SECURITY RISK MANAGEMENT MATURITY IN CRITICAL INFRASTRUCTURE: THE ROLE OF INSTITUTIONAL KNOWLEDGE AND ORGANIZATIONAL SIZE

DOI: https://doi.org/10.37458/nstf.27.2.8
Original Scientific Paper
Received: September 24, 2026
Accepted: November 19, 2026

Ivana Pokrajčić*

Abstract: This article examines the maturity of security risk management in organizations that operate within national critical infrastructure sectors of the Republic of Croatia. The research focuses on whether organizational size and institutional knowledge are associated with differences in risk management maturity. Data

* Ivana Pokrajčić, PhD, Croatian Military Academy, Zagreb, Croatia, email: ivpokrajcic@gmail.com, https://orcid.org/0009-0001-2223-9122

were collected through a survey of medium and large organizations. Methodology included descriptive and inferential statistical methods, Kolmogorov–Smirnov test, independent-samples t-tests, and correlation analysis. The results indicate significant differences in risk management maturity across the sectors. Large organizations have higher maturity scores than medium organizations. The results suggest that institutional knowledge and size have an important role in the development of mature risk management practices and may support the resilience and continuity of critical infrastructure services. The research contributes empirical evidence on risk management within Croatian critical infrastructure, an area that currently has very limited scholarly attention.

Keywords: risk management maturity, critical infrastructure, institutional knowledge, organizational size, resilience

.

Introduction

Risk management in critical infrastructure has been traditionally focused on the identification and mitigation of very specific and narrow range of threats, such as physical damage, theft, operational disruptions, and cyber incidents. However, organizations responsible for essential services increasingly operate in environments characterized by technological dependence, sectoral interconnection, and the possibility that a disruption in one system may affect others and as Hemme (2015) and Macaulay (2019) argue, cause a cascade effect. Today it is evident that risk management cannot be understood solely as a technical or compliance related activity as it was in the past. The effectiveness of risk management today depends on how organizations acquire and retain

knowledge, organize responsibilities, assess their vulnerabilities, and incorporate risk related information into their own decision-making processes (Asbury & Jacobs, 2014; Amaya et al., 2015). From an organizational perspective, the maturity of risk management shows the extent to which the above-mentioned activities are implemented in their regular organizational processes. More mature systems are characterized by formalized procedures, systematic risk assessment, knowledge sharing mechanisms, continuous and systematic monitoring, and the integration of risk related information into decision making processes (Pokrajcic, 2025). Such capabilities may affect not only an organization's ability to respond to individual security incidents but also its capabilities to maintain business continuity under conditions of uncertainty and disruption.

This issue is particularly relevant for critical infrastructure. It is widely agreed upon that its functioning is essential for economic activity, public services, and broader societal stability. In Croatia, the importance of these systems is formally recognized in the Law on Critical Infrastructure (NN 56/13, NN 114/22, NN 89/25), which defines critical infrastructure as assets, networks, and services whose disruption may have significant consequences for national security, economic activity, and the functioning of society. Organizations operating within defined critical infrastructure sectors face risks whose consequences may extend beyond the individual organization and affect other sectors and public services, and cause a phenomenon known as cascade effect.

Existing academic research has addressed numerous aspects of security and risk management, including the physical protection of infrastructure and personnel (Nunes-Vaz & Lor, 2014; Fennelly, 2016; Lichte et al., 2021), business disruptions (Fennelly, 2016), information and cybersecurity risks (Wangen et al., 2018; Berry & Berry, 2018; Alahmari & Duncan, 2020), personal data protection, and risks associated with the increasing use of artificial intelligence in organizational processes (Villegas-Ch & Garcia-Ortiz, 2023). Although this research provides important insights into particular categories of risk, empirical research examining the maturity of security risk management within critical infrastructure organizations is very limited (Tweneboah-Koduah & Buchanan, 2018; Ayeni & Oluwagbenga, 2025).

An important question which this article addresses are factors which contribute to differences in risk management maturity (RMM) between organizations of different size, as well as the differences between organizations which belong to different critical infrastructure sectors. These factors, among others, are organizational scale and institutional knowledge. Organizational scale may influence the availability of financial and human resources, the degree of formalization, and the capacity to establish specialized functions and processes with the organization itself. Contemporary theories of risk management argue that institutional knowledge is considered to be an important factor because risk management depends on an organization's ability to collect, document, interpret, implement and share information concerning risks and their potential consequences. Despite the widely recognized importance of these factors, there is limited

empirical evidence on how are actually organizational scale and institutional knowledge associated with the maturity of security risk management in organizations (Pokrajcic, 2025). This article addresses this gap by examining the maturity of security risk management processes in organizations from national critical infrastructure sectors of the Republic of Croatia. The analysis focuses on three questions: does risk management maturity differ across sectors, do larger organizations demonstrate higher levels of maturity than medium organizations, and is institutional knowledge associated with more developed security risk management practices?

