351.746.5 :[005.52 : 005.334 (497.7) Scientific article

METHODS OF SECURITY RISK ASSESSMENT IN PRIVATE SECURITY

Saše Gerasimoski, PhD
Faculty of Security, Skopje, Republic of Macedonia
E-mail: sasegerasimoski@gmail.com

Abstract

The everyday life has always been filled with security risks, most of which we take for granted and for which we have developed routine strategies and ways of dealing and managing. However, the globalization and post-modern dynamics of contemporary societies have created a societal environment that multiplied the security risks and made their identification, assessment, management and dealing much more complex. This can be observed especially in security risks related with personal and proprietary security. Since personal and proprietary security fall within the field of private security, a question of developing adequate risk assessment as core of preventive work in private security becomes a priority. In this sense, having efficient methods for risk management and assessment is crucial in the overall performance of private security entities, providing subtle balance between their security efficacy and cost efficiency.

This paper deals with some of the most known and used methods for risk assessment, analyzing their importance and application in the private security. Several methods, which have been applied to private security entities in Republic of Macedonia, as well as abroad, are being singled out and closely discussed. Our focus, nevertheless, stays on the application of Keković, Kinney and AUVA methods of risk assessment within private security entities. Although these methods for risk assessment are widely used in different risk assessment methodologies in various spheres, they can be successfully adjusted and implemented in private security companies' risk assessment as well. The paper will consider the possibility of successful implementation of methods of security risk assessment in Republic of Macedonia. In addition, the author of the paper gives proposals, which could prove useful when implementing the risk assessment preventive policies, methods and strategies within the work of the private security entities.

