on the sector which potentially can diminish some type of FinTech (for instance, crowdfunding).

According to collected data and given research companies should focus more on their Operations part and if they are efficient and "save" with their Systems, they might keep close attention to their defined processes and if their Employees receive appropriate understanding and training of given duties. As each companies' employees can have different perception on given processes it can be beneficial for them run an anonymous survey to collect an overview on how their employees are preserving risk that could lead to fraud and scam. At the beginning of the paper a question was raised: What risk financial crimes causes to FinTech companies? At this part of the research it was identified that more in-depth research needs to be done in order to give an answer to this question. More elements of the identified risk categories need to be distinguished. Also, an additional questions need to be raised that will give a more guidelines and structure for the research.

References

Beaumont, C. (1984). Review of *Thinking with Models*, by T. L. Saaty & J. M. Alexander. *The Journal of the Operational Research Society*, *35*(3), 270–270. https://doi.org/10.2307/2581759

Berger, A. N. (2003). The economic effects of technological progress: Evidence from the banking industry. *Journal of Money, Credit, and Banking*, *35*(2), 141–176. https://doi.org/10.1353/mcb.2003.0009

Buckley, R. P., Arner, D. W., Zetzsche, D. A., & Selga, E. (2019). The dark side of digital financial transformation: The new risks of FinTech and the rise of TechRisk. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3478640

Chen, B. C., Chen, J. G., & Alsmadi, M. (2013). Fuzzy AHP-based safety risk assessment methodology for tower crane. *Journal of Applied Sciences*, *13*(13), 2598–2601. https://doi.org/10.3923/jas.2013.2598.2601

Chenyakov, M., & Chernyakova, M. (2018). Technological risks of the digital economy. *Journal of Corporate Finance Research*, *12*(4), 99–109. https://doi.org/10.17323/j.jcfr.2073-0438.12.4.2018.99-109

Christoffersen, P. (2011). *Elements of financial risk management* (2nd ed.). https://www.google.com/books?hl=en&lr=&id=YkcMBGYbRasC&oi=fnd&pg=PP2&dq=Christoffersen,+Peter+F.+Elements+of+financial+risk+management.+Waltham,+MA:+Academic+Press,+2012&ots=IQQaRBALtu&sig=UlnCFcVKkxOMk9AUK46-uRKF1IA

Crouhy, M., Galai, D., & Mark, R. (2008). *The essentials of risk management*. https://www.kyoritsu-pub.co.jp/app/file/goods_contents/1225.pdf

Dyer, J. S. (1990). A clarification of "Remarks on the analytic hierarchy process". *Management Science*, *36*(3), 274–275. https://doi.org/10.1287/mnsc.36.3.274

Eriksonas, L. (2018). *Lithuania is becoming a second home for the international* FinTech *companies entering the EU market*.

European Banking Authority. (2020). *Results from the 2019 market risk benchmarking exercise*. EBA report. https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2020/EBA%20Report%20results%20from%20the%202019%20Market%20Risk%20Benchmarking%20Exercise.pdf

European Parliament and the Council of the European Union. (2015). *Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC* (Text with EEA relevance). *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32015L0849

Faraji Sabokbar, H., Ayashi, A., Hosseini, A., Banaitis, A., Banaitienė, N., & Ayashi, R. (2016). Risk assessment in tourism system using a fuzzy set and dominance-based rough set. *Technological and Economic Development of Economy*, *22*(4), 554–573. https://doi.org/10.3846/20294913.2016.1198840

Financial Inclusion Centre. (2018). FinTech – *beware of "geeks" bearing gifts?* https://inclusioncentre.co.uk/wp-content/uploads/2018/01/FinTech-Beware-of-geeks-bearing-gifts-FIC-Discussion-Paper-Summary.pdf

Financial Stability Board. (2019). FinTech *and market structure in financial services: Market developments and potential financial stability implications*. www.fsb.org/emailalert

Findexable. (2020). *The Global* FinTech *Index 2020*. Retrieved November 14, 2020, from https://lnkd.in/ep6p59S

Frame, W. S., Wall, L., & White, L. J. (2018). Technological change and financial innovation in banking: Some implications for FinTech. In A. Berger, P. Molyneux, & J. O. S. Wilson (Eds.), *Oxford handbook of banking* (3rd ed.). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198824633.013.10

