March 19, 2026

Fourth Memorial Scientific and Professional Conference "Predrag Marić"
MODERN INTEGRATED DISASTER RISK MANAGEMENT

Faculty of Security Studies, University of Belgrade DOI: https://doi.org/10.5281/zenodo.20412812

Article review

Corporate Security as an Integral Part of the Disaster Risk Reduction and Emergency Management System

Jana M. Marković[1]*, Nenad P. Radivojević[2]

[1] Faculty of Security Studies, University of Belgrade, Gospodara Vučića 50, 11000 Belgrade, Republic of Serbia; jana.markovic@fb.bg.ac.rs

[2] Law Faculty in Novi Sad, University of Novi Sad, Trg Dositeja Obradovića 1, 21102 Novi Sad, Republic of Serbia; n.radivojevic@pf.uns.ac.rs

* Correspondence: jana.markovic@fb.bg.ac.rs; tel.: +381 62 264 834

Abstract

The Disaster Risk Reduction and Emergency Management System in the Republic of Serbia (hereinafter: DRREMS) is regulated by the Law on Disaster Risk Reduction and Emergency Management. This Law establishes an integrated approach to disaster prevention, preparedness, resilience, response, and recovery. Although the Law recognizes the importance of companies and legal entities participating in this system, the question of how to operationalize their role in practice arises. Namely, companies and other legal entities have a legal obligation to prepare a Disaster Risk Assessment and a Protection and Rescue Plan, and to undertake risk prevention and reduction measures within the framework of their activities. They are also required to act upon the request of the competent emergency headquarters and participate in implementing protection and rescue measures. A special role is played by companies and other legal entities recognized

Academic Editor:
Prof. Dr. Vladimir M. Cvetković

as of particular importance for protection and rescue, as well as those that perform certain activities, mainly facilities and systems that constitute critical infrastructure. The efficiency and effectiveness of these entities depend on an optimally organized and functional corporate security system. In addition to the basic function of corporate security, which is the security of persons, property, and operations at the level of a legal entity, it should be borne in mind that corporate security systems have significant potential for taking measures to reduce the risk of disasters, for effective risk management, and even for the rehabilitation and mitigation of the consequences of disasters. As the DRREMS is recognized as an integral part of the national security system, corporate security systems can be viewed and appreciated as a subsystem of DRREMS in the same way. The paper starts from the thesis that corporate security is an integral part of DRREMS in the Republic of Serbia. Corporate security, through its functions, primarily through risk assessment, development of protection and rescue plans, crisis management, and ensuring business continuity, contributes to the improvement of proactive action, reduces the consequences of disasters, and increases the overall resilience of society.

Keywords

Corporate security, private security, disaster risk reduction, emergency management, Republic of Serbia.

1. Introduction

Governance has become one of the key tools for addressing an increasingly diverse and complex set of social problems. A special place in this context is occupied by disaster risk management and/or emergency management, as a dynamic and multidisciplinary field that encompasses prevention, preparedness, response, and recovery from various types of risks and disasters. Modern approaches indicate that this field is inseparable from the broader concept of disaster risk reduction, which strives for proactive action and for strengthening society's resilience as a whole. Today, it is impossible to imagine emergency management as an area in which government agencies, i.e., state bodies, act independently (Kapucu, 2012, p. S41). On the contrary, the effective functioning of this system implies the involvement of a wide range of actors, including the private sector, non-governmental organizations, academia, and local communities. Corporate security is of particular importance in this system, which extends beyond individual organizations and becomes an integral element of national security and social resilience.

The Disaster Risk Reduction and Emergency Management System (DRREMS) in the Republic of Serbia is regulated by the Law on Disaster Risk Reduction and Emergency Management (hereinafter: Law). This system is of particular interest to the Republic of Serbia and represents an integral part of the national security system (Article 1, paragraph 2). However, although companies are recognized by law as subjects of this system, their role in practice often remains insufficiently operationalized. Namely, they have certain obligations: to prepare disaster risk assessments and protection and rescue plans, to act at the request of the competent emergency headquarters, or to participate in protection and rescue measures. Despite this, the actual implementation of these obligations in practice remains unclear and questionable. It is accompanied by numerous problems, such as a lack of trained and professional personnel, insufficient financial investment, a lack (or complete absence) of effective cooperation among the system's subjects (for example, those within or between local government units), etc.