Keywords: security risks, risk assessment methods, prevention, private security

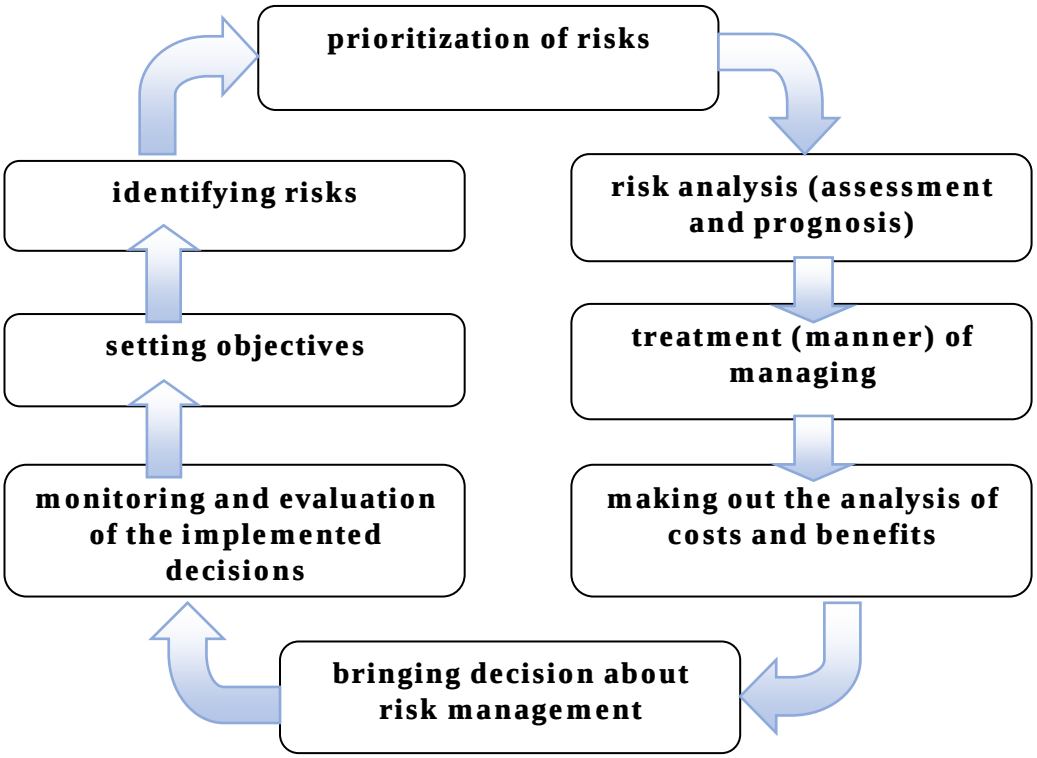
1. Introduction

The private security has experienced significant growth and development all over the world within the last three decades. They have been triggered by the constant growth and development of demand for protection and therefore, more and various private security services have been offered. Considering the character of private security, the services offered to the clients have mainly been preventive. Among the services that every serious private security entity (contract security) or company with integrated security function (proprietary/in-house security) offers in contemporary security environment, are certainly the risk analysis and risk assessment. Risk analysis and risk assessment have proven to be unavoidable in nowadays private security work, since they have to deal with large number or security risks that could affect security of persons, property, events or work processes within given organization or entity. In addition, the cost-effectiveness is the major equation when it comes to work of the security entities or other private entities that work in market conditions. Therefore, implementing quality risk analysis and assessment is crucial for not only the security performance and effectiveness, but is also necessary for proper balancing between security effectiveness and cost made for achieving it. This is simply because, for each private security entity or entity that needs security function, proper dealing with security risks means costs. In fact, for the management of the private security entity or entity that requires security of its assets this implies bringing decisions that see the security programs both from their effectiveness and from their cost efficiency (Hubbard, 2009: 10). That is why they must assure optimal security programme, which could make the security costs justified with its effective performance. Thus, the risk analysis and risk assessment are seen as two essential tools within the broader process of risk management that could make such security programmes optimal.

The contemporary risk management, risk analysis and risk assessment are impossible to imagine without quality risk assessment methodology. In addition, the risk assessment methodology is not something new, but its application in the private security work is relatively recent. The scientifically grounded methods for risk assessment were primarily developed within defendology, martial sciences and industry, but, considering its flexibility and broadness, they could easily be transformed and adjusted to serve the security assessment methodology in the private security sector as well.

Risk analysis and risk assessment as part of the risk management process

Assessment of security risks represents only one stage in the process of risk management with security risks, but also, the assessment is one of the most important documents produced within this process, and is essential for future prognosis, treatment of security risks and adoption of the best possible decisions in the process of risk management. The assessment and prognosis of the risks fall within the phase of risk analysis that covers a multitude of procedures to determine the risk-factors, their significance, the likelihood and possible consequences, criticality and vulnerability of the value to be protected in terms of possible risks and security risks separately. The end result of the risk assessment is determination of the risk size (level of risk, risk index), on the bases of which the most suitable means for the treatment and decisions on risk management with security risks are to be proposed later on. Risk assessment and risk prognosis are both part of the risk analysis, which itself is a phase in the process of risk management with security risks. The risk management is consisted, roughly, of eight phases, which form a cycle that repeats constantly. The eight phases of this cycle given in the graph below are: setting objectives, identifying risks, prioritization of risks, risk analysis (assessment and prognosis) (Герасимоски, 2010b), treatment (manner) of managing (Воган, 2014: 18-20), making out the analysis of costs and benefits, bringing decision about risk management, and monitoring and evaluation of the implemented decisions (ASIS International, 2003: 7).



Graph 1. The stages of the process of risk management

The word assessment itself, and the process of assessing the risks and security risks can be unclear, because the word assessment may relate to determining the nature and components of risk (risk factors) as a basis for scientific prediction or forecasting risks in a close future, but it could also mean a procedure with which the prediction, i.e. forecasting of its manifestation in the future is to be carried out. It is suitable to the spirit of Macedonian language, where, besides as a process of evaluation or assessment (valuation) or the result of it, the assessment is also being understood as an opinion or judgment of a phenomenon or event of reality (Муроски, 2005: 659). Therefore, the assessment may have meaning related to the assessment of risk factors, but also, of their prediction too. However, within the spirit of management science, analysis and assessment of risks and security risks in particular, we will look at the assessment as a procedure which falls within the phase of risk analysis, which aims to determine the nature and contents of the risks in terms of risk factors and to determine the size (level, index) of risk by analyzing the dimensions of risk (probability, criticality,

vulnerability and consequences of risks and security risks in relation to established goals and values of the subject who evaluates). Here, we make a clear determination of scientific prediction of risk, under which we understand the process of risk prognosis, which, together with the risk assessment, make the analysis of the risks and security risks.

If, based on the above, we should define risk assessment of security risks; we could define it as a procedure within the phase of risk analysis, which, by use of appropriate methods of assessment, determines the risk factors of security risks and the size (level, index) of risk, as a basis for further prognosis and treatment of security risks.