Gegužienė, V., Kamienas, E., & Maciukevičienė, L. (2019). Vilniaus regiono smulkaus ir vidutinio verslo įmonių verslo procesų valdymo tobulinimas. Įžvalgos, 2, 12–25. Retrieved November 15, 2020, from www.lvpa.lt

Hwang, C.-L., & Yoon, K. (1981). Methods for multiple attribute decision making. In *Lecture Notes in Economics and Mathematical Systems: Vol. 186. Multiple attribute decision making* (pp. 58–191). Springer. https://doi.org/10.1007/978-3-642-48318-9_3

International Business Machines. (2020). FinTech *explosion and faster payments drive faster financial crime in 2020 – how can banks respond*? IBM RegTech Innovations Blog. https://www.ibm.com/blogs/regtech/FinTech-explosion-and-faster-payments-drive-faster-financial-crime-in-2020-how-can-banks-respond/

International Organization for Standartization. (2018). *Risk management – Guidelines* (ISO 31000:2018). https://www.iso.org/standard/65694.html

Invest in Lithuania. (2020). *The* FinTech *Landscape in Lithuania 2019–2020*. https://investlithuania.com/report/the-FinTech-landscape-in-lithuania-report-2019-2020/

Jorion, P. (2011). *Financial risk manager handbook: FRM Part I / Part II*. GARP (Global Association of Risk Professionals) – Google Books. https://books.google.lt/books?hl=en&lr=&id=4ceVmGJSNpcC&oi=fnd&pg=PT15&dq=Jorion,+Ph.+Financial+Risk+Manager+Handbook.+Wiley+Finance,+2009.&ots=ImgdiZG3ON&sig=2ObAdRD7OJRa0b_8mwc-EUspTJ8&redir_esc=y#v=onepage&q&f=false

Kokangül, A., Polat, U., & Dağsuyu, C. (2017). A new approximation for risk assessment using the AHP and Fine Kinney methodologies. *Safety Science*, *91*, 24–32. https://doi.org/10.1016/j.ssci.2016.07.015

KPMG Global. (2019). *Pulse of* FinTech *H2'19 – Global trends*. Retrieved September 17, 2020, from https://home.kpmg/xx/en/home/campaigns/2020/02/pulse-of-FinTech-h2-19-global-trends.html

Leong, K., & Sung, A. (2018). FinTech (financial technology): What is it and how to use technologies to create business value in FinTech way? *International Journal of Innovation, Management and Technology*, *9*(2), 74–78. https://doi.org/10.18178/ijimt.2018.9.2.791

Lietuvos bankas. (n.d.). *El. pinigų įstaigos*. Retrieved September 18, 2020, from https://www.lb.lt/lt/el-pinigu-istaigos

Lietuvos Respublikos generalinė prokuratūra. (2013). Lietuvos Respublikos Generalinio Prokuroro Įsakymas „Dėl Rekomendacijų dėl nusikalstamu būdu įgytų pinigų ar turto legalizavimo ikiteisminio tyrimo patvirtinimo". *Valstybės* žinios, Sausio 15, 2013, No. 5-209. https://www.e-tar.lt/portal/en/legalAct/TAR.573F6506D8A8

Liu, J., Li, X., & Wang, S. (2020). What have we learnt from 10 years of FinTech research? A scientometric analysis. *Technological Forecasting and Social Change*, *155*, 120022. https://doi.org/10.1016/j.techfore.2020.120022

Micu, A., & Micu, I. (2016). Financial technology (FinTech) and its implementation on the Romanian non-banking capital market. *SEA – Practical Application of Science*, *IV*, 2(11), 379–384.

Ministry of Finance of the Republic of Lithuania. (n.d.). FinTech *market leaders from around the world gather in Vilnius*. Retrieved September 13, 2020, from https://finmin.lrv.lt/en/news/FinTech-market-leaders-from-around-the-world-gather-in-vilnius

Muhtaseb, M. R. (2020). Fraud against hedge funds: Implications to operational risk and due diligence. *Journal of Financial Crime*, *27*(1), 67–77. https://doi.org/10.1108/JFC-03-2019-0032

Padma, T., & Balasubramanie, P. (2007). Analytic hierarchy process to assess occupational risk for shoulder and neck pain. *Applied Mathematics and Computation*, *193*(2), 321–324. https://doi.org/10.1016/j.amc.2007.03.060

Saaty, T. L. (1977). A scaling method for priorities in hierarchical structures. *Journal of Mathematical Psychology*, *15*(3), 234–281. https://doi.org/10.1016/0022-2496(77)90033-5