The paper starts from the thesis that corporate security, as part of the national security system, also constitutes an integral subsystem of the DRREMS, as reflected most clearly in its functions. This thesis is further supported by the fact that the Sendai Framework for Disaster Risk Reduction emphasizes the importance of investing in innovation and technology development in disaster risk management. In this context, in one of the texts of the United Nations Office for Disaster Risk Reduction, the private sector is recognized as an important stakeholder, i.e., an interested party whose role is reflected in the development and application of innovations, technological progress, strengthening public-private partnerships, as well as in improving the connection between science, policy, and practice (UNISDR, 2016). The private sector recognizes this role through corporate security, one of its business functions.

The work is organized into four interconnected units, which move from the general to the specific and individual, in such a way as to enable a gradual, logically connected view of the relationship between DRREMS and corporate security as its significant segment. The first part discusses the concept and importance of DRREMS as an integral part of the national security system; the second part analyzes the concept and functions of corporate security in the protection of persons, property and business; The third part analyzes the Law, with a special focus on the subjects and forces of the system and their obligations; while the fourth part discusses the role of corporate security within the DRREMS, with an emphasis on its functions, i.e. its contribution to prevention, risk management, response to crisis (emergency) situations and ensuring business continuity, which in fact argues for its position as an integral part of this system.

2. The concept and importance of a disaster risk reduction and emergency management system

One of the earliest and probably most frequently cited definitions of a disaster is that developed by Charles Fritz. According to this author, a disaster is "an event, concentrated in time and space, in which a society, or a part of society, is threatened by danger and suffers such losses that the social structure is disrupted and the fulfillment of all or some of the essential functions of society is prevented" (Fritz, 1961, p. 655). An emergency, on the other hand, arises when the consequences of a disaster or serious threat exceed the system's regular capacity and require the application of special response measures.[1]

The DRREMS integrates two directions of action that are usually, and especially in foreign literature, considered separately. These are disaster risk management and emergency management, which will be discussed in the rest of the paper. Some authors point out that, both for scientific study and for practical implementation, a deep understanding of the cultural and social conditions that shape the domains of disaster risk reduction and management is necessary (Sandoval et al, 2023, p. 354). What we must also take into account, and which forms the basis for the organization and operation of any system, including the DRREMS, is the law. In this regard, it is also necessary to analyze the relevant provisions of national legislation.

In the extensive literature on hazards and disasters, the DRREMS is often described through the main methods communities use to protect themselves from disasters. The main methods (or activities) of protecting communities from these phenomena are: Mitigation, Preparedness, Response, and Recovery. Mitigation refers to any action taken to minimize the impact of a potential disaster, while Preparedness refers to specific measures taken before a disaster occurs (Twigg, 2004, p. 2). Mitigation is often closely related to prevention, which refers to proactive measures to reduce the negative impacts of hazards and related disasters. However, since it is unlikely that all causes of a hazard can be proactively eliminated, prevention as a method gives way to mitigation. Although necessary, these steps are sometimes insufficient to enable a community to recover and return to optimal functioning. For this reason, after Response, as a reactive approach to negative impacts, relief and Recovery measures are introduced, which represent a key segment of the reconstruction process, aimed at re-establishing the community's functional capacities and its ability to provide basic services continuously.

1 See more in: Mandić, G. J. & Marković, J. M. (2024). Planovi za vanredne situacije u privatnom sektoru. U: Zbornik radova: Treća memorijalna naučna konferencija „Predrag Marić" (str. 94-106). Univerzitet u Beogradu - Fakultet bezbednosti.

