Ivana Pokrajčić, PhD
Ministry of Defense of the Republic of Croatia
University of Defense and Security "Dr. Franjo Tuđman"
E-mail: ivpokrajcic@gmail.com
Orcid: https://orcid.org/0009-0001-2223-9122

Tonći Lazibat, PhD
Full professor
University of Zagreb
Faculty of Economics and Business
E-mail: tlazibat@net.efzg.hr
Orcid: https://orcid.org/0000-0002-4806-2652

THE CORRELATION BETWEEN THE IMPLEMENTATION OF ISO 31000:2018 AND THE MATURITY OF SECURITY RISK MANAGEMENT IN COMPANIES FROM THE NATIONAL CRITICAL INFRASTRUCTURE SECTOR OF THE REPUBLIC OF CROATIA

UDC / UDK: 006.88:005.334:351.78(497.5)
JEL classification / JEL klasifikacija: M10, H56, G32, D81
DOI: 10.17818/EMIP/2025/26
Original scientific paper / Izvorni znanstveni rad
Received / Primljeno: April 14, 2025 / 14. travnja 2025.
Accepted / Prihvaćeno: May 13, 2025 / 13. svibnja 2025.

Abstract

The implementation of the ISO 31000:2018 and its effectiveness in the segment of national critical infrastructure of the Republic of Croatia has not been sufficiently scientifically explored, despite the fact that its application in this specific segment is normatively regulated. This article empirically investigates, using multivariate statistical analysis methods, the intercorrelation between the implementation of the ISO 31000:2018 and the maturity of security risk management in companies within the national critical infrastructure of the Republic of Croatia. The research results show that the level of implementation of the ISO 31000:2018 standard has a significant and positive impact on the maturity of security risk management. The study also examined the differences between medium-sized and large companies in the sub-dimensions of security risk management, and the results indicate that the maturity of security risk management is higher in large companies compared to medium-sized ones within the national critical infrastructure.

Keywords: ISO 31000:2018, risk maturity, security risk management, national critical infrastructure

1. INTRODUCTION

In today's dynamic business environment, organizations are increasingly exposed to a wide range of risks that can significantly impact their operations and long-term development (Torabi et al., 2016; Dvorski et al., 2021). Over the past fifteen years, various methods and mechanisms have been developed with the aim of mitigating the adverse effects of known risk factors on business continuity and growth. The academic literature consistently underscores the necessity of effective risk management practices, which must be grounded in the latest research findings and internationally recognized standards (Hopkin, 2018; Markova et al., 2018; Rampini, Takia & Berssaneti, 2019).

Risk management today is characterized by an integrated approach, incorporating multiple methodologies and frameworks. Central to this approach is the risk management process itself, supported by a theoretical foundation that collectively forms the basis of risk management standards (Hopkin, 2019; Rampini et al., 2019). Among these, the ISO 31000 standard has emerged as one of the most widely adopted frameworks, providing structured guidance for the identification, assessment, and mitigation of organizational risks.

This article investigates the influence of institutional determinants embedded within the ISO 31000:2018 standard on the maturity of security risk management processes in companies operating within sectors designated as part of the national critical infrastructure. Although recent literature has addressed the relationship between the adoption of ISO 31000:2018 and the maturity of risk management practices, a comprehensive and context-specific analysis of this relationship within the domain of national critical infrastructure remains notably underexplored. This article, therefore, addresses the question of how - and to what extent - the institutional elements of ISO 31000:2018 influence the maturity of security risk management processes in companies belonging to the national critical infrastructure sector of the Republic of Croatia.

Existing theoretical and empirical research on the implementation of the ISO 31000 standard, as well as the factors that may affect its implementation, remains relatively fragmented. To date, no similar study has been conducted on companies in the Republic of Croatia, particularly in relation to the application of the updated ISO 31000:2018 version. Moreover, as highlighted by Teller, Kock & Gemunden (2014), Jun, Qiuzhen & Qingguo (2011), and Thamhain (2013), a universal risk management model is not effective in practice. They argue that future research should focus on identifying contextual determinants that guide the adaptation of existing models, taking into account the specific characteristics of individual organizations.