Saaty, T. L. (1990). How to make a decision: The analytic hierarchy process. *European Journal of Operational Research*, *48*(1), 9–26. https://doi.org/10.1016/0377-2217(90)90057-I

Saaty, T. L. (2003). Decision-making with the AHP: Why is the principal eigenvector necessary. *European Journal of Operational Research*, *145*(1), 85–91. https://doi.org/10.1016/S0377-2217(02)00227-8

Thakor, A. V. (1999). Information technology and financial services consolidation. *Journal of Banking and Finance*, *23*(2), 697–700. https://doi.org/10.1016/S0378-4266(98)00104-6

Thakor, A. V. (2020). FinTech and banking: What do we know? *Journal of Financial Intermediation*, *41*, 100833. https://doi.org/10.1016/j.jfi.2019.100833

Varga, D. (2017). FinTech, the new era of financial services. *Vezetéstudomány / Budapest Management Review*, *48*(11), 22–32. https://doi.org/10.14267/VEZTUD.2017.11.03

Vargas, L. G. (1990). An overview of the analytic hierarchy process and its applications. *European Journal of Operational Research*, *48*(1), 2–8. https://doi.org/10.1016/0377-2217(90)90056-H

Yulong, L., Xiande, W., & Zhongfu, L. (2008). Safety risk assessment on communication system based on satellite constellations with the analytic hierarchy process. *Aircraft Engineering and Aerospace Technology*, *80*(6), 595–604. https://doi.org/10.1108/00022660810911536

Zavadskas, E. K., Turskis, Z., & Tamošaitiene, J. (2010). Risk assessment of construction projects. *Journal of Civil Engineering and Management*, *16*(1), 33–46. https://doi.org/10.3846/jcem.2010.03

Zhu, T., & Chen, L. (2016). *The potential risks and regulatory responses of* FinTech. http://en.cnki.com.cn/Article_en/CJFDTotal-JRJG201607002.htm

Zwikael, O. (2009). The relative importance of the PMBOK ® Guide's nine knowledge areas during project planning. *Project Management Journal*, *40*(4), 94–103. https://doi.org/10.1002/pmj.20116

RIZIKOS VERTINIMAS, SUSIJĘS SU FINANSINIAIS NUSIKALTIMAIS FINTECH

Jelena STANKEVIČIENĖ, Agata TOMAŠEVIČIŪTĖ

Santrauka. Darbo tikslas – ištirti rizikas, susijusias su finansiniais nusikaltimais finansinių technologijų įmonėse, taip pat konsoliduoti būsimų tyrimų darbotvarkę. Taikytini metodai: susijusios mokslinės literatūros turinio analizė, rizikos vertinimo ir valdymo standartų analizė ir jos santrauka. Straipsnyje pateikiamas *FinTech* apibrėžimas, nagrinėjama kai kurie augimo statistiniai duomenys ir apžvelgiama teorinė literatūra. Rizikos analizė yra labai svarbus veiksnys sėkmingam projekto kūrimui ar sėkmingų įmonių egzistavimui, nes *FinTech* įmonės pirmiausia siekia teikti greitas (efektyvias) paslaugas ir pamiršta atsargumo priemones, skirtas savo verslui ir galutiniam vartotojui apsaugoti. Šiame darbe buvo siekiama įvertinti literatūrą ir mokslinius tyrimus, susijusius su *FinTech* ir su jais susiduriama rizika, ir pradėti nuo pirmųjų būsimų darbų tyrimo žingsnių. Šio dokumento naujovė yra susijusi su atotrūkiu, kai jauni *FinTech* atstovai, *per se* startuoliai, nėra visiškai pasirengę reguliavimo / kibernetinio saugumo iššūkiams. Šiuo metu susijęs duomenų rinkimas yra ribojamas, taip pat yra nustatytas ribotas imties dydis, kyla pavojus, kad ekspertai neatsakys. Viešai neprieinama informacija. Pagrindinis darbe keliamas klausimas – kuri galimos rizikos sritis gali sukelti didesnę finansinių nusikaltimų tarp *FinTech* įmonių tikimybę. Tyrimui taikytini metodai yra analitinės hierarchijos procesas (AHP) ir pirmenybės pagal panašumą į idealų sprendimą metodas TOPSIS.

Reikšminiai žodžiai: rizikos vertinimas, rizikos valdymas, *FinTech*, finansiniai nusikaltimai, pinigų plovimo prevencijos direktyva, AHP.