Using primary data, this article examines risk management maturity in organizations which operate within the sectors of national critical infrastructure of Republic of Croatia through five dimensions: institutional knowledge of security risks, risk identification and assessment, risk response, monitoring, and cooperation. By examining these dimensions together, the research provides empirical evidence on how organizational characteristics are associated with the level of maturity of security risk management. The research contributes to the literature in two ways. First, it provides empirical evidence from the organizations which operate within Croatian critical infrastructure sectors, where research in general is very scarce. Second, it approaches security risk management maturity not only as a technical capability but also as an organizational and governance topic which is shaped by institutional knowledge, organizational resources, formalized procedures, and cooperation between relevant actors. The findings are relevant both for organizations responsible for maintaining their business

CC BY NC ND

continuity, and for public authorities which are responsible for the governance and overall resilience of national critical infrastructure.

Theoretical Background

Security Risk Management in Critical Infrastructure

Security risk management in critical infrastructure cannot be considered solely as an internal organizational activity. Organizations operating critical infrastructure provide services and functions whose disruption may affect economic activity of the country, public services, and also affect other interconnected sectors (For example, a disruption in energy sector can greatly affect the functioning of all other sectors). For this reason, weaknesses in the identification, assessment, or management of security risks may produce consequences that extend beyond the individual organization.

Traditional approaches to security risk management have frequently concentrated on specific categories of threats, such as physical damage, theft, operational disruption, and cyber incidents. Existing research has been mainly conducted in specialized areas, such as physical security (Nunes-Vaz et al. 2011; Fennelly, 2016; Lichte et al., 2021), information and cybersecurity risks (Wangen et al., 2018; Berry & Berry, 2018; Alahmari & Duncan, 2020), and the protection of information and personal data (Villegas-CH & Garcia-Ortiz, 2023). Although these areas differ in terms of the threats they address, they are valuable because organizations must consider them within broader risk management practices.

The contemporary integration of security-related risks into enterprise-wide risk management frameworks reflects this development (Marotta & McShane, 2018). Rather than treating security incidents as isolated operational problems, an integrated approach should connect security risks with organizational objectives, resource allocation, decision-making, and business continuity. This is particularly important in critical infrastructure, where the consequences of disruption may involve multiple organizations and sectors.

Interdependencies between infrastructure sectors further complicate security risk management. Research on critical infrastructure consistently highlights sectoral interdependence as a source of systemic vulnerability. Disruptions in one sector may produce cascading effects in others, particularly when critical services depend on shared infrastructures (Hemme, 2015; Macaulay, 2019). Such conditions require organizations to consider not only individual threats but also the relationships between risks, organizational processes, and external actors.

The increasing integration of digital technologies adds another dimension to this problem. Cyber vulnerabilities may have consequences beyond information systems when digital systems support physical infrastructure and essential services. The integration of cyber and physical risk assessment has become increasingly important in critical infrastructure environments, where vulnerabilities may propagate across interconnected systems. The management of security risks requires organizations to establish procedures for identifying risks, assessing their potential consequences, responding to incidents, monitoring relevant indicators, and exchanging information with relevant internal and

external actors. These activities correspond to the main dimensions examined in this article. The level at which they are systematically developed and integrated into organizational processes provides an indication of the maturity of security risk management.

Risk Management Maturity as an Organizational Capability

Risk management maturity refers to the extent to which risk-related activities are systematically developed, formally established, implemented into the business processes, and integrated into organizational decision-making and governance. At lower levels of maturity, risk management tends to be reactive, fragmented, and dependent on individual knowledge or reactive responses to particular incidents. At higher levels, organizations establish formal procedures, conduct systematic assessments, monitor risks, and use risk-related information as part of regular management processes, aiming to predict and prevent risks.

Maturity models commonly describe this development as a progression from informal and reactive practices toward more structured and integrated preventive approaches (Hillson, 2017). Risk resilient organizations which better developed risk management capabilities, have a systematic risk identification procedure, internal responsibilities are more clearly defined, and risk-related information is relevant to managerial and strategic decision-making (Fraser & Simkins, 2010). Most of current approaches to risk management also include continuous risk monitoring, scenario analysis, and the use of information to support organizational adaptation (Aven, 2016).

The value of risk maturity models is in their ability to assess several interconnected aspects of organizational capability rather than focusing on a single procedure or only on a technical aspect. Risk maturity models have been successfully applied in different organizational contexts, and their effectiveness has been empirically tested. Some of the most prominent researches were performed in the construction (& Kishk, 2017), maritime administration (Laine et al., 2024), legal and institutional settings (Unger et al., 2015), and corporate risk management (Oliva, 2016). The purpose of the research was not only to determine the current level of implementation but also to identify areas in which organizational practices require further development (Tubis & Werbińska-Wojciechowska, 2021), and the results obtained from the existing research is implemented into the research presented in this article.

Based on the above, in this article, security risk management maturity is assessed through five dimensions: institutional knowledge of security risks, security risk identification and assessment, security risk response, security risk monitoring, and cooperation and information exchange with relevant actors. When assessed together, these dimensions provide insights into whether security risk management within an organization is based primarily on informal and isolated practices or whether it has become a systematic part of organizational processes. For it to become a systematic part of organizational processes, the institutional knowledge must be shared and implemented across all business processes. From this perspective, it can be said that risk management maturity is an organizational capability, and that its development depends not only on the existence of formal procedures but also on the

knowledge available within the organization, the ability to identify and assess risks, the capacity to implement detective, preventive and responsive measures, the use of monitoring mechanisms, and cooperation with relevant actors.