3. Methods of security risk assessment in the private security

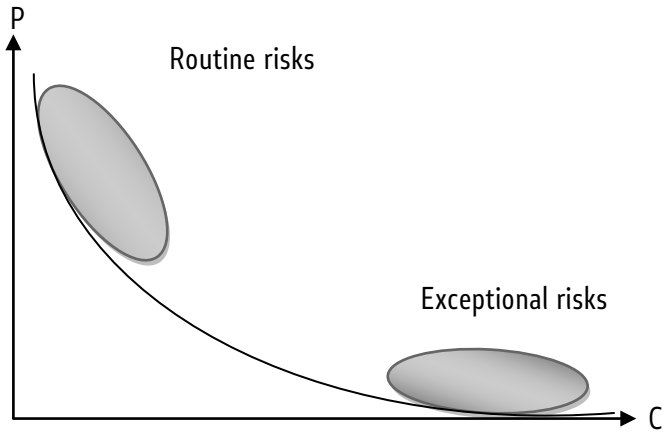
There are a multitude of methods to assess security risks in theory and practice of security sciences. Given the breadth of security as a concept, methods of risks assessment come from different areas in which a need for risk management exists, but most of the methods derive from the science of health and safety at work, military,industry and more recently, from computer security. General speaking, the methods of risk assessment vary according to the complexity, exactness and resources required for their application, and for all of them there is a common tendency to use some level of cross-reference of the variables of risk assessment and a degree of quantification (numerical expression) which connects empiricism with theory. In terms of the types of methods used in assessing security risks, they are divided into three groups: qualitative, quantitative and mixed (qualitative-quantitative). Choosing the method of assessment of the security risks is the decision of the joint consultation of the department/unit for analysis and management of security risks and the management of security entity or entity with an integrated security function. This choice has often been determined based on the entity's objectives, the available resources and acceptable level of risk. Because the security entities that provide private security services or proprietary/in-house security entities have to make risk assessments as part of their everyday work, we consider most of the methods used in other security spheres compatible and applicable to assessing security risks for persons, property or other phenomena (events, processes).

In essence, all methods for security risk assessment start from one basic formula that represents the unity of the values obtained by multiplication of the values of probability and possible detrimental consequences (damage) to the protected values of the entity. The level of

risk is determined as function of probability and consequence, according to the basic formula of risk assessment:

R=PxC where R-level (index, size) of risk
P-probability
C-consequence

When determining the method of risk assessment, it is crucial to have as comprehensive data as possible about the previous manifestations of security risks. This is important because the routine risks (those that are part of everyday work) and exceptional risks (those that happen extremely rare) influence differently on the choice of method for risk assessment, as well as on the whole process of risk management. This can be seen very well on the graph 2 below, showing routine risks as being one with high probability of happening followed with very small potential damage, and on the contrary, exceptional risks as being one with low probability of happening followed with very high potential damage. As we can see, the curve is exponential (goes close to x and y axes, but never touches or intersects them).



Graph 2. Diagram of probability vs. consequence (Кековиќ, Бакрески Стефановски, Павловиќ, 2016: 200)

From the multitude of methods for assessment of security risks that exist today in science and have already been applied in various spheres of security, we consider these three methods to be applicable to modern private security entities: *method of integral management with security risks developed by Zoran Keković and associates, Kinney method of security risk*

assessment and AUVA method of security risk assessment. The first two methods are qualitative, and the last is considered quantitative. The selection of methods is made based on their frequent application in practice worldwide and in our country and their relative ease of application, especially in terms of application of qualitative methods. Here, in this paper, due to standard limitations for the scientific and professional papers, only the very basics of these methods are to be presented.

3.1. Method of integral management with security risks by Zoran Keković and associates

Within its concept of integrated management of security risks in organizations, Zoran Keković, in collaboration with Goran Glisić and Nenad Komazec, developed a general method for assessing security risks (Кековић, Глишић, Комазец, 2010; Kekovič, Glišič, Komazec, 2009; Starčević, Ilić Paunović-Pfaf, 2010: 14). It is regarded as qualitative method, which has similarities with Kinney method, but is more complex in terms of the content of the variables. Thus, if the Kinney method has three variables whose multiplication give the possibilities of risk and afterwards determine the size of the risk (risk level, risk index); here we have a basic formula that includes two variables, which each by itself is calculated as product of two other component variables. This means that this model involves four variables that are integrated into the two basic formulas for calculating the size of the security risk. Thus, the formula for calculating the risk level of security risks according to this method is as follows:

