

Branko LESTANIN¹

Police officer, Ministry of Interior of Republic of Serbia

DOI: 10.5937/bezbednost2602093L

UDK: 351.746.2:005.334(497.11)

340.5(4-6EU)

Pregledni naučni rad

Primljen: 5. 3. 2026. godine

Revizija: 23. 5. 2026. godine

Datum prihvatanja: 17. 6. 2026. godine

Risk Assessment in Serbian Private Security: A Critical Review of the Legal Framework

Abstract: *The author explores risk assessment in the protection of persons, property, and business with special emphasis on its legal regulation in Serbia. In the paper, the author uses the normative method, the method of analyzing the content of available literature and legal regulations, the method of comparative law and, finally, through the synthesis of new knowledge, he tries to reach a unified conclusion. The first part of the research focuses on Serbia and its legal system, which relies on laws and secondary legislation. The second part of the paper deals with the comparative law of EU member states, some former republics of the SFRY, and some countries neighboring Serbia. Its conclusion is that Serbian primary and secondary legislation is not adequately adapted to the needs of private security in Serbia and that its amendment is necessary. Comparatively, the legal system that is best adapted from the aspect of private security risk assessment is that of Croatia.*

Keywords: *risk assessment, private security, law, standard, license.*

Introduction

The completion of the legal system and the improvement of the private security system in Serbia began with the adoption of the Private Security Act – PSA, Official Gazette of the Republic of Serbia, Nos. 104/13, 42/15 and 87/18 and the Private Detective Activities Act, Official Gazette of the

¹ b.lestanin@gmail.com, ORCID 0009-0009-5788-1658.

Republic of Serbia, Nos. 104/13 and 87/18 in November 2013. The adoption of secondary legislation that more closely regulates the area of private security was only completed at the end of 2016. Private security is not only affected by these two regulations, but by the legal system of Serbia as a whole. For example, the licensing procedure is governed by Administrative Law, while the protection of rules is permeated by criminal and misdemeanor legislation. Effective private security depends to a large extent on the legal protection and safety of its officers as holders of certain powers that have a coercive character (Leštanin, Nikač, 2022; Lestanin, Nikac, 2024a; Lestanin, Nikac, 2023a).

The history of risk begins among Greek philosophers and Arab mathematicians, and continues throughout human history among traders, scientists, intellectuals, and all those who deal with ways of predicting the future or prediction methods in their work. All risks that produce effect on the safety of people, property and business represent security risks in a broader sense, regardless of whether they are naturally or socially conditioned. When the source of the risk is the human factor, then we speak of risks with the attribute of unintentionality or intentionality. (Keković, et al., 2011: 24, 35). The term risk appeared in European languages at the end of the 15th century. The term was primarily used in the field of navigation and sea trade and meant the danger that threatened ships from rocks and reefs, as well as exposure to danger, a daring feat, a job or stake associated with the risk of failure, etc. (Grozdanovic, Stojiljkovic, 2013: 14).

The Oxford English Dictionary defines risk as exposure to the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility (<https://www.oed.com/search/dictionary/?q=risk&tl=true> available 25.2.2026). The Cambridge Advanced Learner's Dictionary defines risk as the possibility of something bad happening (<https://dictionary.cambridge.org/dictionary/english/risk> available 25.2.2026). Keković, et al. (2011: 25) understand risk as any possibility in a specific system that, with a certain probability, can cause an unexpected change in quality, i.e. change or loss of the system, as well as a forecast of possible damage, i.e. loss. The Institute of Risk Management defines risk as the combination of the probability of an event and its consequence. Hopkin considers risk as 'an unplanned event with unexpected consequences' (Hopkin, 2017: 15, 17). Katančević and Karović, (2016: 87) emphasize difference between risk and hazard. Risk is a scenario in which there is a probability of a harmful event materializing, which will cause consequences for the

elements of the observed system, while hazard is a potential source of an event that creates these consequences.

The Serbian Ministry of Interior – MoI (through its authorized police officers) and inspection bodies have the right to supervise private security and private detectives, each within its own scope of competences as stipulated by laws (Leštanin, Nikač, 2025c; Leštanin, Nikač, 2024c; Lestanin, Nikac, 2024b). An authorized police officer has the right and duty to inspect the conditions and manner of performing activities, record keeping, and, if necessary, to carry out other actions that provide direct and unannounced supervision into the performance of private security services (Nikac, Lestanin, 2023b). Private security officers in Serbia have certain legal powers that are similar (almost identical) to those of the police. States have gone so far as to 'collocate' the monopoly of force that they have given private security officers the ability, when legally issued conditions are met, to use force and even firearms (Leštanin, Nikač, 2025a; Leštanin, Nikač, 2025b).

