DOI: 10.17747/2618-947X-2020-2-150-159

Definition and measurement of risk in compliance management

A.M. Krepysheva[1]
A.A. Sergievskaya[2]
M.A. Storchevoy[1]
[1] NRU HSE (Saint Petersburg)
[2] "Unilever Rus" LLC

ABSTRACT

The article is devoted to the problem of defining and measuring risk in compliance management - an important management function of a company aimed at complying with laws and ethical norms. A general definition of risk from the theory of probability and various approaches to understanding risk in the literature on risk management are considered, then the definition of compliance risk and ways to managing this risk in compliance management are explored. The problem of quantitative measurement of compliance risks and some methods of its solution are described. The authors analyze the approaches of several international companies (in the mining industry, oil and gas industry, mobile communications, FMCG) to measuring or assessing compliance risks, as well as organizing compliance risk management in practice (organizational structures, processes, etc.). The work also discussed the concept of risk appetite, that characterizes the willingness of an organization to take on a certain positive level of risk, while logically it is poorly compatible with the concept of compliance risk as a risk of violation of the legislation.

KEYWORDS:

compliance, ethics, compliance risk, compliance management, quantitative risk measurement, risk appetite.

FOR CITATION:

Krepysheva A.M., Sergievskaya A.A., Storchevoy M.A. (2020). Definition and measurement of risk in compliance management. *Strategic Decisions and Risk Management,* 11(2), 150-159. DOI: 10.17747/2618-947X-2020-2-150-159.

The authors would like to thank experts who helped in collecting material for the empirical part of the work: Petr Androsenko and Tatiana Pavlenko (VimpelCom), Irina Grekova (Moscow Exchange), Margarita Khomenko (Compliance Elements).

1. INTRODUCTION

In this work, we will try to understand how risk is defined and measured in compliance management, an important management function of the company aimed at complying with laws and ethics. First, we will talk about a general definition of risk, then consider different approaches to understanding risk in compliance management, and at the end we will discuss the approaches of several companies to measure or evaluate compliance risks. In the modern Russian theme, this problem is not sufficiently considered. For example, [Bulyga, Kupriyanova, 2015] deals with the organization of compliance function in general, but risk assessment as such is not discussed. The paper [Komarov, 2020] presents indicators on the basis of which risk assessment takes place and considers categories of risks, but the author does not describe methodology for assessing these indicators and does not cite the scales by which they are measured. In other publications dealing with compliance risks, such as in [Sokolov, 2018], the measurement issue is also not discussed.

2. CONCEPT OF RISK IN MODERN LITERATURE

Concept of risk is, on the one hand, very popular in various scientific and managerial disciplines, and on the other, defined and understood very differently in these disciplines.

There are two strictly defined concepts in probability theory: *probability* and *mathematical expectation* . *Probability* is a quantitative measure of the onset of result *X*, кwhich is one of several alternative outcomes of some action. The probability is measured as *n/N*, where *n* shows how many times the result *X*, occurred, and N is how many times the total this action has been carried out. Accordingly, the probability varies from 0 (absolutely impossible result) to 1 (the result to be obtained anyway). For example, a probability of 0.2 means that, on average, this result is observed in 20% of all cases of the action. *Mathematical expectation* is the multiplication of quantitative measurement of a result (when it has a quantitative dimension) by its probability. For example, if the result is a profit of $100, and the probability of getting that result is 0.5, then multiplying these numbers gives a mathematical expectation of $20: this means that on average we receive 20 dollars of winnings from each implementation of this action. Thus, probability and mathematical expectation are strictly defined mathematical concepts that are used in various scientific disciplines (e.g., insurance, financial management, real option theories, etc.).

As for the term “risk”, probability theory does not use it as a well-defined mathematical concept at all. The word “risk” is used in texts on probability theory or social sciences (such as economics) in an informal way to emphasize the stochastic nature of an event. For example, in the economic and management literature, the problem of choosing between options with random results is called “decisions in a risk environment”, but no quantitative measurement of risk is given in these theories.

In everyday usage, the word “risk” has a narrower definition and refers only to negative results and their probabilities. The commonly used meaning of risk is “the probability of something bad” (for example, the Oxford Dictionary of English defines risk as “the probability of danger, loss, injury, or other adverse effects"). The same situation with the all-language meaning in Russian (for example, Ochegov's Dictionary defines it as "probability of failure, danger").