In addition to its scientific contribution, this article offers practical value by identifying the advantages of effective security risk management in day-to-day business operations, thereby enhancing the understanding of these practices among security professionals and corporate managers.

Following the introduction to the research problem and its relevance, second chapter present a comprehensive theoretical framework that examines key concepts such as ISO 31000 standard, national critical infrastructure and risk management maturity models. Building upon this foundation, the third chapter outlines the research hypotheses and presents the methodological approach adopted for data collection and analysis. The fourth chapter presents the empirical findings and discusses their implications in light of the existing literature. Finally, the article concludes by summarizing the key results, highlighting theoretical and practical contributions, and suggesting directions for future research and policy development.

2. THEORETICAL BACKGROUND

2.1. Standard ISO 31000:2018 - Risk Management

The decision-making process inherently involves risk, which can manifest either as a threat to planning or as an unanticipated opportunity (Olechowski et al., 2016, p. 1571). Consequently, there is a compelling need for the implementation of risk management practices in businesses to enhance the likelihood of success in the complex, multidisciplinary, and challenging activities of project management and product development (Oliva, 2016, p. 73). Over time, scientific research on this topic has gained importance, initially leading to the introduction of Risk Management as a new and significant area of study within academic institutions (Fraser, 2009, p. 101). Subsequently, risk management matured as a discipline, with frameworks developed to assist organizations worldwide in adopting common best practices (Rosa & Toledo, 2015).

Best practices in risk management have evolved over time, culminating in the development of specialized standards, norms, and frameworks based on accumulated research and practical experience (Doi, 2017). One of the most important and widely recognized standards is ISO 31000 - Risk Management, established by the International Organization for Standardization (ISO), which is applied globally (Lalonde & Boiral, 2012). According to Lalonde & Boiral (2012), in the context of applying the ISO 31000 standard to security risk management, the approach is typically understood as a “top-down” methodology, which is analyzed in this article through the institutional determinants. As Scolobig et al. (2015, p. 203) noted, institutional risk management is a hierarchically organized process, where the level of implementation and coordination is proportional to the size, scope, and activities of the organization. This traditional approach assumes that the entire responsibility for risk management rests with the company, while employees are merely passive observers. Furthermore, Boss and Kirsch (2007) and Lee et al. (2016) emphasize that the institutional imposition of mandatory compliance with security procedures, often referred to in the literature as the implementation of safety standards and policies, is a proactive and widely accepted approach that all organizations should strive for. Olechowski et al. (2016) propose the use of risk

management principles as an alternative to universal practices or tools. Research on the effects of ISO 31000:2018 indicates that companies that have adopted the standard experienced significant improvements in their risk management processes, particularly in better identification, assessment, and mitigation of risks, as well as a more comprehensive integration of risk management into overall decision-making within the organization (Hillson & Murray-Webster, 2020). Additionally, companies that have implemented ISO 31000:2018 have enhanced their organizational resilience. ISO 31000:2018 highlights the importance of building organizational resilience to risks, and studies suggest that organizations adhering to this standard are better equipped to withstand and recover from adverse events (Hardjmidjojo et al., 2022, p. 4). Moreover, companies that have adopted the standard show an increase in trust among all relevant stakeholders.