The implementation of prevention and mitigation, preparedness, emergency response, and relief and recovery measures is also known as "disaster management" or "disaster risk reduction", which "aims to prevent new and reduce existing disaster risks and manage residual risks, all of which contribute to strengthening resilience and thereby achieving sustainable development" (UNDRR, 2017a). The term "disaster risk management" is also widely used in the literature, referring to "the implementation of disaster risk reduction policies and strategies to prevent new disaster risks, reduce existing disaster risks and manage residual risks, contributing to strengthening resilience and reducing disaster losses" (UNDRR, 2017b). This is also recognized in our Law, in which the DRREMS is defined as "part of the national security system and represents an integrated form of management and organization of the entities of this system in the implementation of preventive and operational measures and the performance of tasks of protecting and rescuing people and property from the consequences of disasters, including measures for recovery from those consequences" (Law, Art. 10).

Based on the above, we can say that the disaster risk reduction system encompasses a wide range of activities undertaken by various societal actors (each within its own jurisdiction and capabilities), all aimed at reducing the risks of disasters to an acceptable level.[2] Understood in this way, the disaster risk reduction process is increasingly integrated into the daily planning and decision-making processes at the corporate management level. It becomes an integral part of its regular activities across all functions of the corporate security system.

2 The solutions provided for in the Law also support the above. "Disaster risk reduction, among other things, includes: 1) accurate identification, regular assessment and monitoring of disaster risks for the purpose of their control; 2) reducing the impact of factors that cause or increase disaster risks through responsible and appropriate management of the environment, land, water and other natural resources, planned land use and taking appropriate technical and other measures; 3) mitigating harmful consequences based on a more complete understanding of their risks, planning for their prevention and increasing preparedness for response and effective response; 4) rebuilding after a disaster in accordance with the principle of building a better system, which will make infrastructure and society as a whole more resilient to future disasters; 5) investing in disaster prevention and risk reduction through encouraging public and private investment and taking structural and non-structural measures; 6) building a culture of safety and resilience of individuals and communities to disasters; 7) intensive mutual cooperation of all competent institutions at all levels of government, as well as partnership with private and public enterprises, other legal entities, entrepreneurs, civil society organizations and all interested citizens who can contribute to disaster risk reduction; 8) establishment of precise procedures for the exchange of information and experiences of importance for risk reduction and for the efficient provision and receipt of international operational and humanitarian assistance for the purpose of eliminating the consequences of a disaster and the initial reconstruction of affected areas; 9) monitoring climate change and community adaptation to the expected consequences" (Law, Article 11, paragraph 2).

One of the key activities of the DRREMS that permeates all phases of disaster risk management is effective information management. This activity includes the collection, processing, use, exchange, and distribution of information. This aspect is particularly evident in the risk assessment phase, when potential hazards are identified by analyzing historical, statistical, and other relevant data. In addition, the importance of information management is reflected in its role in enabling high-quality inter-sectoral cooperation, since the timely and reliable exchange of information among various actors involved in the risk management system is a prerequisite for making sound decisions and acting effectively across all phases of management.

The importance of the DRREMS is recognized in normative and legal regulation, where its role is defined within the framework of the entire national security system. Namely, the Law (Article 1) stipulates that the DRREMS is "of special interest to the Republic of Serbia and is part of the national security system". Such a legal solution shows that the system is not isolated but rather an important part of the institutional framework that helps prevent risks, mitigate disasters, and manage emergencies effectively. At the same time, its place in the national security system also underscores the system's recognized strategic importance in protecting and preserving societal stability.