RL = PxC, where RL-risk level
P-probability of certain event to result with negative Outcome
C-consequence or effect, which the negative event inflicts On value

The probability, on the other hand is being calculated by the following formula:

P = FxV, where P-probability
F-frequency of occurrence (appearance)
V-vulnerability or sensitivity of the organization to the Possibility of realization of risk and turning it into an Adverse event

The consequence is being calculated according to the following formula:

C = DxC, where C-consequence or effect

D-damage, as value (size) of damage of the protected Value on which the negative event caused consequences

C-criticality, which indicates the value or importance of The protected value for the organization on which the Negative event caused consequences

The calculation of the level of risk is carried out in such a manner that, first, a qualitative (descriptive) categories for the variables of probability and consequence are being determined and expressed through two-dimensional matrices and tables. The descriptive values are expressed through five categories for all variables of the matrices. Thus, the frequency can range from very rare, which is assigned a value of one, two is assigned for occasional, three for frequent, four for significantly frequent and five for very frequent. While the vulnerability has also five categories and can range in value from very large 1, large 2, medium 3, small 4 and very small 5. By multiplying these values and making out the matrix table the values of probability are being determined, which later on represent one variable within the calculation of the level of risk in the general formula. The damage as a variable gets the following values: very low one, low two, medium 3, large 4 and very large 5. Besides that, the criticality values are as follows: very large 1, large 2, medium 3, small 4 and very small 5. By crossing the values of these variables the matrix and the matrix table of the probabilities and consequences are being made and these values are then multiplied to obtain the values of the main matrix and the size of the risk.

We will present only the outlook of the final 5x5 matrix that determines the levels of risk by crossing the values of probability and consequence. The levels of risk ranging from 1-5 are considered as acceptable (marked with bright gray nuance), while the levels ranging from 6-25 (marked with darker to darkest gray nuances) are considered unacceptable and require some kind of treatment. This can be seen from the table 1 below:

Consequences		Very light	Light	Medium hard	Hard	Extremely hard
Probability		1	2	3	4	5
Rare	1	1	2	3	4	5
Less probable	2	2	4	6	8	10
Moderately probable	3	3	6	9	12	15
Probable	4	4	8	12	16	20
Almost certain	5	5	10	15	20	25

Table 1. Risk matrix with levels of risk according to the method of integral management with security risks by Zoran Keković and associates

This method for assessment of security risks is considered as easily adaptable and applicable in private security entities. Its relative easiness in use is complemented by the possibility to assess all assets and values of the private security entity or entity with an integrated security function (proprietary/in-house security). One can easily determine the risk factors, level of risk and propose adequate security treatment on different company values, whether they are assets such as physical objects, personnel, events or processes. Although mainly deemed as qualitative method, the method does not lack the necessary exactness, which can be seen through the 5x5 matrices of determining risk level. In addition, this method for assessing security risks also gives good cost-effectiveness ratio.

3.2. Kinney method of security risk assessment

Kinney method for assessing security risks is among the most widespread and popular qualitative methods for security risks assessment. Its wide application and popularity are owing to its relative ease of use, comprehensiveness, the relatively small resources needed for implementation and a good ratio of quality assessment against the costs of its application. These features make it a very competitive method of assessing security risks, considering even the far superior and more exact quantitative methods of security risks assessment (Gerasimoski, 2016a). This method was developed in 1976 by the Naval Weapons Center in California, USA, by G.F. Kinney and A.D. Wiruth. Due to the fact that G.F. Kinney was the lead

researcher of the research published in the paper "Practical risk analysis for security management", the method was named Kinney method (Kinney & Wiruth, 1976: 3-10).

The Kinney method stems from three basic assumptions:

- The risk can never be eliminated,
- The care and effort can reduce the risk down to acceptable level,
- Efforts to reduce risk should lead to the greatest possible benefits.