The paper focuses on research into the legal framework through which the author will attempt to answer the questions of the compliance of the legal framework with the needs of private security in Serbia, using the normative method, the method of content analysis of available literature and legal regulations, the comparative law method, and finally, through the synthesis of new knowledge, to reach a comprehensive conclusion.

Risk Assessment in Private Security and Legal System of Serbia

Private security in Serbia occurs in two basic forms: 1) the provision of physical and technical protection by business entities that hold a legally issued license; and 2) the organization of an internal security service, i.e. in-house or self-protection activities (Leštanin, 2021). Risk assessment in the protection of persons, property, and businesses is only one type of activity in the field of private security for which a license is issued. Serbian legislator in Article 3 paragraph 1 point 6) of the PSA defines risk assessment as an analysis and evaluation in the protection of persons, property and business. International Standard ISO 31073:2022 Risk management – Vocabulary defines risk assessment as an overall process of risk identification, risk analysis and risk evaluation (<https://www.iso.org/> available 25.2.2026). This definition is also adopted by the Serbian standard SRPS A.L2.003:2025, Security and

resilience – Risk assessment – Requirements and guidance for conformity assessment (ISS, 2025).

A turning point in risk management occurred in the 1950s with the development of network planning techniques, such as the Critical Path Method and the Program Evaluation and Review Technique Method (Grozdanovic, Stojiljkovic, 2013: 35; Dionne, 2013). The overall risk management process aims to create adequate assumptions for making correct, timely and realistic decisions. Decision-making is the result of the risk management process and is determined by certainty, risk and uncertainty. Risk management can be defined as a process that aims to help an organization understand and assess risk and take steps to increase the likelihood of success and reduce the possibility of failure and uncertainty in achieving goals (Keković, et al., 2011: 52-53). The need to act now will often conflict with long-term goals and strategies, and in this sense, awareness of systemic risks and the changes they produce will increasingly be an imperative in the decision-making process in non-routine environments and situations characterized by a high degree of uncertainty (Keković, 2022: 33). According to Milošević and Keković (2011: 248), the concept of risk connects interdependent activities of management entities – analysis and assessment of risks, and their management, on the one hand, and planning and responding to unforeseen, complex and urgent situations caused by the realization of risks, on the other. Within the framework of such defined risk management activities, an important place is occupied by procedures for prioritizing and assessing previously identified risks. Risk assessment is a process that requires the application of special techniques and procedures, and therefore an adequate methodological approach. In other words, the basic activity in risk management is to eliminate the causes of risk events, eliminate the consequences and implement measures that lead to minimal losses if the event occurs. Consequently, it is a process that consists of risk identification, risk analysis and risk evaluation to assist the organization in the process of decision – making.

Risk assessment is regulated in the PSA Article 20, which is very complicated and, one might say, rigid due to the amendments and supplements to the PSA from 2018. Originally, this article of the PSA was reserved for regulating contractual issues in the field of private security, which the Serbian legislator used to 'attach' the issue of risk assessment. Article 20, paragraph 4 of PSA issues that a provider of private security services, except for risk assessment services in the protection of persons, property and business, **may not conclude a contract** with a service user **that establishes a lower level**

of security services than those provided for in the **act on risk assessment** in the protection of persons, property and business when this assessment is mandatory in accordance with this law. This specifically means that a risk assessment act would first have to be written down, recommending a certain level of security measures. Security measures would include physical and technical protection measures that would have to be specified. This means that the risk assessment act should not contain general security measures, but rather specific ones according to type, place and time of application. Only in this way can a risk assessment act written for the protection of persons, property and business lead to a reduction or complete exclusion of risks in a specific area of work and business. This provision of the law also has its own penal provision, and if someone fails to comply with it, a very strict fine is foreseen for licensed business entities.