3. Corporate security – concept and functions

Corporate security is an important segment of the broader system of private and national security, the functioning of which affects economic, social, and national security. Its importance is reflected in its dual role: on the one hand, protecting one's own values and interests, and on the other, contributing to society and the state's ability to meet its needs. Consequently, corporate security goes beyond the scope of individual organizations and is a significant factor in preserving economic stability and overall social resilience, including resilience to disasters.[3]

Given the multitude of definitions of corporate security, both because the concept is still developing and because of the divergence in the literature, choosing one is not easy. At the highest level of generality, it represents

3 This is also confirmed by the position expressed in the National Security Strategy of the Republic of Serbia (2019), which states that legal entities, entrepreneurs and individuals who perform private security activities, in accordance with the law, constitute the internal security system. In this regard, "the internal security system is a part of the national security system intended for performing tasks that ensure the safety of citizens and property... *implement preventive and operational measures and perform tasks of protecting and rescuing people and property from the consequences of natural disasters and other accidents, including measures to recover from those consequences*."

nothing less than an organization's overall security. Regardless of the organization's nature, any security-related activity falls under the umbrella of corporate security.

For this paper, we highlight the definition that defines corporate security as "a characteristic of a legal entity manifested as a state, process and/or instrument of protection of persons, property and operations (objects of protection) that are protected from all sources, carriers and forms of threat, and which is achieved by the human, material and organizational capacities of that entity" (Mandić, 2020, p. 169). From the above definition, it is clear what is protected – the values of the legal entity (persons, own and entrusted property, including information, and operations); from what – all sources, carriers and forms of threat, both internal and external, and in what way – by using all available resources, namely organizational, material and personnel capacities.

In addition to the diversity in defining the term, there is a significant body of work in the scientific and professional literature on the analysis of the functions and elements of corporate security (Marković, 2025, pp. 96-98). Understanding the functions and elements of corporate security has multiple significances. First of all, it enables the systematization and clearer definition of the role of corporate security within the organization. Furthermore, understanding these aspects contributes to improving the organization's overall security management process through better planning, coordination, and control of all security-related activities. In this way, the integration of corporate security with other organizational functions is also enabled, thereby strengthening overall resilience and ensuring business continuity. By reviewing the literature, we can see all activities of an organization that are of a security nature through the following corporate security functions (Marković, 2025, p. 191):

- workplace safety – employee safety (safety and health at work, protection from violence and mobbing);
- physical and technical protection of persons, property, and business (engaging security officers and implementing technical protection);
- collection, verification, protection, and security of data and information;
- *supervision and control* – proactive action to prevent a harmful event: supervision and control over the operations of certain sectors, process operations in production, warehouse processes (input/output of goods, semi-finished products or raw materials), supervision and control over the implementation of internal regulations;

- internal investigations (conducting internal investigations in the event of a harmful event within the organization);
- fire protection;
- environmental protection;
- *risk assessment, control, and management;*
- *crisis management;*
- *business continuity.*

In addition to the above functions, some organizations also provide others, such as economic security, property insurance, authorized supervision, and control of content placed in the media, all due to the specific activity to which the system or organization belongs (Marković, 2025, p. 191).

Of the previously mentioned, we highlight three corporate security functions that have a direct impact on disaster risk reduction and emergency management, namely risk assessment, control and management, crisis management, and business continuity management. *Risk management* is integral to business. All legal entities with potential disaster risks are required to provide procedures for identifying, assessing, analyzing, and managing key risks. It is a continuous process that consists of developing a strategy, setting goals, and making decisions. The goal of risk management is to minimize rationally possible risks. *Crisis management* encompasses a set of activities aimed at identifying, analyzing, and predicting potential crisis situations, and establishing mechanisms that enable an organization to prevent or effectively deal with a crisis, mitigate its consequences, and return to normal functioning as quickly as possible. *Business continuity management* aims to mitigate the consequences of emergencies and crises, including disasters, that directly or indirectly affect the organization. It includes identifying the risks of business processes being exposed to internal and external threats, quantifying and mitigating their impact, and ensuring rapid and efficient recovery in the event of a disaster (Cabric, 2015, p. 198).

In addition to the above, the *function of supervision and control*, carried out with a proactive aim, is also highlighted here because it enables the timely detection of deficiencies and deviations in the corporate security system. Particular importance is given to verifying compliance with applicable regulations, internal procedures, and plans, as well as to verifying the level of equipment and training for disaster risk management. In this sense, this function enables not only the identification of deficiencies, but also their timely elimination. This reduces the likelihood of unwanted events and mitigates their consequences, but also strengthens the corporate security functions, including the three highlighted above.