How do you understand risk in the literature on risk management? Here, the notion of risk does not only come down to negative events and includes any events - both positive and negative. However, there is no universal definition of risk here. Consider a few reputable sources as an example.

For example, in a monograph on risk management, Paul Hopkin [Hopkin, 2018] examines different definitions of risk and concludes that there is no universal definition and every organization should adopt the definition according to their needs. In the context of an organization, risk is usually understood to be something that can affect the achievement of corporate goals. Hopkin himself proposed the following definition: "An event capable of affecting (suppressing, amplifying, or arousing doubt) effectiveness of the organization's core processes."

An authoritative source can be ISO standards, which formulate universal and optimal ways to solve any technical or managerial tasks. There is a separate ISO 31000 standard called Risk Management[1]. A new version of this standard from 2018 defines risk as "the impact of uncertainty on targets." The impact means that the result is different from what is expected. This impact can be "positive, negative, or both and can concern, create or lead to opportunities and threats." Obviously, standards don't limit the scope of risk to just negative events. In addition, the concept of risk exposure is highlighted, which essentially corresponds to the mathematical expectation in the theory of probability — the product of probability of an event by possible losses with which this event is accompanied.

A slightly different definition of risk is given by the Institute of Internal Auditors, the world's leading organization for standards development and professional development of internal auditors. According to it, the risk is "the uncertainty of an event that can have an impact on the achievement of goals. Risk is measured in terms of consequences and probability."

As can be seen in this brief overview, leading organizations in risk management talk about the same thing, although they define risk somewhat differently – "event", "event uncertainty", "influence of uncertainty", etc. One of the authors [Ramakrishna, 2015] highlighted five typical ways of determining risk: 1) an unwanted event that may occur, 2) the cause of an unwanted event that may occur, 3) probability of an unwanted event that can occur, 4) mathematical expectation of an undesired event, 5) indication of the fact that the decision is made in a situation of quantified probabilities, not in a situation of uncertainty on Knight.

Experts in the field of operational risk management [A new approach.., 2010] note that the understanding of risk is gradually evolving and the modern approach to risk management is significantly different from traditional. Traditional risk management theory defines risk as "the probability that an event will occur and adversely affect the achievement of an organization's mission or business goals." This risk can be calculated as multiplying the probability by the value of the loss.

A modern approach in risk management defines risk otherwise as "a measure of exposure to losses at the level of uncertainty". Differences between the two concepts are presented in Figure 1. It can be seen that the highest risk in the traditional approach occurs when the probability of loss is 100%. In modern interpretation, maximum risk exists where probability (or frequency) is low and severity is high.

3. CONCEPT OF RISK IN COMPLIANCE MANAGEMENT

Definitions of compliance risk in literature also differ somewhat among each other. To some extent, these differences depend on the specific understanding of regulators or researchers who seek to define it. The common denominator of all definitions is that compliance risk appears in the field of regulation, but there are different concepts of its measurement.

Concept of compliance risk has emerged in literature over the past decade (e.g., in a collective monograph [Molak, 1997] on various areas of risk management, the problem of compliance risk not mentioned at all). However, in [Hopkin, 2018] compliance risk is listed first in the classification of four risk types and defined as a "liability management risk category". To minimize compliance risks, organizations need to be aware of compliance requirements they need to meet. There may also be a regulatory body - in the industry or sector that monitors compliance; in the event that organization has failed to meet them, regulator has the power to demand termination of its activities. Many industries are now highly regulated: medicine, insurance, finance, transportation, etc. In addition to regulators, companies must also comply with requirements imposed on them by various laws. In addition to compliance risk, Hopkin also highlights the *opportunity risk* associated with the possibility of obtaining any benefit, control, *risk* the possibility of deviating project execution from the specified framework, and the *net risk* associated with such events that can only bring losses and never give nothing useful (like fire or fraud).

Consulting company Deloitte defines compliance risk as "a threat to financial, organizational or reputational status of an organization arising from violations of laws, regulations acts, codes of conduct or organizational standards of practice" [2].