The formula for calculating the size of risk, according to Kinney method consists of three variables as follows:

R = LxExC, where R-risk size (level, index)

L- Likelihood of occurrence of an adverse event

E-exposure to an adverse event (Доревски, 2013: 84)

C-possible consequence of the realization of the adverse Event

This formula indicates that the multiplication of the values of the three variables is done by crossing the values of variables in the matrix and thus we receive values of the risk size (level, index), which may range in values of 20 or less for negligible risk, up to 400 or greater for risk whose occurrence could have disastrous consequences. Like any other method for assessing security risks, Kinney method also takes the data related to the previous manifestation and realization of the security risks in the form of encroachments. To this end, statistical data and other secondary data used to perform risk assessment and its prioritization depending on the goals of the entity evaluated are being primarily used. In Kinney method, previous security risks taken into account in relation to a particular security occurrence (event), may be expressed in units of damage as relations within the whole (for instance: number of attacks on object-theft, damage, sabotage, etc. for a period of time, or a certain number of cases if it comes to property, or number of injuries or deaths in the entity for a period of time or as the proportion in terms of a number of an investigated statistical mass if the appearance was present in the past, if it comes to persons). In addition, within the original version of the Kinney method, the expected detrimental effect on the risk is being expressed in dollars, so that it greatly facilitates the application of the appropriate treatment of security risks and application of the cost-benefit analysis.

The obtained sizes of risk are basis on which to propose measures and actions for security treatment of the related security risks. In the following table 2, descriptive categories

of the risk level, the values of the risk level and the measures and actions that should be taken for treatment of security risks, are being given.

Risk level	Value	Treatment of security risks
Very high risk	›400	Termination of activity
High risk	200-400	Taking urgent security measures and actions is necessary
Significant risk	70-200	Taking certain security measures and actions is necessary
Possible risk	20-70	Significant attention and monitoring of the situation is required
Insignificant (acceptable risk)	›20	Risk can be maintained; no need for taking any measures and actions

Table 2. Risk level, risk value and treatment of security risks according to Kinney method of security risk assessment

3.3. AUVA method of security risk assessment

AUVA method for security risks assessment is the abbreviation of the German AUVA (Allegemeine Unfall Versicherungs Anstalt) and loosely translated means a method for risk assessment in the workplace, i.e., a method of assessing professional risks (security risks associated with the profession). The Austrian association of producers of pulp and paper in 1995, in order to assess the professional security risks that the employees may face during the working process, developed it. This method is very similar to BG method for security risks assessment developed in Germany. The AUVA method is considered as quantitative or half-quantitative method for assessing the security risks in the workplace and is regarded as more accurate and less subjective than Kinney method (Gemović, 2011: 6-11; Stanković & Stanković, 2013: 135; Moraru, 2012: 13). Compared to Kinney method it is more complex, it requires greater expertise of the analysts for assessment of risks and implies higher costs and more

time for implementation. This method primarily applies to security risks assessment on the workplace and in the working environment.

The basic formula for security risk assessment according to AUVA method is identical to the aforementioned general formula for estimating the size (level, index) of security risks by the method of Zoran Keković and his associates, with one remark that the assigned values for the categories of variables are different. Thus, the basic formula for calculating the size of the security risk according to AUVA method is as follows:

R = PxC, where R- risk level
P-probability of an event resulting in negative outcome
C-consequence or effect of a negative event on the value

It should be noted that according to this method, the calculation of the level of risk is being carried out by the general formula and by making the matrix of the two variables (probability and consequence), but all of that after the probability was being calculated with a separate sub-matrix and the values of consequence (effect) were being determined. A key variable by which this method is known and differs from other methods, is the introduction of the variable for the fulfillment of the safety conditions in the workplace (working environment), which as variable enters within the formula and sub matrices of probability. Hence, the probability is calculated by the following formula:

P = ExFC, where P-probability
E-exposure of employees to possible dangers (harmful Effects)
FC-fulfillment of the safety conditions in the workplace (working environment)

Here, we'll only present the check-list for determination of the fulfillment of the safety conditions in the workplace (working environment) and the final table with numbers of the risk values, qualitative description of the risks, quantitative ranking of the risks and measures and actions for risk treatment. The variable of fulfillment of the safety conditions in the workplace (working environment) actually represents the assessment of security situation in the workplace (working environment) and is being determined with the help of checklists. A yes/no answers are being given for each separate category of check-list, and the goal is to determine the level of compatibility of safety requirements in the workplace (working

environment) with established security standards defined by legal acts (laws, rulebooks, statutes, etc.) and unwritten, but known ethical principles, practices and standards of performance in the field. An example of a checklist is given below.