According to the express provision of paragraph 5 of Article 20 of the PSA, the risk assessment in the protection of persons, property and business is carried out according to the requirements and in the manner issued by the applicable **Serbian standard in the field of private security** (more about standards later). In this way, all those who write the risk assessment act are obliged to apply the standard. Although this provision has an imperative character, it does not have a binding provision in the penal part of the PSA, so if someone does not act according to the standard and produces an act that is not in accordance with it, they will not be punished.² This has led to 'variegatedness' in the market for providing risk assessment services in the protection of persons, property and businesses, as some licensed business entities strictly adhere to the standards, some only partially and some not at all. PSA has a solution for such situations, but it is not implemented. Namely, the Accredited Body should and must assess the compliance of the quality of private security services with applicable Serbian and European standards. These activities are carried out at the request of the user of private security services, the provider of private security services or other interested parties (Article 75a).

If services are provided to users for the purpose of protecting persons, protecting residential buildings, or protecting public gatherings where security services are provided only by stewards hired by the organizers of the

² According to Art. 17 of the Standardization Law, Official Gazette of the Republic of Serbia, No. 39/09 & 45/15, the application of Serbian standards is voluntary and no one can be obliged (forced) to apply them.

gathering, a **risk assessment** for the protection of persons, property, and business **does not have to be performed**. Risk assessment does not have to be carried out also for the protection of micro legal entities and entrepreneurs (paragraph 6 of Article 20 of the PSA). This norm is interpreted as meaning that the law has envisaged exceptions to risk assessment and that it 'implies' that everyone who undertakes security measures is required to conduct a risk assessment before implementing security measures. Risk assessments can only be performed by business entities that hold a license for these activities, with the proviso that business entities with a self-protection license can also, for their own needs only, prepare a risk assessment report themselves.

The question may be raised as to why the legislator established certain exceptions to risk assessment. This especially applies to security and personal protection of persons. Personal protection is a particularly complex system of activities undertaken to prevent the security of a certain very important person (VIP) from being compromised. Before providing VIP security services, a risk assessment must precede it. The VIP security risk assessment act would contain a system of recommended or even mandatory physical and technical protection measures to mitigate the risks that threaten VIPs. The exemption of residential buildings from risk assessment is purely social, not security-related. By exempting these buildings, the legislator wanted to avoid a blow to the budgets of residents of certain low-income housing communities. However, the question arises as to how these communities have the money to take security measures but not to assess the risk, and how the level of security measures to be taken in a housing community will be determined.

When the act on risk assessment in the protection of persons, property and business is drawn up it becomes the basis for creating a **security plan**, or a risk management plan. When the risk assessment is not mandatory, the security plan is drawn up based on the request of the service user or the organizer of the public gathering. The requests are outlined in the PSA and the rules of the profession, but without specifying relevant provisions of the PSA, rules of the profession or even which profession specifically it concerns (paragraphs 7 and 8 of Article 20 of the PSA).

The Serbian legislator believed that it was not necessary to regulate the issue of risk assessment through secondary legislation and that referring to non-binding standards was sufficient. The first standard was SRPS

A.L2.003:2010, Social security – Risk assessment in the protection of persons, property and business, adopted in 2010, three years before the PSA itself. This standard was replaced by the SRPS A.L2.003:2017, Social security – Risk assessment in the protection of persons, property and business, which was valid until February 2025, when SRPS A.L2.003:2025, Security and resilience – Risk assessment – Requirements and guidance for conformity assessment, was adopted.

The latest standard, similar to its predecessors, provided the subject matter and scope of application, defined the main terminology used in the standard, provided normative references, regulated the risk assessment process (principles, values, context, identification, analysis, evaluation, etc.), defined the requirements for risk assessment, i.e. a description of the criteria that must be met by the organization being assessed, determined the methodology for conducting risk assessment, provided instructions for the assessment of organizations and individuals, and finally normative and informative annexes.

The main changes compared to the previous edition are that the title has been changed in the new standard, where the wording ‘Requirements and guidance for conformity assessment’ has been added, which represents an adaptation to changes in the field of work of the commission and certification needs. The normative references that served as the basis for the development of this edition, where the range of standards has been changed and expanded, have been updated. Additional terms that are important for understanding risk assessment and are not defined in the standard SRPS A.L2.001, Social security – Private security services – Glossary, have been defined (e.g., notes have been removed for resilience, the definition of business continuity has been changed, the definition of risk has been changed with fewer notes, etc.).