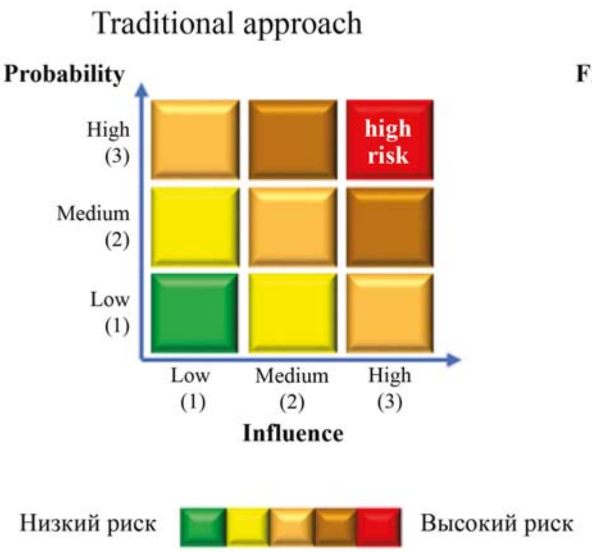
ISO 19600 International Standard "Compliance Management Systems"[3] follows the wording of ISO

[1] ISO 31000:2018 – Risk management — Guidelines. URL: https://www.iso.org/standard/65694.html.

[2] Compliance risk assessments. The third ingredient in a world-class ethics and compliance program. 2015. URL: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-compliance-risk-assessments.pdf

[3] ISO 19600:2014 – Compliance management systems. In official Russian translation «Системы управления соответствием» ("Compliance Management Systems"). URL: https://www.iso.org/ru/standard/62342.html.

Figure 1. Traditional and modern approach to risk



Source: [A new approach.., 2010].

31000, which defines risk as the “impact of uncertainty on objectives” (uncertainty on objectives), with the impact being both positive and negative. Accordingly, compliance risk is defined as the “impact of uncertainty on compliance objectives”. Further, another definition of compliance risk is given: it can be described as likelihood of failure to conform to compliance obligations of organization and their consequences. Probability is denoted by the word likelihood to contrast its mathematical probability, which has an exact quantitative dimension. Accordingly, compliance obligations are defined as the need to comply with requirements (compliance requirements or compliance commitments), which in turn are defined by rather broadly as “demands or expectations of certain behavior from an organization”. Note that ISO standard does not specify that these violations are primarily or only violations of the law. It is also a violation of ethical obligations, as well as any other voluntarily assumed by the company (such as industry standards, best business practices, etc.). Standard has section 4.6 “Identification, Analysis and Evaluation of Compliance Risks”, but it does not provide any indication of how to measure a given risk.

Several types of compliance risk are identified in [Ramakrishna, 2015]: 1) the risk of unethical behavior (integrity risk), 2) business risk, 3) reputation risk, 4) regulatory risk, 5) risk of unspecified legal requirements (interpretational risk), 6) legal risk, 7) litigation risk, 8) risk of financial loss. This classification seems to us rather loosely structured, as separate parts of it intersect among themselves. For example, harrasment in a company can be attributed to risk of unethical conduct, legal risk, risk of prosecution, risk of financial loss, and reputational risk.

4. PROBLEM OF QUANTIFYING COMPLIANCE RISK

Various tools are used to manage compliance risk to facilitate detection, measurement and streamlining. In this work, we are interested primarily in the problem of quantitative measurement of risk. As you know, qualitative control of the object or process is impossible without measurement, so this problem is of paramount importance.

In the literature on compliance there is often a traditional matrix for risk management, which has already been given in Figure 1, in the traditional form, with the filling of all cells. However, no practical methodology or guidance provides a single rigorous way of assessing these risks. It is often suggested to use expert method, survey method, etc., but the problem of choosing the best method and its detailed setting remains in abeyance . Many authors, for example [Nicolas, May, 2017] do not attach serious importance to the development of a methodology for assigning risks to a specific level, but rather focus on the fact that the system for compliance risk assessment should be comprehensively thoughtful and constantly operational.

The Institute for Strategic Risk Analysis of Management Solutions (ISAR) recommends, in its training materials, the following criteria for risk assessment by magnitude and probability (see Table 1, 2).

As can be seen, the general logic of these estimates is similar to those already described, but there are also a number of undefined places, such as “average income decline” or grounds for inferring that the risk ”is implemented within a year.”