No.	Workplace/working environment security rules	Analysis and assessment of compatibility with security requirements	The security situation in the workplace / working environment YES/NO
1.	Working space		
2.	Working surface		
3.	Tools and work equipment		
4.	Raw materials, basic and auxiliary materials		
5.	Fire and explosion protection		
6.	Brightness		
7.	Electromagnetic radiation		
8.	Noise		
9.	Tools and personal protective equipment		
10.	Crossing paths, access and evacuation		

Table 3. Checklist for determination of fulfillment of the safety conditions in the workplace (working environment)

When we obtain the values of probability and consequence, we make out the 5x5 matrix and get 25 possible risk values that represent the size (index, level of risk). This table is similar to the table for determination of the value of security risks by the previously elaborated method of integral management with security risks by Zoran Keković and associates. The final step of the AUVA method, as seen from the table 4, is making out of the table that contains numbers of the risk values, qualitative description of the risks, quantitative ranking of the risks and measures and actions for risk treatment.

Risk value number	Qualitative description of risk	Quantitative ranking of risk	Measures and actions of risk treatment (removal, prevention or reduction)
1, 2	Insignificant	1	Optimal working conditions (optimal protection of the employees).
3, 4, 5	Small	2	Satisfactory working conditions (the risk can be brought to ranking 1 with improvement of the work discipline and internal supervision).
6, 8, 9	Medium	3	Working conditions, which can, under certain conditions, lead to fulfillment of possible detrimental consequences and there is a residual risk that must be put under control.
10, 12, 15, 16	High	4	The work takes place in difficult conditions, with the strong possibility of incurring injuries or damage to the health of employees. Additional protective measures based on the analysis of injuries and diseases of employees have to be undertaken.
20, 25	Extreme	5	Very heavy working conditions with constant exposure of employees to harmful consequences during working activities. Banning the working activities is indispensable.

Table 4. Risk values, qualitative description of the risks, quantitative ranking of the risks and measures and actions for risk treatment according to AUVA method of security risk assessment

4. Some possible improvements from application of risk assessment methods in Republic of Macedonia's private security

Private security entities and entities with an integrated security function (proprietary security entities) should seriously consider the risk assessment as part of their management process, especially when managing security risks. Managing the security risks has become unavoidable since security risks are increasing in size and variety, as well as are getting more serious in terms of the consequences towards value and goals of the market-oriented entities. Therefore, private security entities, whether they are contract or in-house, must establish and develop quality risk management process where risk assessment takes crucial role (Станковски, 2013).

Republic of Macedonia has been developing its private security sector (subsystem) within the last 25 years. Although the risk management is not so recent in other parts of the world, the Macedonian experience in this field so far could be deemed as more than modest. Namely, most of the private security entities have not recognized adequately the need and importance of risk management as part of the wider management process, and particularly of management with security risks. However, since the status and role of the private security has been defined as primarily preventive-oriented, than, the private security entities in Republic of Macedonia have only recently understood the real need and potential of the process of security risks management, and, assessment of security risks as part of that process. It seems that nowadays, the private security entities are becoming more and more aware of their necessity and of the many improvements that they could bring to their work, both in terms of their professional performance and efficacy and in their economic performances. In this respect, according to the insight and knowledge of the author, some of the largest private security entities in Republic of Macedonia are seriously interested in implementing sound and up-to-date risk management process and risk assessment, speaking of security risks at first place. Thus, they have started to recognize that a quality and optimal risk management process and risk assessment of security risks could not be attained only through their empirical knowledge, but, they have to be prepared and willing to invest in implementing scientifically based processes of risk management and risk assessment, and, especially, in implementing sound methodology for assessment of security risks. Their implementation nowadays represents crucial precondition for their future status within the private security sector, since more of their clients seek high quality preventive security services, something that could not be achieved without sound and optimal risk management process and risk assessment methodology.

Without any doubt, bringing higher scientific standards and knowledge from this field to the private security entities and entities with an integrated security function should make them more competitive, professional and socially responsible. The optimal risk management process and risk assessment methodology can ease the risk identification, determination of their size and seriousness, as well as provide clear and quality alternatives in security risk treatment. Especially, we find the method of security risks assessment within organizations by Keković and associates, as well as the Kinney method, as highly suitable and easily implemented on risk assessment of different values and goals of private entities and private security entities in Republic of Macedonia in the future. The AUVA method could also been implemented because of its reliability and objectivity, but, it lacks the possibility to be implemented for assessing risks related to other values of the entities except persons (personnel and working environment).