Defining the external context	The external context includes the risk assessment for facilities or areas that are not physically located within the organization's perimeter or premises, but are under its control or influence. This assessment includes an analysis of the risks and their impact on the organization, taking into account external factors such as location, accessibility, the surrounding environment and potential threats that may arise from sources outside the organization.
-------------------------------	--

Deadlines for implementing measures	Timelines for implementing measures are critical to effective risk management. The security partner, or risk manager in the case of an assessment for its own purposes, should define clear deadlines for each risk mitigation measure. These deadlines should be realistic and based on resources, the complexity of the measure and the priority of the risk. Establishing deadlines will allow for regular monitoring of progress, identification of potential bottlenecks and ensure that measures are implemented on time. The organization should conduct regular audits to ensure that deadlines are met and that corrective action is taken if deviations occur.
Monitoring and reporting on the implementation of measures	Each risk mitigation measure should be assigned a responsible person who will be responsible for monitoring its implementation and reporting on progress. Reports should contain information on the current status of the measure (new, implementation in progress, partially implemented, implemented, measure abandoned) and be provided to management at regular intervals. In the event that a measure is not implemented within the planned deadline, it is necessary to analyze the reasons for the delay and define a new action plan in order to successfully implement the measure.
Priorities and time alignment of measures	Risk mitigation measures should be prioritized based on the level of risk and resource availability. Timing should take into account the urgency and importance of each measure to ensure optimal implementation and minimize the negative impacts of the risk on the organization.
Control and audit have been supplemented	Monitoring and ensuring the implementation of measures in accordance with defined deadlines; to identify and correct deviations from the defined deadlines for the implementation of measures in a timely manner, in order to ensure their efficient and timely implementation; to regularly report on the status of the implementation of measures, including the current status, identified bottlenecks and corrective measures taken to overcome these bottlenecks.
Registration of the risk assessment process	All relevant risk assessment information must be recorded in a digital risk assessment register, which allows for full traceability in accordance with the prescribed standard forms.

IT support for the risk assessment process	All collected data related to risk assessments and their revisions must be stored by the security partner in a digital risk assessment register.
Assessment of service providers	Service provider assessment is a process that ensures that a service provider (security partner) meets all the necessary standards and criteria in the risk assessment for the observed organization. The conformity assessment body is responsible for conducting the security partner assessment to ensure the legality, impartiality, accuracy and reliability of the data in the risk assessment process.

Table 1. *The main changes in risk assessment process*

The risk assessment process has been described in more detail and supplemented (Table 1) in the part relating to defining the external context, deadlines for implementing measures, monitoring and reporting on the implementation of measures etc. The changes compared to the previous edition are in general where the risk assessment requirements are expressed qualitatively (textual description of the criteria) and quantitatively (numerically from 0 to 5, or as a percentage, or in monetary terms), depending on how conformity assessment bodies and/or organizations can assess compliance for their own purposes. All relevant information must be recorded in a digital risk assessment register, which allows full traceability in accordance with the prescribed forms given in the standard.

Requirements for an organization that provides risk assessment services	The requirements for the qualification of a risk manager require the manager to have a security certificate, in accordance with the regulations on the protection of data confidentiality, when his/her organization provides services to critical infrastructure facilities and knowledge of at least one foreign language at the A1 level. The manager is not required to have passed a professional exam in fire protection or a license for risk assessment in the protection of persons, property and business.
Requirements for general business activities	Creditworthiness assessment is no longer required, but an assessment of organizational measures is performed (for example, whether it has a rulebook on the organization and systematization of work, a (public) procurement plan), and the requirements for having records of various types of damage remain.

Requirements for safety and health at work and in the work environment	Based on the assessment of the risk to safety and health at work, a special inspection is carried out into the fulfillment of the conditions for security officers who are hired by an external licensed legal entity or are hired as part of a self-protection activity, which is particularly emphasized in the analysis.
Requirements for fire risk and explosion risk	Consent of the MoI on the investment and technical documentation, the fulfilled condition and use of the facility or part of the facility is no longer an item that affects the assessment.
Requirements for natural disasters and other accidents	Equipment for dealing with emergency situations and the established early warning, notification and alert system are also checked.
Requirements for the assessment of ICT systems	Completely changed

Table 2 – Main changes in requirements for risk assessment

According to Table 2, risk managers in the future must modify survey questionnaires or interview checklists depending on the methods they used to collect data about the organization being assessed. The risk assessment guide, i.e. the application of the risk assessment methodology with precisely defined criteria and methods for calculating the risk level, is presented in more detail. Risk managers must use certain attachments in the assessment process and provide evidence thereof. Consequently, the amended requirements have also changed the criteria for assessing the fulfillment of requirements, resources and quality of services of organizations and persons performing risk assessment. In the criteria for determining probability, the criteria for determining exposure and vulnerability have been changed and the impact of the magnitude of the hazard has been introduced, and in the criteria for determining consequences, the criteria for determining damage have been changed, where the criterion for determining the probable maximum damage has been added and the impact of the activity has been introduced into the calculation.