Institutional Knowledge and Security Risk Management Maturity

Institutional knowledge represents an important component of organizational risk management because security and risk related decisions depend on the availability and use of information concerning threats, vulnerabilities, previous incidents, and their potential consequences. In the past, organizations may have possessed such knowledge only through the knowledge, experience and education of their employees, but today, and specifically when belonging to critical infrastctructure, they are obligated to develop strong formal mechanisms for documenting, updating, sharing (internally and with other actors), and reporting the authorities on risk-related information. Current literature shows that the difference between these approaches is particularly relevant to the development of mature risk management systems. In the organizations where knowledge remains primarily dependent on individual employees, those organizations may face difficulties when experienced personnel leave or when information is not transferred across organizational units. Formalized knowledge systems, by contrast, enable organizations to retain information and make it available for future risk assessments and decision-making (Zou et al., 2010). Zou et al. (2010) emphasize the importance of organizational knowledge and learning in the development of risk management capability. Risk management therefore

CC BY NC ND

involves more than the application of analytical tools. Organizations must also be able to collect information from internal and external sources (including international cooperation), interpret previous events, and incorporate relevant knowledge into their future assessments and procedures.

In the context of security risk management, institutional knowledge supports other dimensions of risk management maturity as well. Gathered information about previous incidents and vulnerabilities can improve future risk identification and assessment. Also, knowledge of potential consequences may contribute to the development of preventive measures and response and risk mitigation scenarios. The systematic exchange of information can improve cooperation between organizational units and external actors, such as other similar organizations within the critical infrastructure sector, interdependent organizations from other sectors, partners, and most importantly governing organizations making the entire system of critical infrastructure more risk resilient. Therefore, organizations with more developed institutional knowledge are expected to demonstrate higher levels of security risk management maturity. This relationship is examined empirically through the third hypothesis of the research presented in this article.

Organizational Scale and Security Risk Management Maturity

One of the assumptions this article considers is that organizational scale may also influence the development of security risk management practices. Larger organizations generally operate through more developed

organizational structures and may have greater access to more financial resources, specialized trained personnel, and better established formal administrative procedures. It is also the case that large organizations can afford outsourcing risk management to specialized partners. These characteristics generally facilitate the establishment of dedicated functions and processes for managing security risks.

Medium organizations may face different organizational conditions and challenges when it comes to risk management. Risk management responsibilities may be a focus of a smaller number of individuals, and specialized security functions may not always be formally established. This does not necessarily mean that smaller organizations are unable to manage risks effectively, but differences in available resources and organizational structure may influence the extent to which risk management practices are integrated into organizational processes.

The relevance of organizational resources is also reflected in the existing literature on risk management maturity. Mature systems require more than just awareness of potential risks. They regularly perform assessments, documentation, monitoring, coordination, and the implementation of preventive and corrective measures. The development and maintenance of these activities required administrative capacity and the allocation of organizational resources (personnel and financial). Organizational scale may therefore be associated with differences in the maturity of security risk management. Large organizations are expected to have greater capacity to establish formal procedures and maintain specialized tehnical systems, while medium

CC BY NC ND

organizations generally rely more heavily on informal arrangements or a smaller number of responsible individuals. This relationship is examined through the second hypothesis of the research.

Sectoral Differences and Security Risk Management Maturity

Organizations operating in different critical infrastructure sectors do not necessarily face the same risk environment. The nature of essential services, technological dependence of their business processes, organizational structures, regulatory requirements, and relationships with other actors between sectors can be significantly different. These differences may influence how organizations identify and manage security risks.

Research on critical infrastructure emphasizes the diversity and interdependence of critical infrastructure systems. Baker et al. (2022) identify natural hazards, human-induced threats, and technical failures as important categories of risk affecting critical infrastructure. At the same time, sectoral interdependencies may increase the consequences of individual incidents, particularly where disruptions affect services on which other sectors depend (Hemme, 2015; Macaulay, 2019).

Differences between sectors may also influence the organizational arrangements through which risks are managed. Some sectors may operate within highly formalized regulatory environments, while others may have different organizational structures or patterns of interaction with public authorities and private partners. The technological characteristics of a sector may also

influence the types of threats that organizations prioritize and the business procedures developed to manage them.

These differences provide a theoretical basis for examining whether security risk management maturity varies between companies operating in different sectors of national critical infrastructure. The first hypothesis therefore tests whether the differences in the maturity of security risk management processes across the different sectors of critical infrastructure of Croatia which were included in the research.