When listing the numerous possible improvements which private security entities (both contract and in-house) in Republic of Macedonia could get from the application of quality risk assessment methods, we could single out the following:

- Strengthening of preventive politics and approaches within the entities;
- Reduction of subjectivity in risk management and risk assessment;
- Obtainment of highly reliable values of risk size (level, index);
- Setting quality basis for security risks prognosis;
- Determination of the most adequate treatment of security risks;
- Making out balanced cost-benefit analysis;
- Providing optimal grounds for risk management decisions.

5. Conclusion

All private security entities (contract or in-house) have to implement optimal and up-to-date security risk management process and risk assessment methodology. They are unavoidable for them because of their preventive role and function within the contemporary systems and their need to be competetitive in the market of private security services. Among numerous methods of security risk assessment, we find the Zoran Keković and associates method, the Kinney method and AUVA method to be suitable, reliable and practically applicable within the work of the private security entities in the Republic of Macedonia. We consider that application of these risk assessment methods could bring numerous and

significant improvements of the work to these entities, such as reduction of subjectivity in risk assessment, obtaining of highly reliable and useful values of risk size (level, index), determination of the most adequate treatment of security risks, making out of balanced cost-benefit analysis and other improvements in the overall risk management process.

References

1. ASIS International (2003). *General Security Risk Assessment*. Alexandria VA: ASIS International.
2. Воган, Џ. Е. (2014). *Управување со ризици*. Скопје: Арс Ламина.
3. Gemović, B. (2011). *Upravljanje rizicima kao elemenat integrisanog sistema menadžmenta preduzeća,* (neobjavljeni doktorski rad, iz arhiva autora). Beograd: Fakultet tehnickih nauka.
4. Gerasimoski, S. (2016a). "Application of Methods of Risk Assessment in Private Security". in *Private Security in the XXI-st century: Experiences and Challenges*. Skopje: Chamber of Republic of Macedonia for Private Security. pp: 327-338.
5. Герасимоски, С. (2010b). "Прогноза на ризиците во приватниот безбедносен сектор". *Хоризонти*. Битола. бр. 6. сс: 319-326.
6. Герасимоски, С. (2010c), "Проценка на ризиците во приватниот безбедносен сектор*". Годишник на Факултетот за безбедност*. Скопје. бр. 5. сс: 70-77.
7. Доревски, З. (2013). *Управување со ризици, обезбедување и кризни ситуации како елементи на безбедносниот менаџмент во компаниите во Република Македонија*. (необјавена докторска дисертација, од архивата на авторот). Скопје: Факултет за безбедност.
8. Kinney, G.F., & Wiruth, A.D. (1976). *Practical Risk Analysis for Safety Management*. China Lake CA: Naval Weapons Center.
9. Кековиќ З., Бакрески О., Стефановски С., Павловиќ С. (2016). *Планирање и процена на ризик: во функција на заштита на лица, имот и работење*. Скопје: Комора на Република Македонија за приватно обезбедување.
10. Кековић З., Глишић Г., Комазец Н. (2010). "Приступ методологији интегралног управљања ризиком у организацији*". Војно дело*. сс: 243-257.
11. Kekovič Z., Gliščič G., Komazec N. (2009), "Pristup metodologiji procene rizika*". Nauka, Bezbednost, Policija NBP, Žurnal za krimialistiku i pravo*. ss: 103-116.

12. Moraru, R. I. (2012). *Current Trends and Future Developments in Occupational Health and Safety Risk Management: Risk Management for the Future - Theory and Cases*. Rijeka: Intech.
13. Мургоски, З. (2005). *Речник на македонскиот јазик*. Скопје: Филолошки факултет „Блаже Конески".
14. Stanković M. & Stanković V. (2013). "Comparative analysis of methods for risk assessment-Kinney and AUVA". *Safety engineering*. Vol. 3, No. 3. pp: 129-136.
15. Станковски, Љ. (2013). "Планови за обезбедување и процена на безбедносната ситуација". *Современа македонска одбрана*. Том 13. Бр. 24. сс: 137-148.
16. Starčević J., Ilić M., Paunović-Pfaf J. (2010). *Priručnik za procenu rizika*. Beograd: Globe Design.
17. Hubbard, D. W.(2009). *The Failure of Risk Management*. Hoboken NJ: John Willey & Sons.
18. CoESS & UNI Europa (2004). *Preventing occupational hazards in the private security sector*. Wemmel: CoESS.