When dealing with risks, it is envisaged that taking measures may be different and depend on financial capabilities, available time and other factors. Consequently, the organization may take measures that will not have a full impact and reduce the risk to an acceptable level. In this case, the remaining risk is called residual and is subject to further measures. Deadlines for updating the risk assessment act and the security plan are prescribed. A

large number of annexes have been changed, but most importantly, the template for the risk assessment act has been changed so that the layout must be changed in practice. The previous points in the Introduction relating to the initiation of the process and the legal basis have been deleted; the handling of risks is presented differently; a conclusion to the act is introduced; and monitoring and communication with risks are no longer mentioned. Probably the most important change to the standard relates to the introduction of digitalization in the area of risk assessment in the protection of persons, property and businesses, where recommendations are also made as to which programs/platforms can be used in the creation of a digital risk register.

Private Security Risk Assessment in Comparative Law

Analysis of ISO standards showed that there are three main standards in the area of risk management in private security: 1) ISO 31000:2018 Risk management – Guidelines, 2) IEC 31010:2019 Risk management – Risk assessment techniques, and 3) ISO 31073:2022 Risk management – Vocabulary. The standard ISO 31000:2018 Risk management – Guidelines replaces the first edition from 2009. As the publisher himself states, the main changes are: principles of risk management, highlighting of the leadership by top management, greater emphasis on the iterative nature of risk management and streamlining of the content with greater focus on sustaining an open systems model to fit multiple needs and contexts. As the title of the standard itself suggests, IEC 31010:2019 Risk management – Risk assessment techniques addresses the topic of risk assessment techniques and methods and replaces the 2009 version. The most important feature of this standard is the informative annexes that specifically explain the risk assessment process and the application of techniques and methods for conducting the risk assessment process. The standard ISO 31073:2022 Risk management – Vocabulary represent the basic vocabulary to develop common understanding on risk management concepts and terms among organizations and functions, and across different applications and types and replaces the 2009 version (<https://www.iso.org/available> 25. 2. 2026).

Although **Slovenia** is a member of the EU, its legal system is similar to that of Serbia, as the two countries were once part of a single legal system. Consequently, Slovenia has regulated the area of risk assessment with its PSA and one regulation. Article 5 point 12 PSA defines risk assessment as an assessment of the danger or threat, which is based on the security needs

of the protected area, compliance with regulatory requirements, capacities and other circumstances, and the likelihood of consequences that could affect security, and is the basis for drawing up a security plan (<https://pisrs.si/pregledPredpisa?id=ZAKO5760> available 3.3.2026). Slovenia did not recognize risk assessment in its PSA as a specific type of license that a persons or business entities need to hold in order to carry out risk assessment in the field of private security.

Art. 2 point 3 of Regulation on the Mandatory Organization of Security Services at Public Events stipulates that risk assessment is an assessment of the risk that a public event could result in a serious breach of order involving a large number of people (<https://pisrs.si/pregledPredpisa?id=URED5288> available 3.3.2026). Also it can be defined as threat to public order, possibly conducive to violence or general disorder, thereby endangering the safety of people and property or endangering public traffic, and is the basis for drawing up a security plan. Art. 3 paragraph 2 of Regulation stipulates that providing security services includes the preparation of a risk assessment, a security plan and the regular implementation of physical security or physical and technical protection of public events based on the prepared plan. The Regulation then in Article 5 defines the level of risk (low, medium and high) where risk level assessment shall be made taking into account the nature and program of the event, the venue, the number and structure of participants, the duration of the event and other circumstances that affect the provision of safety. Since Slovenia is a member of the EU and ISO, it can be assumed that it is fully compliant with the standards of these organizations.