Table 1. Weighing Factors for the Calculation of RMM

	1		2	
Aspect	Weigh	Maturity level	Weigh	Maturity level
Institutional Knowledge	0.2	3	0.1	3
Identification and assessment	0.3	3	0.3	3
Risk Response	0.3	2	0.3	2
Risk Monitoring	0.2	3	0.1	3
Cooperation with actors	-	-	0.2	1
Overal Indicator	2.7		2.3	

Source: Author according to: Tubis & Werbinska-Wojciechowska (2021:14)

CC BY NC ND

Based on the model developed by Tubis and & Werbinska-Wojciechowska (2021:14), predefined weighting factors (Table 1) are assigned to each dimension. These factors reflect the relative importance of individual components within the overall risk management framework. The aggregated maturity score is derived as a weighted sum of performance across all domains, providing a composite indicator of organizational capability in managing security related risks. The model was contextualized to capture the specific operational dynamics of critical infrastructure, particularly concerning cyber-physical threats and crisis management responses. The framework incorporates five primary dimensions: VAR1 – Institutional Knowledge, VAR2 – Risk Identification and Assessment, VAR3 – Risk Response, VAR4 – Risk Monitoring, and VAR5 – Cooperation with actors. The weighting scheme assigned to each dimension within the overall Security Risk Management (RMM) maturity index aligns with the baseline methodology of the original authors and core tenets of business continuity standards (ISO 31000 / ISO 22301). The highest relative weights were allocated to risk assessment, risk response, and institutional knowledge (25% each), as these pillars directly underpin an organization's operational resilience.

The remaining dimensions, monitoring and stakeholder cooperation, were assigned weights of 12.5% each in the composite index. The psychometric properties of the measurement instrument were evaluated through internal consistency and construct validity analyses. Internal consistency across all subscales exceeded the standard threshold of $\alpha=0.70$ (Cronbach's alpha for the VAR1 scale was 0.84, while the overall SRM instrument

CC BY NC ND

yielded α=0.91). Convergent validity was established via the average variance extracted (AVE > 0.50 across all constructs).

Hypothesis development and methodology

Based on the findings of previous studies and considering the interdependencies among the sectors of national critical infrastructure, as well as the potential for cascading effects as discussed by Hemme (2015) and Macaulay (2019), this research investigates the maturity of risk management processes in companies within the national critical infrastructure sectors. The following hypotheses have been formulated:

H1: Significant differences exist in the maturity level of security risk management processes across the sectors of national critical infrastructure in the Republic of Croatia.

H2: The maturity of security risk management processes is higher in large organizations compared to medium organizations which belong to the national critical infrastructure sectors of the Republic of Croatia.

H3: Companies with better institutional knowledge of security risks exhibit a higher maturity level in their security risk management processes.

Research Design and Sample

This research draws upon the primary empirical dataset gathered during broader doctoral research (Pokrajčić, 2025) and builds upon preliminary descriptive observations reported in Pokrajčić and Lazibat (2025). While Pokrajčić and Lazibat (2025) focused primarily on general determinants of risk management, the distinct scientific contribution of this study lies in its granular

examination of the interaction between institutional knowledge (VAR1) and organizational size on overall SRM maturity. Furthermore, it offers a cross-sectoral comparative analysis of critical infrastructure organizations in the context of recent regulatory shifts (the EU NIS2 Directive and the Croatian Critical Infrastructure Act). The statistical modeling and analytical framework presented herein have not been published previously.

The research is based on primary data collected through a structured questionnaire distributed electronically to target population. The target population were organizations which, according to the National Classification of Economic Activities (NKD), operate within the sectors of national critical infrastructure of the Republic of Croatia. The sampling frame was constructed using the Digital Chamber database of the Croatian Chamber of Economy (HGK) and the info.BIZ database of the Financial Agency (FINA).

A stratified sampling approach was employed, with two strata established according to organizational size: mediums and large organizations. The research focused on medium and large organizations because organizational size was taken as one one of the variables examined in relation to the maturity of security risk management. The research ultimately obtained 125 valid responses from the 330 organizations included in the research sample. Although 126 participants initially accessed the questionnaire, one response was excluded because the participant did not provide answers to any of the items measuring the variables relevant to the research questions. Consequently, 125 responses were retained for further statistical analysis. Regarding organizational

size, the final sample included 70 respondents from large organizations and 53 from medium organizations, and the organizational size of two respondents was not specified. The questionnaire was sent to members of top management and individuals responsible for security related activities or security risk management within their organizations. Participants were selected on the assumption that their professional responsibilities and organizational positions enabled them to provide information about internal security risk management practices, relevant procedures, and organizational arrangements.

Data Analysis

Descriptive statistical analysis was conducted to examine the distribution and central tendency of the collected data. The analysis included arithmetic means, standard deviations, medians, minimum and maximum values, and interquartile ranges. The distribution of the overall security risk management maturity score was examined with Kolmogorov–Smirnov test. Because the distribution significantly deviated from normality, measures such as the median and interquartile range were also used to describe the central tendency and dispersion of the results.

The first hypothesis examined whether security risk management maturity differed significantly across different sectors of national critical infrastructure. The second hypothesis examined differences in security risk management maturity between medium and large organizations. An independent samples t-test was used to compare the arithmetic means of the two groups. Prior to conducting the analysis, homogeneity of variances

was assessed using Levene's test. Where the assumption of equal variances was violated, the corresponding correction for unequal variances was applied.

The third hypothesis examined the relationship between institutional knowledge of security risks and the overall maturity of security risk management. Pearson's correlation coefficient was used to examine the relationship between institutional knowledge and security risk management maturity.