4. Legal framework for the disaster risk reduction and emergency management system in the Republic of Serbia

The DRREMS in the Republic of Serbia is regulated by the Law on Disaster Risk Reduction and Emergency Management from 2018. This Law defines subjects of the disaster risk reduction and emergency management system as state administration bodies, autonomous province bodies, and local self-government units, public services, companies, as well as other legal entities whose activities are of importance for this area (Law, Article 13, paragraph 1). In addition to them, organizations whose activities are of particular interest for the development and functioning of the DRREMS are classified as forces of the disaster risk reduction and emergency management system (Law, Article 13, paragraph 3).

The Law stipulates the obligation of legal entities to prepare certain documents, including the Disaster Risk Assessment, the Protection and Rescue Plan, and the Disaster Risk Register (Law, Articles 15-22).[4] The Republic of Serbia, autonomous provinces, local government units, entities of special importance for protection and rescue, as well as companies and other legal entities that carry out certain activities, are obliged to prepare a Disaster Risk Assessment (Law, Article 15). Entities that are obliged to prepare a risk assessment are also obliged to adopt a Protection and Rescue Plan (Law, Article 17). The preparation of the above documents is entrusted to authorized companies and other legal entities (Law, Articles 19-20).

A special obligation relates to the preparation of an Accident Protection Plan, which must be in place for companies and other legal entities that use or may use hazardous substances in their activities in prescribed quantities

4 "The Disaster Risk Register is an interactive, electronic, geographic-information database for the territory of the Republic of Serbia, maintained by the Ministry (of Internal Affairs) in cooperation with the competent state administration bodies, other state bodies and holders of public authority. The Risk Register contains *data of importance for risk management*, including: 1) physical-geographical data on the area affected by the risk; 2) data on the number and structure, as well as exposure and vulnerability of the population that may be affected by the occurrence of a disaster; 3) data on residential buildings and buildings for other purposes, infrastructure and other facilities, their exposure and vulnerability; 4) data on previous disasters and their consequences; 5) description and characteristics of the hazard; 6) other data of importance for risk reduction." (Law, Art. 22, paragraphs 1 and 2). The Disaster Risk Register is established, coordinated and managed by the Ministry of Internal Affairs, while other institutions – subjects of the disaster risk reduction and emergency management system, are obliged to provide the Ministry of Internal Affairs with up-to-date risk data required for the development of the Risk Register. The Republic Geodetic Authority has the role of establishing and maintaining the technical infrastructure for accessing and using data from the Risk Register. See: https://drr.geosrbija.rs/drr/home, accessed: 5 May 2026.

(Law, Articles 64-66). Based on these plans and official records, a Register of Entities Handling Hazardous Substances is formed (Law, Article 67). Also, all legal entities that are part of this system are obliged to submit up-to-date data to the Ministry of Internal Affairs to maintain the Disaster Risk Register (Law, Article 22, paragraph 3), as we mentioned earlier.

The Law specifically recognizes entities of importance for protection and rescue, which include companies and legal entities in the fields of telecommunications, energy and mining, transport, meteorology, hydrology, seismology, nuclear safety, environmental protection, water management, forestry, agriculture, healthcare, social care, veterinary, communal activities, construction, catering and other activities that have resources significant for disaster risk reduction (Law, Article 31). These entities have special legal obligations, but at the same time, every company and legal entity is obliged to implement prevention and risk reduction measures within its scope of activity, participate in protection and rescue activities upon request by the competent authorities, and provide the necessary data (Law, Article 30). In addition, all entities are obliged to provide and maintain means and equipment for personal and mutual protection, as well as to organize employee training (Law, Article 55).

Furthermore, the Law also prescribes special obligations for entities in certain activities (electronic communication networks and information systems and connections) (Law, Article 32), as well as for certain categories of companies, such as those that manage hydroaccumulations, tailings dumps and ash dumps, or are engaged in the production, storage and trade of hazardous substances (Law, Article 97). Special obligations also apply to radio and television stations and mobile telephony operators (Law, Articles 98 and 100).