Croatia, like Slovenia, is a member of the EU and ISO and once was part of a unified legal system, and has regulated the area of risk assessment with its PSA and detailed with rulebook. Article 2, point 22 of the Croatian PSA defines a threat assessment as a document that determines the assessment of the probability of an event that poses a possible danger and threat to persons and property (<https://www.zakon.hr/z/291/zakon-o-privatnoj-zastiti> available 3.3.2026). Article 3, paragraph 2, stipulates that before establishing private protection, it is necessary to prepare a threat assessment that will determine the actual level of risk of committing felonies and endangering the lives and property of persons in a facility or on a public or other surface, depending on external and internal threat factors. This also includes technical protection, which is specified in Article 79, paragraph 1, which stipulates that before installing elements, structures, devices and technical protection systems, a vulnerability assessment is made for each

protected object, space or surface, which will be used to categorize the protected object, space or surface. The obligation to prepare a risk assessment exists both before commencing security work for particularly important persons (Article 64) and before establishing protection for other consignments and persons in road transport (Article 67). These four imperative norms are linked to the penal part of the PSA, which envisages fines for business entities that behave contrary to these four norms. As can be seen, the Croatian legislator has clearly and unequivocally taken the position that a risk assessment is carried out in all cases when security measures are implemented under the jurisdiction of private security, without exception. Of course, this rule is reinforced by the fact that the Croatian legal system has also recognized risk assessment as a special type of license in private security businesses. In addition to its supervisory powers in the implementation of the PSA, the Croatian MoI also has the obligation to give consent to risk assessments and project documentation for Category I, II and III facilities and Category I public areas, and participates in technical acceptance of installed elements, devices and technical protection systems for the same categories of facilities and areas.

When categorizing issue, the Croatian PSA distinguishes between protected objects and spaces in general and public and other areas (Article 79). Protected objects and spaces can be categorized into six categories: Category I – highest level of protection, Category II – high level of protection, Category III – higher level of protection, Category IV – medium level of protection, Category V – lower level of protection, and Category VI – minimum level of protection. Public and other areas can be categorized into three categories: I – high level of protection, II – medium level of protection, and III – lower level of protection. The vulnerability assessment for Category I and Category II facilities and Category I public areas is prepared for a period of five years, after which it is revised.

By properly considering the problem of risk assessment in private security, the Croatian legislator adopted a rulebook that regulates the procedure and method of categorizing protected facilities, preparing a threat assessment, implementing the audit procedure, and the quantification procedure. The Rulebook on Making Assessments of Threats to Persons, Objects and Spaces specifically addresses the issue of the content of the risk assessment and security plan for the protection of very important persons, especially for facilities and public areas, but also as part of the risk assessment for all types of security work. This particularly applies to the description of

the existing situation, hazard analysis, quantification of vulnerability, the issue of categorization and consent to the risk assessment. It is particularly important that the rulebook contains a large number of annexes, similar to the Serbian standard, which assist in the preparation of a risk assessment.

Germany is a member of the EU and ISO and certainly serves as an example for both Serbia, which is not a member of the EU, and other EU members. According to Tóth (2023: 176) *Verband der Sachversicherer e.V.* (VdS), is the umbrella organization of the German insurance industry. It performs risk assessments, product certifications, site inspections, and certifies businesses and professionals in the areas of property protection, fire and occupational safety, and cyber security. Their knowledge, their tests and certifications as well as their risk assessments and training courses are decisive success factors for their customers and partners. The task of their risk management business unit is to holistically identify various internal sources of danger, to provide specific recommendations for preventive action (directly on site), and thus place the security of companies on a solid foundation (<https://vds.de/ueber-vds> available 3.3.2026). Based on these statements, we conclude that in the German legal system there is no license for performing risk assessment, but rather there is one company that issues certain types of certificates and simultaneously performs risk assessment work. All of these jobs are focused on the safety of property from an insurance perspective in order to prevent large insurance premium payments due to the occurrence of a harmful event.

The Hungarian Act CXXXIII of 2005 on the Rules of Personal and Property Protection and Private Investigation Activities (<https://njt.hu/jogszabaly/2005-133-00-00> available 3.3.2026), and the Bulgarian PSA (<https://www.mvr.bg/en#> available 3.3.2026), do not regulate the area of risk assessment. Hungary and Bulgaria are members of the EU and ISO.

Montenegro is another state which emerged from the Yugoslav community and is not yet a member of the EU, and which has regulated private security by Protection of Persons and Property Law (<http://sluzbenilist.me/> available 3.3.2026). Article 14, Paragraph 2 of the Protection of Persons and Property Law provides that the protection of a mandatory protected facility is carried out on the basis of a protection plan that contains an assessment of safety, vulnerability and risk, a physical security report and a technical protection project. Paragraph 4 of the same article regulates the duty of the client to engage the business company that performs the protection activities referred to in paragraph 1 once a year, and when certain circumstances

change during the year, based on a risk assessment, and before the expiration of one year, to audit the protection plan. From the cited provisions of the regulations, we can see that the Montenegrin legislator did not want to deal too much with regulating risk assessment. Also, there is no special type of license for these private security jobs in the legal system. The risk assessment is only part of the security plan that is drawn up only in a situation where the security of the facility that is mandatorily secured is being maintained. Regarding membership in ISO, Montenegro currently has observer status but has the possibility to adopt standards.