Research demonstrates that implementing the standard leads to improved relationships with clients, investors, regulators, and other stakeholders who value transparency and accountability in risk management (Yuwono & Ellitan, 2023, p. 2031). Furthermore, companies that have implemented the standard are more agile in adapting to changing circumstances (Bjarte et al., 2020, p. 36). Boss and Kirsch (2007) and Lee et al. (2016) further emphasize that the institutional enforcement of security procedures, or the implementation of safety standards and policies, is a proactive and universally accepted approach that all organizations should pursue. Olechowski et al. (2016) suggest utilizing risk management principles as an alternative to universal practices or tools. Olechowski et al. (2016) conducted a scientific study on the effectiveness of the ISO 31000 standard, surveying a sample of 291 respondents employed by companies within the defense industry. Among other aspects, they explored the interrelationship between the core principles of the standard. Their investigation into the links between these principles revealed a statistically significant correlation between certain principles. Similarly, Oehman et al. (2014) examined the relationship between each individual core principle of ISO 31000 and the implementation of risk management practices, as well as the final outcomes of specific development projects. The study demonstrated a statistically significant connection between the implementation of practices prescribed by ISO 31000 and project success. However, they also concluded that measuring the effectiveness of risk management based solely on overall project and product success is insufficient (Oehman et al., 2014, p. 25). Although the study provided empirical evidence for the existence and strength of this connection, statistical measures of association or correlation, by their nature, do not imply causality. When discussing the structural dimension of the ISO 31000:2018 standard, it encompasses those principles of the standard that are implemented within the organizational structure, while the process dimension involves those principles that are incorporated into the business processes of the company.

2.2. National Critical Infrastructure - the importance of security risk management

National critical infrastructures consist of systems, networks, and facilities of national importance, whose disruption or the interruption of goods or services delivery could have severe consequences for national security, public health and safety, property, the environment, economic stability, and the continuous functioning of government authorities. The protection of critical infrastructures is also a priority of the European Union. The sectors of national critical infrastructure include the financial sector, energy, communications and information technologies, transportation, healthcare, water management, and food production. Hemme (2015) highlights the strong interdependencies among the sectors of national critical infrastructure in the context of security risk management, which manifest through a domino or cascading effect, meaning that the potential impact of security incidents in one sector can spill over into others. Rinaldi, Peerenboom & Kelly (2002) examined the interrelationships between these sectors and concluded that they form a complex adaptive system, which, when adapting to disruptive events, should be viewed through various organizational determinants. However, Weiss and Biermann (2021) stress that in order to protect national critical infrastructure, security risk management must be more aggressively enforced by the state. Hemme (2015) also discusses the potential for a domino or cascading effect should one segment of the national critical infrastructure be incapacitated. Additionally, Macaulay (2019) further investigated and confirmed the interdependence of national critical infrastructure segments, notably highlighting the interdependence of all sectors on the energy sector (Macaulay, 2019, p. 72).

In the context of the Republic of Croatia, it is important to note that the sectors of national critical infrastructure are legally defined as "of special importance," and their owners/operators are legally obligated to conduct risk analyses as a basis for creating a Security Plan (Critical Infrastructure Act, NN 65/13). In line with the principles of aggressive state intervention proposed by Weiss and Berman, and in accordance with binding European regulations, Croatia has also developed more detailed guidelines, criteria, and standards for the identification of critical infrastructures. Specifically, the 2016 Regulation on the Methodology for Business Risk Analysis of Critical Infrastructures stipulates these provisions and identifies the responsible parties for conducting business risk analyses of critical infrastructures, in accordance with the ISO 31000:2009 standard. This transfer of responsibility for security risk management almost entirely shifts the burden to businesses. Security risks can have adverse effects on business operations and outcomes (Pertu, 2016), and therefore, many companies treat them as a distinct category within their risk management processes. Security risks refer to risks related to breaches of information security within a company (Alberts, 2003; Miyazaki, 2001), such as theft of intellectual property, business plans, or personal data of employees, clients, and partners. They also include risks to the security of business processes (Speight, 2011; Shaw & Smith, 2010) and

risks to physical security (Fennely, 2016), such as theft of tangible assets and other property, as well as employee safety.

2.3. Risk Management Maturity Models

The application of risk management maturity models has been explored in various industries within the scientific literature, including the variableion sector (Motaleb & Kishk 2017), maritime sector (Laine et al., 2024), legal sector (Unger et al., 2015), corporate sector (Oliva, 2016), logistics processes evaluation (Tubis & Werbińska-Wojciechowska, 2021), as well as in financial institutions and high-tech companies (Alijoyo et al., 2021). Tubis and Werbińska-Wojciechowska (2021) emphasize that the maturity of risk management can be defined as the status of completeness, development, or compliance with prescribed standards. Caiado et al. (2016) compared five different models for evaluating risk management and concluded that business risk management can be continuously improved if the determinants that influence it are identified and understood in terms of their impact.