Table 2. Overview of the research variables and their measurement methods

Security Risks Management (SRM) The variable will be measured using statements from validated scales, Tubis and Werbińska-Wojciechowska (2021).
VAR1- Institutional Knowledge of Security Risks
VAR2 - Security risk identification and assessment
VAR3 - Security Risk Response
VAR4 - Security Risk Monitoring
VAR5 - Cooperation

Source: Author

Research Results

Table 3 shows the distribution of participants based on organization size and sector. The largest pnumber of participants came from the food sector (32,0%), followed by energy (19,2%), transport (14,4%), water management (12,8%), and communication and information (12,0%). The finance, health, and public services sectors were represented by smaller numbers of participants. One participant answered that their

organization belongs to the public services sector, although this sector was not originally included in the research population, and his response was not included in the analysis.

Table 3. The distribution of participants based on the size and sector of the organization.

	n	%
Size		
Medium (> 50, <250 employees)	53	42.4
Large (> 250 employees)	70	56.0
I am not sure	2	1.6
Sector		
Food	40	32.0
Energy	24	19.2
Transport	18	14.4
Water management	16	12.8
Communication and Information	15	12.0
Finance	6	4.8
Health	4	3.2
Public Services	1	0.8

Source: Author

The professional roles of participants are presented in Table 4. The largest group consisted of members of high management or supervisory boards (36.8%), followed by heads of security units (27.2%). Employees responsible for the implementation of security measures accounted for 16.8% of the sample, while security

consultants represented 13.6%. The remaining 5.6% selected the category "None of the above."

Table 4. Distribution of Research Participants According to Their Role in the Company

	n	%
I am a member of the Management Board or Supervisory Board and I am familiar with all regulations and standards, as well as the internal security management processes within my company.	46	36.8
I am the head of the security unit and I am familiar with all regulations and standards related to business security, as well as overseeing the implementation of business processes related to business security.	34	27.2
I am a security consultant and I am actively involved in all decision-making processes related to business security and their implementation.	17	13.6
I am an employee of the company responsible for tasks related to the implementation of security measures in business operations.	21	16.8
None of the above	7	5.6

Source: Author

The overall result of security risk management maturity was determined by evaluating the five aspects of risk management, with each aspect weighted (as shown in Table 1, Option 2). These weighted results were then summed to calculate the total score. The distribution of the results is displayed in Graph 1. The results ranged from 1 to 5, with a mean score of 3.33 and a standard deviation of 1.35, as presented in Table 5. This provides an indication of the maturity level of security risk management within the observed sample.

Table 5. Security Risks Management Maturity - overall result

	M	*SD*	*t(ss)*	*K-S*	*p*	*C*	*IQR*
SRM	3.33	1.35	125	0.12	< 0.001	3.50	2.00-4.75

Source: Author

However, the distribution of the results was skewed towards higher values and statistically significantly deviated from a normal distribution, as indicated by the Kolmogorov-Smirnov test ($z = 0.12$, $ss = 125$, $p < 0.001$). Therefore, the measures of central tendency were determined using both the median and the interquartile range. The median was 3.50, and the interquartile range spanned from 2.00 to 4.75.

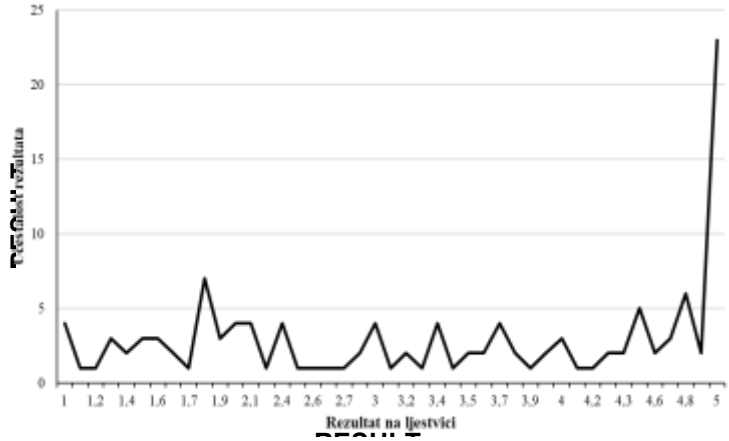


Figure 1. Frequency of each total score on the scale designed for measuring security risk management, Source: Author

According to Tubis and Werbinska-Wojciechowska (2021), risk management maturity models relate to the concepts of company risk management and are based on general business assumptions implemented at the

corporate management level. By measuring factors related to institutional knowledge in medium and large organizations, it was found that 20% of participants believe there is a lack of knowledge about security risks and their potential consequences in their organizations, while 35.2% indicated the highest level of knowledge about security risks in their organization (Table 6).

Table 6. VAR1 - Institutional knowledge of security risks

	Maturity level 1	**Maturity level 2**	**Maturity level 3**	**Maturity level 4**	**Maturity level 5**
n	25	16	21	19	44
%	20	12.8	16.8	15.2	35.2

Source: Author

The identification and assessment of security risks is the second dimension in the model used to assess the maturity of security risk management. A total of 24% of respondents indicate that risks are assessed using qualitative tools and that the results are communicated only to the company's management. A significant number of respondents (31.2%) report that risk assessments are based on expert evaluations by responsible individuals, and that the results of the analysis are communicated to all areas of the company's operations, which corresponds to the highest level of process maturity (Table 7).