Interviews with compliance managers of Russian companies show that they assign characteristics “low”, “medium” or “high” very arbitrarily. For example, according

Table 1
Risk value in ISAR method

Level		Damage
High	3	Implementing one or more risks in this category can result in a significant decrease in revenue or increase company's costs or reputational damage to the company
Medium	2	Implementing one or more risks in this category can lead to an average decrease in revenue or increase the company's expenses and insignificant reputational damage
Low	1	Implementation of risks in this category can lead to an insignificant decrease in revenue or increase the company's expenses

to the compliance manager of a global grocery company, any corruption risk they automatically have refers to high risks. Compliance manager of mobile operator noticed that a high risk is considered, which leads to a serious fine (for example, a fine of 1 million rubles for bribing an official when obtaining a permit to construction). Obviously, there is no common methodology for understanding Russian companies of what is a risk and how to consider it. Meanwhile, without a clear technique, these characteristics can be meaningless. As internal audit specialist Linford Graham writes: "I am not a fan of high-medium-low terms for risk assessment. In my experience, if these terms are not defined first well using visual scenarios, detailed examples, or even clear quantification of probability (e.g. probability less than 20%), even those managers who have similar perceptions of risk would find it difficult to develop a common opinion. <...> I would suggest estimating the risk in percentages or in interest ranges that are much less ambiguous when discussed, even if they are subjective estimates rather than the result of accurate calculations" [Graham, 2015. P. 69].

Of course, in the case of compliance risks, each company faces many unknowns, and it's quite difficult to quantify probability. This problem is especially true for young and small companies that do not have their own statistics. However, for large companies numbering tens of thousands of workers and working many years, there are *internal violations statistics* that can be used to calculate both minimum probability of violations. The size of the negative impacts changes from year to year in line with regulatory changes, but these figures are also available to companies that monitor the changes. For small companies, general statistics can be used for a given sector of the economy or the economy as a whole. For example, according to the available statistics, one corruption violation per 4 thousand employed is recorded per year. Consequently, if the company employs 2 thousand employees, it can be expected that the corruption violation will occur with a probability of 50% within a year (or, the same, will necessarily happen times in two years).

An attempt to develop a quantitative assessment of the risks of theft was jointly undertaken by the Russian branches of the Association of Certified Fraud Examiners and Ernst & Young in 2013 [Martynov, Novikov, 2013]. The researchers surveyed more than 500 professionals working in investigations, internal audit, risk management and other business security areas and asked to evaluate the importance of each of the thirty theft indicators, which included the characteristics of the company's management system (for example, the existence of a program to counter theft), the economic situation in companies (staff dissatisfaction with salary levels), external environment (e.g. instability and crisis events), control results (e.g. lack of primary supporting documents), etc. Based on the survey, the weight of importance for each indicator on an ordinary scale from 1 to 5, where 1 means that the indicator is loosely associated with the risk of theft, and 5 - that the indicator is quite certain (very often) is accompanied by embezzlement. The

Table 2
Risk probability in ISAR method

Level		Probability of occurrence
High	3	Risk has already been realized many times in the past, there is a high degree of uncertainty about the likelihood of realizing the risk or internal or external prerequisites that indicate that the risk is rather total, is implemented over the next year
Medium	2	Risk is likely to be realized within a year
Low	1	Low probability that risk will be realized within a year

Table 3
Risk gradation of financial losses (mining company)

Risk	Financial losses (thousands of dollars)	Impact on the company	Impact on company's EBITDA (%)
Insignificant	Less than 20	Minor operations, strategy, security, image problems	Less tha 1
Insignificant	20–100	Some operations, strategy, security, image problems	1–5
Moderate	100–200	Serious operations, strategy, security, image problems	5–10
Large	200–1000	Important operations, strategic, security, image problems	10–50
Critical	More than 1000	Critical operations, strategy, security, image problems	More than 50

indicator "loss or destruction of documents and electronic files containing key information about dubious operations" received the highest weight, and the lowest, oddly enough, "level of corporate culture." The authors indicate that in order to calculate the overall risk index of theft, it is necessary to combine all observed parameters with their weights into a single formula, which should use the logarithm of the number of indicators found and the sum of the weights of all the risk indicators found, but the exact justification of this formula requires additional research.