According to Tubis and Werbińska-Wojciechowska (2021), the development of the risk management concept has led to the need for the creation of tools that will (a) enable the organization to assess the current level of implementation of specific solutions that support the process of addressing adverse events, and (b) indicate the direction for further development or changes that will strengthen the resilience of processes to security incidents or disruptions in business operations. The risk management maturity model developed by Tubis and Werbińska-Wojciechowska (2021) is presented in Table 1.

Table 1 Security Risk Management Maturity model

	1 - Low	2 - Basic	3 - Good	4 - Satisfactory	5 - Excellent
Knowledge	There is a lack of knowledge about security risks and their potential consequences. The company relies solely on its own knowledge.	The individuals responsible for managing security risks rely on the knowledge of employees, but this knowledge is not systematically documented anywhere.	Based on the security risk reports, individuals responsible for security report on the most significant security incidents.	A knowledge base has been established that covers the causes, effects, occurrence, and critical processes exposed to security risks.	The knowledge base on security risks is regularly updated with identified risks and events that impact processes and business outcomes. The knowledge is also based on the knowledge of external entities. Defined principles are in place, based on the acquired knowledge of security risks.

Risk identification and analysis	No security risks have been identified that could affect business operations or business processes.	In the event of a security incident, risks are assessed using qualitative tools. The results of the analysis are communicated only to the company's management.	Risk identification and analysis are carried out only at the request of management and are conducted by employees responsible for the specific area covered by the risk. Qualitative tools are mainly used. The results are communicated to management and to the business segment affected by the risk.	Risk analysis is conducted at regular intervals for all business processes. The analysis is carried out using both quantitative and qualitative tools. The results of the analysis are communicated to management and executive personnel.	Risk assessment is conducted in a planned manner and is regularly updated. The assessment is based on the knowledge of executives from different areas – an expert team consisting of individuals from various operational areas of the company. Advanced quantitative and qualitative methods and tools are used. The results of the analysis are communicated to all operational areas of the company.
Risk response	Critical business processes have not been identified in the company. Limitations or undesired security events that may impact business processes have not been considered	Critical business processes or activities that are essential for project implementation and company operations have been identified.	The results of the conducted analysis are used for planning high-security-risk business processes. Prevention is not sufficiently developed, nor are the measures for mitigating security risks. Business processes are not improved based on existing identified security risks.	Procedures and scenarios have been developed for the prevention of security incidents for business processes and activities that are most exposed to security risks.	Risk assessment results are the basis for planning all business processes. Preventive measures have been developed to protect critical business processes, and scenarios have been developed for managing the consequences of security risks.
Risk Monitoring	A system of indicators used to monitor the effectiveness and efficiency of business processes has not been developed.	Basic indicators have been developed for monitoring. Risk assessment indicators are insufficiently developed.	Indicators for monitoring the efficiency and effectiveness of processes have been developed, and they are regularly calculated, with reports provided to the company's management.	A formalized system of indicators is used to monitor the efficiency of processes and their compliance with defined security procedures.	A comprehensive system of indicators has been implemented. Regular analysis and interpretation of observed deviations are conducted. The results are shared with all business segments.
Cooperation	There is no exchange of information about security risks within the company or with business partners.	For critical security risks, information is exchanged among different business segments in accordance with management guidelines.	Data on security risks are communicated among different business segments. There is internal collaboration in planning business processes exposed to security risks. Information on security incidents is exchanged with business partners.	Data on security risks and the occurrence of security incidents are exchanged within the company and with strategic partners. Scenarios for crisis management in the event of a security incident have been developed.	Information on security risks and the occurrence of security incidents is exchanged within the company and with business partners. There is collaboration with partners to prevent security risks or reduce the consequences of security incidents. A plan for a coordinated response to the occurrence of harmful events exists.