Table 7. VAR2 - Identification and assessment of security risks

	Maturity level 1	Maturity level 2	Maturity level 3	Maturity level 4	Maturity level 5
n	10	30	18	28	39
%	8	24	14.4	22.4	31.2

Source: Author

The third dimension which was assessed investigated how organizations respond to identified security risks and the extent to which risk assessments are incorporated into business processes and preventive planning. As shown in Table 8, he highest level of maturity was reported by 30.4%. These organizations used the results of risk assessments as a basis for planning business processes, have developed preventive measures for protecting critical processes, and have prepared scenarios for managing the consequences of security incidents, but these practices were not equally established throughout the sample.

Table 8. VAR3 -Security Risks Response

	Maturity level 1	Maturity level 2	Maturity level 3	Maturity level 4	Maturity level 5
n	10	32	15	30	38
%	8	25.6	12	24	30.4

Source: Author

The fourth dimension examined the use of indicators to monitor the effectiveness and efficiency of business processes and their compliance with security procedures.

The results show that 28% of participants reported that their organization has implemented a comprehensive system of indicators used to monitor the efficiency of business processes and their compliance with security procedures. On the other hand, 11.2% of companies have not developed a system of indicators for monitoring the effectiveness and efficiency of business processes (Table 9).

Table 9. VAR4 - Security risk monitoring

	Maturity level 1	**Maturity level 2**	**Maturity level 3**	**Maturity level 4**	**Maturity level 5**
n	14	28	23	25	35
%	11.2	22.4	18.4	20	28

Source: Author

Cooperation within the company, as well as the exchange of data on security risks with partners, is an indicator of a high level of security risk management maturity, which was detected in 23.2% of companies. Lower levels of collaboration, indicating a complete or significant lack of communication about security risks within the company, were detected in 43.2% of companies (Table 10). This result is significant in the context of the issues discussed in this article and will be further explained and elaborated in the discussion of the research results.

Table 10. VAR5 - Cooperation

	Maturity level 1	**Maturity level 2**	**Maturity level 3**	**Maturity level 4**	**Maturity level 5**
n	26	28	18	24	29
%	20.8	22.4	14.4	19.2	23.2

Source: Author

In order to confirm or refute Hypothesis 1, a statistical analysis of the data collected from the survey was conducted, and the averages of security risk management maturity were calculated by sectors of the national critical infrastructure (Table 11).

Table 11. Arithmetic means of security risk management maturity by sectors of NCI.

	Energy	Communication and Information	Transport	Health	Water Management	Food	Finance
N	24	15	18	4	16	40	6
SRM	3.47	4.31	3.46	2.47	2.08	3.30	4.32
SD	0.53	0.51	1.01	0.89	0.91	0.70	0.44

Source: Author

To examine the interrelationships between the investigated variables, correlation coefficients were determined. Statistically significant correlations were

found between all the investigated variables, as shown in Table 12.

Table 12. Interrelationship Between Constructs Expressed Through Pearson's Correlation Coefficient Across the Entire Sample

	SRM	SRM1	SRM2	SRM3	SRM4	SRM5
SRM	-					
VAR1	0.93	-				
VAR2	0.97	0.90	-			
VAR3	0.96	0.88	0.92	-		
VAR4	0.94	0.85	0.90	0.90	-	
VAR5	0.97	0.90	0.92	0.90	0.89	-

Note: All correlation coefficients are significant at the statistical significance level of $p < 0.001$.
Source: Author

Statistical data analysis was conducted to differentiate between medium and large companies, with the goal of gaining insight into the differences between these two groups, and the results are presented in Table 13.

Table 13. Arithmetic Means of Constructs Divided by Medium and Large Organizations

	M		L			
	M	*SD*	*M*	*SD*	*t(ss)*	*p*
SRM	2.24	1.03	4.18	0.91	-11.13(121)	< 0.001

Source: Author

The relationships between the constructs of the model, expressed through Pearson's correlation coefficient for medium and large companies, are presented in Table 14 and Table 15. The findings provide insight into which specific variables or aspects of security risk management differ significantly between medium and large companies, which may be useful for further analysis or strategic decision-making within these types of companies.