5. EXAMPLES OF APPROACHES OF SPECIFIC COMPANIES TO RISK ASSESSMENT

Consider the approaches of different companies to assess compliance risks. Names of some of the companies discussed in this section are omitted at the request of our respondents.

An international company in the extractive industry defines two risk categories. Risks of the first category have a strong impact on the company, and at worst they result in value-added tax, loss of reputation, loss of business, etc. In addition, the company could be fined more than $1 million. Compliance managers should immediately report such risks and include relevant information in the monthly report. The second risk category has a moderate impact on the company. The fine can amount to between $10,000 and $1 million. Compliance managers report such risks in the form of monthly reports. To complete a compliance risk report or report it immediately, the compliance manager uses a risk notification form aimed at data collection, monitoring and risk control. Report requires the following information:

- compliance risk area,
- date of the event that caused the risk
- enterprise,
- description of a risk event,
- presumptive cause of this event,
- possibility of a recurrence of risk
- possible consequences.

Head office accumulates risk reporting, describing risk factors, probability of their realization and possible impact on the company; also, risks are assigned an assessment (low, medium, or high) and specifies the applicable and planned procedures to mitigate the impact of the realization of risk.

The company has developed scales to evaluate individual indicators, such as the *impact* of *risk* and *probability*, on the basis of which the risk is assigned final score. The impact of risks is measured by financial losses, the impact on the

Table 4. Risk gradation by probability of occurrence (mining company)

Risk	Probability (%)	Frequency of occurrence
Almost impossible	Less than 5	In exceptional cases
Hardly probable	5–20	Approximately once every five years
Moderately expectable	20–50	Approximately every two years
More expectable	50–90	Approximately once a year
Almost inevitable	More than 90	Approximately once a month

Table 5. Risk card (mining company)

PROBABILITY	medium	significant	significant	high	high
	medium	medium	significant	high	high
	low	medium	medium	significant	high
	low	low	medium	medium	significant
	low	low	low	medium	medium
INFLUENCE					

company's EBITDA (thousands of dollars) and has the following scale (see Table 3).

Risk probability scale is presented in Table 4.

After reviewing two indicators, the compliance manager assigns a risk score according to the risk map (see Table 5). Horizontal axis (*X*) reflects the impact of risk on a scale from non-essential to critical, ordinate axis (*U*) reflects the scale of probability from almost impossible risk to almost inevitable.

The international company in the oil and gas industry reported the following approach to risk assessment. Four probability categories are used (see Table 6). Risk matrix of this company is presented in table 7).

However, the company did not provide guidance on the implementation of the assessment, and therefore the principles of probability assignment as well as loss estimation remain unclear.

The experience of one of the authors of this article on the position of compliance manager in different companies shows that they use very similar tools to the assessment of compliance risks. Matrices and schemes to determine the impact of risk, given above, are literally borrowed by companies from each other or from textbooks.

At the same time, companies that are just beginning to implement compliance, at first risk assessments do not do at all. Often the following scenario is observed: first the firm introduces a standard set of compliance systems: developing a code of ethics, policies and procedures for interaction with third parties, trainings, hot line, internal investigation procedure. These standard paragraphs can be found in legislative requirements or methodological recommendations thereto. And when in the campaign appoint employees responsible for implementation of compliance function, then soon they have a number of questions, the main of which is: "Why do we need it?" And the answer is that the set of documents and procedures itself is ineffective. It is necessary to conduct a risk assessment to understand how the identified risks are relevant in a particular organization and how the measures taken really minimize them, and to determine how much the process is risk management.

Evaluation (revaluation) should be carried out on a regular basis with the frequency most similar to the particular company and its business model. This need is related, among other factors, to the matrix structure of some global companies, which involves frequent rotation of staff, changes of functionality and areas of responsibility. These changes in the interactions of people can constantly make their adjustments to the building of the work of compliance functions. For example, employees who have never interacted with government bodies before begin to do so, and here you need to pay special attention to their work, to make sure their understanding of the process. This work with staff helps to identify system shortcomings or, conversely, to gain confidence in the absence of critical gaps.