The North Macedonian PSA (<https://mvr.gov.mk/mk-MK/legislativa/zakoni> available 3.3.2026), and the Russian Federal Law on Private Detective and Security Activities from 1992 (<http://www.consultant.ru/> available 3.3.2026) do not regulate the area of risk assessment. North Macedonia and the Russian Federation are full members of ISO, where they not only participate in the implementation but also in the adoption of standards.

Conclusion

From the introductory discussion, we conclude that the history of risk dates back to ancient times. Nevertheless, to this day there is no single definition of risk, so it can be concluded that there are as many definitions as there are scholars. In the 21st century, legal regulations also deal with the definition of risk, risk management and other concepts. Serbia is making its early steps in this area because it started legal regulation of private security comparatively recently. Regardless of the differences in defining risk and risk management, the point is that management is a process that aims to reduce the impact of risk on the ultimate outcome of a particular organization's goal. That goal can be non-profit or profitable, depending on the type of organization affected by the risk.

The Serbian Private Security Act has attempted to regulate the area of risk assessment in private security, but not very successfully. First of all, the legislator tried to place all the rules on risk assessment and private security planning in one article of the law, which is impossible for such an issue. In addition, although the norm has an imperative character, there is no penal norm that would, in the event of non-compliance, lead to adequate punishment and thus acquire a full legislative character. The application of non-binding standards, on the one hand, may seem like a good legal solution, however, in the specific case of Serbia, we have a completely opposite

situation. Although there is a special body that should deal with compliance assessment, it has not been implemented in Serbia. A much better solution is to regulate the risk assessment process through secondary legislation that is binding for all licensed business entities. In this sense, *de lege ferenda* should explicitly regulate the performance of private security services without a risk assessment as a misdemeanor with a serious fine. The assessment activity itself should also be regulated by secondary legislation. Ultimately, the police should give consent to the risk assessment.

On the international 'playground', there are standards regulating the area of risk assessment, with which the Serbian standard is more than compliant. This means that the Serbian standard is more detailed and certainly more extensive than international ones, with the main drawback being that it is non-binding for those who apply it. In comparative law, we note that all analyzed countries are ISO member states and accept standards in the field of risk assessment. Some countries have dared to fully regulate the risk assessment process through law and secondary legislation, some refer to the application of standards, and some only mention risk assessment as part of the planning process, implying the application of standards. The best solution, however, is to fully regulate the rules of risk assessment through legal regulations that have a binding character.

References

1. Dionne, G. (2013). Risk Management: History, Definition, and Critique. *Risk Management and Insurance Review*, 16(2): 147-166. <https://doi.org/10.1111/rmir.12016>
2. Grozdanović, M., Stojiljković, E. (2013). *Metode procene rizika*. Fakultet zaštite na radu, Niš.
3. Hopkin P. (2017). *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management* 4th ed. Kogan Page Ltd, London, New York.
<https://mvr.gov.mk/mk-MK/legislativa/zakoni>
<https://njt.hu/jogszabaly/2005-133-00-00>
<https://pisrs.si/pregledPredpisa?id=ZAKO5760>
<https://pisrs.si/pregledPredpisa?id=URED5288>
<http://sluzbenilist.me/>
<https://vds.de/ueber-vds>
<http://www.consultant.ru/>