Table 14. Interrelationship between Constructs Expressed Through Pearson's Correlation Coefficient for Medium Companies

	SRM	VAR1	VAR2	VAR3	VAR4	VAR5
SRM	-					
VAR1	0.83	-				
VAR2	0.91	0.76	-			
VAR3	0.92	0.78	0.83	-		
VAR4	0.80	0.66	0.72	0.73	-	
VAR5	0.89	0.78	0,.83	0.77	0.64	-

Note: All correlation coefficients are significant at the statistical significance level of $p < 0.001$.
Source: Author

Table 15. Interrelationship between Constructs Expressed Through Pearson's Correlation Coefficient for Large Companies

	SRM	VAR1	VAR2	VAR3	VAR4	VAR5
SRM	-					
VAR1	0.84	-				
VAR2	0.91	0.81	-			
VAR3	0.90	0.78	0.81	-		
VAR4	0.91	0.80	0.84	0.82	-	
VAR5	0.93	0.78	0.82	0.78	0.85	-

Note: All correlation coefficients are significant at the statistical significance level of $p < 0.001$.
Source: Author

Discussion

A primary insight from this research is the influence of organizational size and institutional knowledge on SRM maturity. Large organizations demonstrated significantly higher maturity levels ($t=-11.13$, $p<0.001$, $t=-11.13$, $p<0.001$), supporting the hypothesis that scale enables more advanced risk management practices. This advantage may be the result of greater financial and human resources, specialized security personnel, and formalized operational procedures. On the other hand, medium organizations most likely due to resource and personnel constraints, operate on a more reactive basis, relying on individual employee expertise rather than formalized institutional protocols. Descriptive variations across critical infrastructure sectors further highlight the

impact of regulatory context. Cross-sectoral comparison reveals that the financial and energy sectors achieve higher average maturity scores (4.31 and 3.47) than water management and food supply. The reason behind this difference is the fact that financial institutions and telecommunications operators have long been subject to strict compliance frameworks (e.g., DORA, ISO 27001, and sector-specific central bank regulations), which have forced them to formalize their SRM architectures over time. In contrast, sectors such as health, water supply, and food management have so far faced less such formalised requirements. Another dimension that requires attention is stakeholder cooperation and information exchange (VAR5). A significant number of surveyed organizations (43.2%) has shown low maturity in this dimension. This result shows a hesitation to share vulnerability information with others, possibly due to a fear of reputational damage. Primary reason of this hesitation could be the concern over possible reputational damage if the information was shared with clients, partners or competitors. As highlighted by Alahmari and Duncan (2020), critical infrastructure operators often hesitate to disclose security incidents or operational vulnerabilities to government bodies or industry peers unless explicitly mandated by law. These findings carry significant practical and policy implications for strengthening security risk management across national critical infrastructure. To address structural resource constraints, particularly within medium organizations, public authorities should develop standardized risk assessment toolkits, tailored implementation templates, and sector-specific technical guidance. Furthermore, regulatory frameworks should not only encourage but formally prescribe information

CC BY NC ND

sharing about risks, to avoid cascade effects of possible incidents between the sectors of critical infrastructure which are interconnected.

Conclusion

This article examined the maturity of security risk management in organizations which belong to sectors of national critical infrastructure in the Republic of Croatia. The analysis covered five variables: institutional knowledge, risk identification and assessment, risk response, monitoring, and cooperation and information exchange. The results show differences in the level of security risk management maturity among the organizations included in the research. Descriptive differences were also observed between different sectors. The highest average results are in the finance and communication and information sectors, while the lowest averages were found in the health and water management sectors. A clearer difference was found between medium and large organizations. Large organizations achieved significantly higher maturity levels, supporting the hypothesis that organizational size is associated with more developed security risk management practice. This may be related to greater resources, better trained personnel, and more formalized organizational procedures, although these factors were not directly examined in this research. Institutional knowledge was strongly associated with overall security risk management maturity. Organizations with more developed practices for collecting, implementing and sharing institutional knowledge about security risks reported better developed risk management practices. The results show that security risk management maturity is not based on a single procedure or capability. It

depends on the development of all the interconnected processes which were tested in this research. The research presented in this article has several limitations. First, the number of participant that belong to each sector were different, that is, some sectors were represented by a relatively small number of participants, and the research relied on self reported assessments, which may have been subjective. Future research could therefore use larger and more balanced samples and combine survey data with interviews or other forms of organizational evidence, such as business results, number of security related incidents, etc. Despite these limitations, the research gives insight into the development of security risk management practices in Croatian critical infrastructure. The results suggest that organizations do not all operate at the same level of maturity and that organizational characteristics, particularly organizational size and institutional knowledge, are relevant when examining how security risk management practices are implemented and followed. These findings may help both organizztions within critical infrastructure and public authorities identify and focus on specific areas to improve their security risk management processes.

Literature:

1. Alahmari, A. & Duncan, Bob. (2020). Cybersecurity Risk Management in Small and Medium-Sized Companies: A Systematic Review of Recent Evidence. 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, 15-19 June 2020, 1-5.
2. Alijoyo, F. A., Bonita, I., & Sirait, K. B. (2021). The Risk Management Maturity Assessment: The case of an Indonesian fintech firm. Proceedings of the 4th International Conference on Research in Management and Economics.