Many international manuals write about risk assessment from the perspective of the business process, but it would be more reasonable to place this function on the business unit area. It is common knowledge that sales, procurement, participation in tenders, marketing, etc., are high-risk areas, and this information does not represent value for management. The most important for both the company and the risk owners themselves[4] is to understand which specific

Table 6. Risk gradation by probability (oil and gas company)

Possible scenarios	Probability factor
Probability of implementation of compliance risk is low	1
Probabilities of implementation and failure to implement compliance risk are roughly equal	2
Compliance risk is more likely to be realized	3
Compliance risk is surely realized	4

[4] The risk owner is a manager whose operational or strategic objectives are exposed to this risk. Typically, it is the head of a business unit. For example, the risk of situations such as a pandemic has an impact on sales, and the owner of the risk in this case will be the head of sales.

Table 7. Risk gradation by the magnitude of losses (oil and gas company)

Estimation of materiality of possible losses of the company or enterprise (RUB million)	Коэффициент вероятности наступления комплаенс-риска		
	1	2–3	4
Over 500	Medium	High	High
50-500	Low	Medium	High
Up to 50	Low	Low	Medium

people (in what positions) are in the compliance risk zone. This information is easier to work with at the business unit level.

A compliance manager should not assess compliance risks alone. This should be the responsibility of either risk owners (e.g. through record keeping) or a compliance manager based on the views of staff. For example, Unilever's “Code of Business Principles” has the following clause: “Liability: They are obliged to identify risks and to manage risks that relate to their duties ”[5].

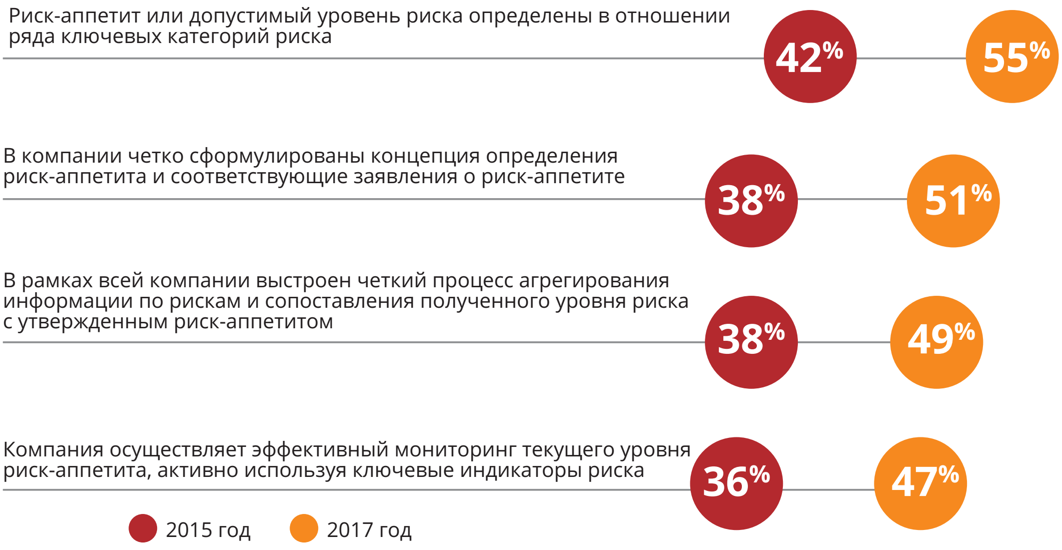
Compliance-risk management is sometimes carried out independently by a compliance unit, and sometimes can be transferred to the company's general risk management system (ERM) as it is done in many companies (like VEON). But at the same time, the compliance officer must either be actively involved (lead the process) or have a full understanding of how that assessment was made. It is important to understand the compliance risks of the company and its employees, and then to build interactions in the system.

The methodology of the compliance system should always include a description of the system itself and the processes within it, as well as information on the activities undertaken, including their objectives, results, provided procedures in case of compliance risk implementation with the indication of the responsible person. Therefore, companies create risk committees, compliance committees, ethics committees, etc.

6. COMPLIANCE RISKS AND RISK-APPETITE

We need to raise the logical question of how should companies use quantitative assessments of compliance risks? Many researchers point out that different types of risk should be managed differently. Some authors, for example [Hopkin, 2018], argue that compliance risk should be minimized because in nature is close to net risk, while financial risks are usually risks opportunities and are balanced by returns, so it is not necessary to minimize them. However, the original concept of risk appetite is often found in consultant materials or in financial management literature, which means that company is willing to go to a certain level of risk. Deloitte refers to the definition of the Basel Committee

Figure 2. Improving approaches to risk appetite determination



Source: [Risk View.., 2017].