- <https://www.iso.org/>
<https://www.mvr.bg/en#>
<https://www.zakon.hr/z/291/zakon-o-privatnoj-za%C5%A1titi>
4. ISS (2025). *SRPS A.L2.003:2025, Security and resilience – Risk assessment – Requirements and guidance for conformity assessment*. Institute for Standardization of Serbia, Belgrade.
 5. Katančević, V. T., & Karović, S. (2016). Threat identification, and risk assessment and monitoring as a form of early warning. *Vojno delo*, 68(2): 84-107. <https://doi.org/10.5937/vojdela1602084K>
 6. Keković, Z. (2022). Effects of uncertainty in decision-making about system risks. *Godišnjak Fakulteta bezbednosti*, (1): 15–37. https://doi.org/10.5937/fb_godisnjak0-37572
 7. Keković, Z., et al. (2011). *Procena rizika u zaštiti lica, imovine i poslovanja*. Centar za analizu rizika i upravljanje krizama, Beograd.
 8. Lestanin, B., Nikac Z. (2024a) Criminal Law Protection of Private Security Officer in Serbia. In *International Scientific Conference 'Dynamics of Modern Legal Order' Thematic conference proceedings*, Kosovska Mitrovica, pp 41-50.
 9. Lestanin, B., Nikac Z. (2024b) Legal Aspects of Police Supervision of Private Physical Security in Serbia. In *Conference Proceedings of International Significance 'Archibald Reiss Days'*, vol. 13, Belgrade, pp 195-205.
 10. Lestanin, B., Nikac Z. (2023a). Legal Framework for Life Protection of Private Security Officers in Serbia. In *International legal relations and justice: proceedings of the 36th Meeting of Kopaonik School of natural law - Slobodan Perovic, international scientific conference*. Vol. 1, Belgrade, 135-150.
 11. Leštanin, B., & Nikač, Ž. (2022). Prekršajna odgovornost u oblasti privatne bezbednosti u Srbiji. *Pravna riječ* 65(19): 570-593.
 12. Leštanin, B. S., & Nikač, Ž. V. (2025a). Private security officers as officials in criminal law of Serbia. *Baština*, (65): 413-430. <https://doi.org/10.5937/bastina35-56650>
 13. Leštanin, B. (2021). *Privatna bezbednost*, Službeni glasnik i Akademija Oxford, Beograd.
 14. Leštanin, B., & Nikač, Ž. (2025b). Powers of private security officers in Serbia and human rights and freedoms: Some dilemmas and possible solutions. *NBP. Nauka, bezbednost, policija*, 30(2): 159-176. <https://doi.org/10.5937/nabepo30-55299>

15. Lestanin, B., Nikac Z. (2024c) Specificities of Private Detective Activities Supervision by the Police in Serbia. In *International Scientific Conference Challenges and Open Issues of Service Law* vol. 2, Kragujevac, pp. 289-303.
16. Lestanin, B., Nikac Z. (2025c). Supervision of Technical Protection by the Police in Serbia: Legal and Practical Aspects. In *Zbornik radova sa Savetovanja pravnika XXVIII Savetovanje Budvanski pravnički dani*, Belgrade, pp. 401-418.
17. Milošević, M., & Keković, Z. (2011). Risk assessment in protection of persons, property and business affairs: Risks of illegal behavior and lack of adequate normative regulations. *Vojno delo*, 63(1): 346-360.
18. Nikac Z., Lestanin, B. (2023b). *Privatna bezbednost: pravo, teorija i praksa*. Kriminalističko-policijski univerzitet, Beograd.
19. Private Security Act, Official Gazette of the Republic of Serbia, No. 104/13, 42/15 and 87/18.
20. Private Detective Activities Act, Official Gazette of the Republic of Serbia, No. 104/13 and 87/18.
21. Standardization Law, Official Gazette of the Republic of Serbia, No. 39/09 & 45/15.
22. Tóth, A. (2023). Establishing the Evaluation Criteria System for Private Security Companies in Hungary. *Hungarian Law Enforcement*, 23(1): 173–189. <https://doi.org/10.32577/mr.2023.1.11>

Процена ризика у приватној безбедности у Србији: критички осврт на правни оквир

Анстракт: Аутор истражује процену ризика у заштити лица, имовине и пословања са посебним акцентом на њено правно уређивање у Србији. У раду аутор користи нормативну методу, методу анализе садржаја доступне литературе и правних прописа, упоредно-правну методу и кроз синтезу нових знања покушава да дође до јединственог закључка. Први део истраживања фокусира се на Србију и њен правни систем, који се ослања на законе и подзаконске акте. Други део рада бави се упоредним правом земаља чланица ЕУ, неких бивших република СФРЈ и неких земаља које су суседи Србији. Закључено је да српско примарно и секундарно законодавство није адекватно нити прилагођено потребама приватног обезбеђења у Србији и да је његова измена неопходна. Упоредно гледано, најбоље прилагођен правни систем са аспекта процене ризика у приватној безбедности је у Хрватској.

Кључне речи: процена ризика, приватна безбедност, закон, стандард, лиценца.