3. Amaya, D., Gauthier, G., & Léautier, T. O. (2015). Dynamic risk management: Investment, capital structure, and hedging in the presence of financial frictions. Journal of Risk and Insurance, 82(2), 359–399
4. Asbury, S., & Jacobs, E. (2014). Dynamic risk assessment: The practical guide to making risk-based decisions with the 3-level risk management model. Routledge.
5. Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research, 253(1), 1–13.
6. Ayeni, G. O., & Oluwagbenga, T. A. (2025). Evaluating and enhancing resilience in critical infrastructure: Strategies for risk management. International Journal for Information Security Research, 14(1), 1093-1100.
7. Baker, M., Bearse, R., Mey, R., Evans, C. V., Anderson, C., Baker, M., & Biçakci, S. (2022). Physical threats to critical infrastructure. In Enabling NATO's collective defense: Critical infrastructure security and resiliency. Strategic Studies Institute, US Army War College. http://www.jstor.org/stable/resrep44875.7 Resiliency (NATO COE-DAT Handbook 1). Strategic Studies Institute, US Army War College.
8. Barker, K., Bessarabova, E., Radhakrishnan, S., González, A. D., Weber, M. S., Marquez, J. E. R., Vorobeychik, Y., & Jiang, J. N. (2025). Risk analysis of disinformation weaponized against critical networks. Risk Analysis, 45, 4088–4096. https://doi.org/10.1111/risa.70062.
9. Berry C.T. & Berry, R.L. (2018). An initial assessment of small business risk management approaches for cyber security threats, International Journal of Business Continuity and Risk Management, 8(1), 1–10.
10. Fennelly, Lawrence J. (2016). Effective physical security. Butterworth-Heinemann.
11. Fraser, J., & Simkins, B. J. (Eds.). (2010). Enterprise risk management: Today's leading research and best practices for tomorrow's executives. John Wiley & Sons.
12. Fraser, J.R.S. (2013). Message from the chair on introducing company risk management (ERM) to a company, International Journal of Disclosure and Governance, 10 (2), 98–104.
13. Hemme, K. (2015). Critical infrastructure protection: Maintenance is national security. Journal of Strategic Security, 8(3), 25-39. http://dx.doi.org/10.5038/1944-0472.8.3S.1471.

14. Hillson, D., & Murray-Webster, R. (2017). Razumijevanje i upravljanje stavom prema riziku. Routledge.
15. Laine, J., Valdez Banda, O. A., & Goerlandt, F. (2024). A Delphi matrix for identifying safety indicators in maritime transport. WMU Journal of Maritime Affairs, 23, 137–163. https://doi.org/10.1007/s13437-023-00328-z
16. Lichte, D., Witte, D., Termin, T. & Kai-Dietrich,W. (2021). Representing Uncertainty in Physical Security Risk Assessment. European Journal for Security Research, 6, 189–209.
17. Macaulay, T. (2019). The danger of critical infrastructure interdependency. Centre for International Governance Innovation. https://www.cigionline.org/articles/danger-critical-infrastructure-interdependency/.
18. Marotta, A., & McShane, M. (2018). Integrating a Proactive Technique Into a Holistic Cyber Risk Management Approach. Risk Management and Insurance Review, 21(3), 435–452. DOI: 10.1111/rmir.12109
19. Motaleb, O. H., & Kishk, M. (2017). Assessing risk response maturity: A framework for construction projects success in the United Arab Emirates. International Journal of Managing Projects in Business, 10(2), 247-262.
20. Nunes-Vaz, R., Lord, S. & Ciuk, J. (2011). A More Rigorous Framework for Security-in-Depth, Journal of Applied Security Research, 6(3), 372-393.
21. Oliva, F. L. (2016). A maturity model for enterprise risk management. International Journal of Production Economics,173, 66–79. https://doi.org/10.1016/j.ijpe.2015.12.007.
22. Pokrajčić, I. (2025). Odrednice upravljanja sigurnosnim rizicima u srednjim i velikim poduzećima iz domene nacionalne kritične infrastrukture Republike Hrvatske u skladu s normom ISO 31000: 2018 (Doctoral dissertation, University of Zagreb. Faculty of Economics and Business)
23. Pokrajčić, I., & Lazibat, T. (2025). Odrednice upravljanja sigurnosnim rizicima u srednjim i velikim poduzećima obuhvaćenima nacionalnom kritičnom infrastrukturom Republike Hrvatske. Ekonomska misao i praksa, 34(2), 369–394.https://doi.org/10.17818/EMIP/2025/26
24. Tubis, A. A., & Werbińska-Wojciechowska, S. (2021). Risk Management Maturity Model for Logistic Processes. Sustainability, 13(2), 659. DOI 10.3390/su13020659
25. Tweneboah-Koduah, S., & Buchanan, W. J. (2018). Security Risk Assessment of Critical Infrastructure Systems:

A Comparative Study. Computer Journal, 61(9), 1389-1406. DOI 10.1093/comjnl/bxy002

26. Unger, C. J., Lechner, A. M., Kenway, J., Glenn, V., & Walton, A. (2015). A jurisdictional maturity model for risk management, accountability and continual improvement of abandoned mine remediation programs. Resources Policy, 43, 1–10.

27. Villegas-Ch, W., & García-Ortiz, J. (2023). Toward a Comprehensive Framework for Ensuring Security and Privacy in Artificial Intelligence. Electronics, 12(18), 3786.

28. Wangen, Gaute, Hallstensen, C. & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness. International Journal of Information Security, 17(6): 681–699.

29. Zou, P. & Chen, Y. & Chan, T. (2010). Understanding and Improving Your Risk Management Capability: Assessment Model for Construction Companies. Journal of Construction Engineering and Management, 136(8), 854-863.

BY NC ND