[5] URL: https://www.unilever.ru/Images/code-and-code-policies-2017-rus_tcm1315-508300_ru.pdf.

on Banking Supervision: "Risk appetite is pre-determined levels and types of risks within the permissible level of risks that the bank is ready to adopt to achieve its goals based on the scope and nature of its activities within the strategy and business plan" [6]. However, in the previous version of the Basel requirements, the concept of risk appetite was not mentioned at all [Gontarek, 2016]. PWC [Risk View.., 2017] study found that companies are gradually expanding their use of the concept. Figure 2 presents data for 2015 and 2017 (in orange) years. The results of the study showed that the number of companies determining their risk appetite increased by 13%, as did the number of companies in which the concept was formulated and made relevant statements about risk-appetite.

However, with respect to compliance, the concept of risk-appetite is somewhat controversial, as it suggests that the organization does not attempt to completely eradicate any violation of the law (as this is implied for law-abiding citizens), but allows a conscious violation of it under certain conditions. Indeed, sometimes taking a risk and, as a result, for example, paying a fine for a company will result in the possibility of receiving a greater benefit.

Note that a conscious decision to assume a positive compliance risk may not be caused by a self-interested desire to earn a profit, but rather by a responsible decision related to preventing any more serious adverse effects on the company's steakholders. In our practice, there was a case where an employee was dismissed because he appeared at work with serious hungover syndrome. Dissenting from dismissal and seeking to retain the job at all costs, the staff member went to medical examination where alcohol was confirmed in his blood and, as a result, the unsubstantiation of his dismissal. Such a legal move was predictable, and the compliance manager of the company guessed about the actions that the employee intended to take, as well as that the results of the examination to be carried out after an hour, may be negative. However, if the employee was allowed to work that day, there could be irreparable consequences: injury at work, failure of equipment. Thus, the compliance manager knowingly went to accept compliance risk and this risk was realized in the form of litigation initiated by the fired employee. Is it correct to attribute this action to risk appetite?

Another ethical dilemma from this category may be the situation in which a person is lost in the forest and relatives or search team ask the mobile operator to report geolocation data from his mobile phone. However, a mobile operator cannot do so under the law, and a breach could carry the risk of a huge fine by the regulator. In most cases, mobile operators do not have enough risk-appetite in this situation to violate personal data law, but many people are killed as a result. Is it correct to consider this action in terms of risk-appetite?

Ideologically, many companies proclaim a different policy zero tolerance to any compliance violations, and above all corruption. For example, VEON group's code of ethics establishes "complete intolerance of bribery and corruption" [7]. Compliance manager of this company reported that in general they adhere to zero tolerance in relation to all compliance risks, but for other risks there are established levels of risk-appetite. Yandex claims to "profess the principle of zero tolerance for any breach of corporate ethics rules[8]". Auchan also follows this policy[9]. Perhaps this position is caused by the fact that if companies openly declare a non-zero appetite for risk, it will be perceived sharply negatively and by regulators, for which it is ideologically important to seek respect for the law and regulations, and investors. However, in reality it is impossible to achieve zero compliance risk, so such statements appear somewhat contradictory. Some companies withdraw from this provision by claiming zero tolerance for failure to report violations. EuroKhim, for example, says "zero tolerance for non – compliance obligations" [10] – it is implicitly acknowledged that the violations themselves cannot be completely eliminated.

CONCLUSIONS

As the present study suggests, the concept of risk is key to compliance management, but it is not strictly understood by different sources. Among the practical tasks, the most relevant is the development of a methodology for measuring compliance risk. At present, all approaches to measurement are very approximate and subjective, providing opportunities for further research in the field.

An important conceptual problem is the level of acceptable compliance risk (risk appetite), which is not fully understood in practice and requires deeper study.