Another important law for the establishment and functioning of the DRREMS is the Law on Critical Infrastructure from 2018. The Law on Critical Infrastructure recognizes the importance of risk management by requiring critical infrastructure operators to develop security plans, conduct risk analysis, and appoint a liaison officer to coordinate with competent authorities.[5] These solutions are primarily aimed at prevention through threat and vulnerability identification, the planning of risk reduction measures, and

5 The Law on Critical Infrastructure requires each operator to develop a Security Risk Management Plan, a document that establishes risk mitigation measures, defines responsibilities and duties, and procedures for eliminating or mitigating the consequences of security threats identified in the risk analysis, which is an integral part of the plan (Article 8, paragraph 1). However, the aforementioned law does not prescribe specific risk mitigation measures or provide a framework for their definition, leaving each operator to determine them independently based on the identified threats. Such a legal solution may result in the methods of protection being left entirely to the different interpretations and practices of the operators themselves (Radivojević & Marković, 2025, pp. 719-720).

the continuous exchange of information with competent institutions. At the same time, certain overlaps with the planning documents prescribed by the Law on Disaster Risk Reduction and Emergency Management indicate a regulatory inconsistency that may further burden critical infrastructure operators. However, such legal solutions confirm that risk management is a key element of critical infrastructure protection (Radivojević, 2022, pp. 114-117). What is positive about the Law on Critical Infrastructure is that it emphasizes the importance of integrating critical infrastructure into spatial, security, and emergency plans, with a focus on preventive measures and priority actions in crises, thereby encouraging a proactive approach to protection (Radivojević & Marković, 2025, p. 721).

5. The role of corporate security in the disaster risk reduction and emergency management system of the Republic of Serbia

The previous text indicated that corporate security already has functional mechanisms aligned with the concept of integrated risk management (Table 1).

Table 1. Comparative overview of DRREMS phases and separate corporate security functions (Source: Authors)

DRREMS phases	Corporate security functions
Prevention (and Mitigation)	Risk Assessment
Preparedness	(Protection) Planning
Response	Crisis Management
Recovery	Business Continuity

In the prevention phase, the emphasis is on risk assessment, which includes the identification of threats, analysis of the probability of their occurrence and possible consequences, then the categorization of risks (the so-called "triage" for their evaluation), as well as the mapping of critical processes and resources in the organization. Of particular importance is the collection of historical, statistical, and other data. Based on the risk assessment, mitigation activities are undertaken to help prevent or reduce society's vulnerability to the impacts of disasters. The role of corporate security here is primarily proactive because, through strategic planning and organizational policies, it helps reduce the overall level of risk and strengthen the organization's resilience, and, indirectly, the community's resilience.

The preparedness phase involves comprehensive protection planning through the development of various planning documents and procedures. This includes a risk management plan, a protection and rescue plan, a fire protection plan, a plan of safe work measures, a preventive health care plan, a plan for the transport of hazardous materials, and a physical and technical protection plan (security plan)[6] and an information security management plan. In addition, it includes an equipment plan, a training and development plan, a protection and rescue plan, a civil protection plan, an evacuation plan, a crisis communication plan, a plan for operating under special conditions, a chemical accident response plan, and a plan for dealing with natural disasters. This phase also envisages the activation of crisis headquarters, the definition of operational protocols for emergencies, and the development of business continuity, recovery, and damage repair plans, with mandatory analysis following the event. At the same time, preparedness also includes early warning systems for hazards, providing emergency shelter, establishing and maintaining supplies, and all other measures taken to minimize the immediate impact of disasters. Corporate security is an integrative framework that unites all of the above plans and procedures, as well as all activities carried out at the organizational level or in which the organization participates, into a single, coordinated protection system.