REFERENCES

1. Bulyga R.P., Kupriyanova L.M. (2015). Otsenka komplayens-riskov [Assessment of compliance risks]. *Ekonomika. Biznes. Banki [Economics. Business. Banks]*, 3, 16-32.
2. *Vzglyad na riski. Upravleniye riskami «na peredovoy» [Risk in review. Managing risk from the front line]* (2017). PWC. URL: https://www.pwc.com/ee/et/publications/pub/pwc-2017-risk-in-review-study.pdf.
3. Komarova E.O. (2020). *Otsenka i raschet komplaens-riska. Materialy II mezhdunarodnoy nauchno-prakticheskoy konferentsii "Tendentsii i perspektivy razvitiya bankovskoy sistemy v sovremennykh ekonomicheskikh usloviyakh", 17-18 dekabrya 2019*

[6] Risk-appetite strategy: best practices (2020). Deloitte. Online Webinar. URL: https://www2.deloitte.com/content/dam/Deloitte/kz/Documents/risk/Вебинар_стратегия%20риск-аппетита_9%20июня.pdf.

[7] VEON Group Code of Conduct (2019). URL: http://static.beeline.ru/upload/contents/297/Kodeks_povedenija_veon.PDF.

[8] Yandex updated the rules of corporate ethics for employees and external partners of the company (2020) // Yandex.ru. March, 10. URL: https://yandex.ru/company/press_releases/2020/2020-03-10.

[9] Auchan Retail Code of Business Ethics. URL: https://auchan-supply.ru/ethics-hotline/kodeks-delovoy-etiki/.

[10] EuroKhim – VolgaKalii (2018). Policy on ensuring compliance with regulatory requirements (compliance). URL: https://www.eurochemgroup.com/ru/legal-and-compliance/.

[Assessment and calculation of compliance risk. Materials of the II International Scientific and Practical Conference "Trends and Prospects for the Development of the Banking System in Modern Economic Conditions", December 17-18, 2019]. Bryansk, Bryansk State University named after I.G. Petrovsky.

4. Martynov S., Novikov A. (2013). *Otsenka riskov khishcheniy kak aktual'noye napravleniye v bezopasnosti biznesa [Assessment of theft risks as an important area in business security]*. Moco, ACFE.
5. Sokolova E.Yu. (2018). Printsipy upravleniya komplayens-riskom v kreditnykh organizatsiyakh [Principles of compliance risk management in credit institutions. *Alleya nauki [Alley of Science]*, 9(25).
6. Gontarek W. (2016). Risk governance of financial institutions: The growing importance of risk appetite and culture *Journal of Risk Management in Financial Institutions*, 9(2), 120-129.
7. Graham L. (2015). *Internal control audit and compliance: documentation and testing under the new COSO framework*. New Jersey, John Wiley & Sons.
8. Hopkin P. (2018). *Fundamentals of risk management: understanding, evaluating and implementing effective risk management*. New York, Kogan Page Publishers.
9. Kim A.C., Lee S.M., Lee D.H. (2012). Compliance risk assessment measures of financial information security using system dynamics. *International Journal of Security and Its Applications*, 6(4), 191-200.
10. Liebergen B. van (2017). Machine learning: A revolution in risk management and compliance? *Journal of Financial Transformation*, 45, 65-72.
11. Moeller R.R. (2011). *COSO enterprise risk management: establishing effective governance, risk, and compliance processes*. Vol. 560. New Jersey, John Wiley & Sons.
12. Molak V. (1997). *Fundamentals of risk analysis and risk management*. Boca Raton, FL, USA, Lewis Publishers, 233-245.
13. Nicolas S., May P.V. (2017). Building an effective compliance risk assessment programme for a financial institution. *Journal of Securities Operations & Custody*, 9(3), 215-224.
14. *A new approach for managing operational risk* (2010). Towers Perrin & OpRisk Advisory, 10-17. URL: https://www.soa.org/globalassets/assets/Files/Research/Projects/research-new-approach.pdf.
15. Ramakrishna S. (2015). *Enterprise compliance risk management: An essential toolkit for banks and financial services*. Vol. 641. Singapore, John Wiley & Sons.

ABOUT THE AUTHORS

Anzhelika M. Krepysheva
Bachelor of NRU HSE (Saint Petersburg).
Research interests: compliance, business ethics.
E-mail: likamarkovna@mail.ru

Arina A. Sergievskaya
Business conduct leader of "Uniliver Rus" LLC.
Research interests: compliance, business ethics.
E-mail: arina.sergievskaia@unilever.com

Maxim A. Storchevoy
Candidate of economic sciences, associate professor of NRU HSE.
Research interests: compliance, business ethics, economics, management.
E-mail: m.storchevoy@rben.ru