The response phase is the part of emergency management that involves immediate action during and immediately after a disaster. It includes the establishment and operational functioning of crisis headquarters, decision-making under conditions of uncertainty, effective management of available resources in real time, and cooperation and coordination with competent state authorities (primarily the competent emergency headquarters and the police) and other relevant actors. The main focus is on saving lives, meeting basic human needs, and preventing further destruction of property and the environment. Some activities in disaster response include search, rescue, assistance, evacuation, sheltering, and medical assistance. In this context, corporate security plays a significant operational role, ensuring the organization's internal capacity to respond effectively in emergencies. Through established procedures, trained personnel, technical protection systems, and other material assets, corporate security contributes to the rapid mobilization of the necessary resources for response, the protection of its employees and property, and the protection of the wider community and the environment. Corporate security engagement ensures an integrated response to disasters within a broader social context.

Finally, the recovery phase aims to ensure business continuity by activating alternative operations and recovery plans, returning the organization to

6 In accordance with the Law on Private Security (Official Gazette of the Republic of Serbia, No. 104-2013, 42/2015 and 87/2018).

regular operations as quickly as possible. In this context, corporate security plays a key role, as it encompasses planning, implementation, and control of measures to preserve critical functions and resources and minimize the harmful consequences of disruptions. Through the development and implementation of business continuity plans, corporate security directly contributes to strengthening the organization's resilience, reducing operational losses, and faster stabilization after emergencies.

By analyzing the relevant provisions of the Law, we can conclude that they largely follow the logic of the disaster management cycle. We will list only some of the solutions prescribed by this Law. The first phase includes disaster risk reduction (Article 3), risk assessment and preventive measures and activities (Article 4, Article 15), and strengthening community resilience (Article 11). The second phase includes the adoption of a strategy (Article 12), the development of disaster risk reduction plans (Article 16), protection and rescue plans (Article 17), including the part relating to the establishment of an early warning system, the development of major accident protection plans (Article 18), the accident protection plans (Articles 64-66), as well as the establishment of emergency headquarters (Article 41) and formation of civil protection units (Article 55, Articles 77-78), maintaining in good condition the necessary means and equipment for personal and mutual protection (Article 55, paragraph 2) and training and capacity-building (Article 101). The third phase, the response phase, relates to the declaration of an emergency (Article 38), the coordination of emergency headquarters (Article 43), and the undertaking of protection and rescue measures (Article 56). Finally, for the recovery phase, we can say that the Law also recognizes the implementation of recovery measures, i.e., reconstruction after a disaster, in accordance with the principle of building a better system.

6. Conclusions

The increasingly numerous and destructive consequences of disasters pose new challenges to society in terms of finding new approaches, primarily in their prevention, and then in reducing harmful consequences, as well as the fastest possible recovery of society. This will necessarily require a holistic approach that includes other social entities, in addition to the actions of state authorities and bodies. The entire logic of disaster risk management is directed toward reducing disaster risks, i.e., taking activities to minimize the impact of potential disasters, as well as taking specific measures and activities before a disaster occurs. After a disaster manifests, a response is necessary in the form of reactive action aimed at reducing negative (threatening) impacts, followed by recovery, i.e., a reconstruction process aimed at re-establishing

society's capacity to perform its basic functions. All of the above clearly indicate the breadth of entities that must be included in the above processes. One of these entities is certain companies and other legal entities (organizations).

All modern organizations (public or private), by developing their own capacities to protect their vital assets (employees, property, business), directly contribute to strengthening the resilience of society against the harmful consequences of disasters. Understood as a business function, corporate security directly contributes to reducing disaster risk and managing emergencies, and is integral to the system of the same name. This is supported by the following functions of corporate security: risk assessment, control and management, crisis management, business continuity, and supervision and control. In the Republic of Serbia, the DRREMS is institutionalized and regulated by the Law. Based on the analysis of the Law, we can conclude that the Law largely follows the classic disaster risk management cycle, which includes prevention, preparation, response, and recovery, and that these phases can be directly linked to the corporate security functions.

7. References

1. Cabric, M. (2015). Corporate security management: Challenges, risks, and strategies. Oxford: Butterworth-Heinemann is an imprint of Elsevier.
2. Fritz, C. E. (1961). "Disaster". In: Merton, R.K. and Nisbet, R.A. (Eds.), Contemporary Social Problems (pp. 651-694). New York: Harcourt, Brace and World.
3. Kapucu, N. (2012). Disaster and emergency management systems in urban areas. Cities, 29 (1), S41–S49. https://doi.org/10.1016/j.cities.2011.11.009.
4. Mandić, G. J. & Marković, J. M. (2024). Planovi za vanredne situacije u privatnom sektoru. U: Zbornik radova: Treća memorijalna naučna konferencija „Predrag Marić" (str. 94-106). Beograd: Univerzitet u Beogradu - Fakultet bezbednosti.
5. Mandić, J. G. (2020). „Korporativna bezbednost – poslovna funkcija pravnog lica". U: V. N. Cvetković (Prir.). Nauke bezbednosti – vrste i oblici (str. 167-182). Beograd: Univerzitet u Beogradu, Fakultet bezbednosti.
6. Marković, J. (2023). "Uloga službenika obezbeđenja u vanrednim situacijama". U: N. Stekić i M. Milošević (Ur.). Zbornik radova: Druga memorijalna naučna konferencija „Predrag Marić" (str. 299-310). Beograd: Univerzitet u Beogradu-Fakultet bezbednosti.

7. Marković, M. J. (2025). Korporativna bezbednost kao element sistema nacionalne bezbednosti u zaštiti kritične infrastrukture Republike Srbije. Doktorska disertacija. Beograd: Univerzitet u Beogradu, Fakultet bezbednosti.
8. Radivojević, N. (2022). Uloga privatnog obezbeđenja u upravljanju rizicima od katastrofa: The role of private security in disaster risk management. Proceedings (Collection of Papers) of the Scientific-Professional Society for Disaster Risk Management (SPS-DRM) and the International Institute for Disaster Research (IDR), 110-120.
9. Radivojević, N., & Marković, J. (2025). Zaštita kritične infrastrukture u Republici Srbiji – aktuelno stanje i mogućnosti daljeg razvoja i unapređenja, Zbornik radova Pravnog fakulteta u Novom Sadu 3, 707-726. https://doi.org/10.5937/zrpfns59-62252
10. Sandoval, V., Voss, M., Flörchinger, V. et al. (2023). Integrated Disaster Risk Management (IDRM): Elements to Advance Its Study and Assessment. Int. J. Disaster Risk Sci. 14, 343–356. https://doi.org/10.1007/s13753-023-00490-1
11. Strategija nacionalne bezbednosti Republike Srbije. (2019). Sl. glasnik RS, broj 94/2019.
12. Twigg, J. (2004). Disaster risk reduction: mitigation and preparedness in development and emergency programming. Overseas Development Institute (ODI).
13. UNISDR (United Nations Office for Disaster Risk Reduction). (2016). Sharing innovations to improve implementation and reporting of the Sendai Framework for disaster risk reduction 2015–2030. Short concept note: Work Stream 3, Working Group 3. UNISDR.
14. United Nations Office for Disaster Risk Reduction (UNDRR). 2017a. The Sendai Framework Terminology on Disaster Risk Reduction. "Disaster risk reduction". Accessed 14 April 2026. https://www.undrr.org/terminology/disaster-risk-reduction.
15. United Nations Office for Disaster Risk Reduction (UNDRR). 2017b. The Sendai Framework Terminology on Disaster Risk Reduction. "Disaster risk management". Accessed 14 April 2026. https://www.undrr.org/terminology/disaster-risk-management.
16. Zakon o kritičnoj infrastrukturi. (2018). Sl. glasnik RS, br. 87/18.
17. Zakon o privatnom obezbeđenju. (2013). Sl. glasnik RS, br. 104/13, 42/15 i 87/18.
18. Zakon o smanjenju rizika od katastrofa i upravljanju vanrednim situacijama. (2018). Sl. glasnik RS, br. 87/2018.