Source: Author, model adjusted to Tubis and Werbińska-Wojciechowska (2021)

It is important to note that risk maturity models are typically qualitative models, designed to describe the current state of risk management process implementation within an organization. These models generally consist of attributes that aim to describe key characteristics of risk management, such as management's commitment to risk management. In the mentioned study, different weighting criteria (weights) were assigned to these attributes in order to calculate the maturity level, as shown in Table 2.

Table 2 Calculation of Risk Management Process Maturity

	Option 1		Option 2	
Area	**Weight**	**Level of maturity**	**Weight**	**Level of maturity**
Knowledge	0,2	3	0,1	3
Risk indetification and analysis	0,3	3	0,3	3
Risk response	0,3	2	0,3	2
Risk monitoring	0,2	3	0,1	3
Cooperation	-	-	0,2	1
Indicator of Maturity	**2,7**		**2,3**	

Source: Tubis and Werbińska-Wojciechowska (2021, pp. 14).

3. HYPOTHESIS DEVELOPMENT

The main research questions of this article are as follows:

RQ1: To what extent do the institutional provisions of the ISO 31000:2018 standard affect the maturity of the security risk management process in companies within the critical national infrastructure sector of Croatia?

RQ2: Which sectors of national critical infrastructure exhibit the highest degree of compliance with ISO 31000:2018?

RQ3: What is the difference in the maturity of security risk management between medium-sized and large companies?

Based on these research questions, the following hypothesis and sub-hypotheses were formulated:

H1: Compliance with ISO 31000:2018 (fundamental principles, structural dimension, and process dimension) positively and statistically significantly influences the maturity of the security risk management process in companies from the national critical infrastructure sector of Croatia.

H1a: Acceptance of the fundamental principles (ID1) of the ISO 31000:2018 standard positively influences the maturity of the security risk management process in companies from the national critical infrastructure sector.

H1b: Implementation of the structural dimension (ID2) of the ISO 31000:2018 standard positively influences the maturity of the security risk management process in companies from the national critical infrastructure sector.

H1c: Development of the process dimension (ID3) of the ISO 31000:2018 standard positively influences the maturity of the security risk management process in companies from the national critical infrastructure sector.

H2: The maturity of the security risk management process is higher in large companies from the national critical infrastructure sector.

The impact of the institutional provisions of the ISO 31000:2018 standard on security risk management in companies was examined through three sub-hypotheses. Respondents answered individual statements using the Likert scale; thus, the aggregate variable for the implementation of the institutional provisions of the ISO 31000:2018 standard was formed as the arithmetic mean of the group of questions related to the institutional provisions of these sub-hypotheses. Reliability was tested using Cronbach's alpha coefficient. The variable representing the impact of the implementation degree of institutional provisions of the ISO 31000:2018 standard on the maturity of security risk management was assessed using the variables listed in Table 3. In order to test Hypothesis 2, statistical analysis was conducted on the collected data for medium-sized and large companies, providing valuable insights into the differences between them.

Table 3 Presentation of research variables and their measurement methods

Institutional dimension (ID)	
ID1 - Application of basic principles **(ISO 31000:2018)**	Respondents express their level of agreement with the statements (ISO 31000:2018) on a Likert scale from 1 to 5. A higher total score means that the company has implemented the core principles of risk management in accordance with ISO 31000:2018 to a greater extent. (Olechowski et al., 2016.) (q1) Risk management adds value to the company (q2) Risk management is an integral part of every business process (q3) Risks are considered when making business decisions (q4) Risk management is based on available information (q5) Risk management is tailored to the specifics of the company (q6) It takes into account human and cultural factors (q7) The risk management process is transparent and inclusive (q8) The risk management process is dynamic and adaptable (q9) The risk management process supports continuous business improvement
ID2 - Implementation of the structural dimension (ISO 31000:2018)	Respondents express their level of agreement with the statements (ISO 31000:2018) on a Likert scale from 1 to 5. A higher total score means that the company has successfully implemented the structural dimension of risk management in accordance with ISO 31000:2018. (q10) In my organization, roles and responsibilities for risk management have been divided (q11) Risk management planning and resource allocation have been carried out or are being carried out (q12) Allocated resources are sufficient for effective risk management (q13) Regulations and procedures related to risk management have been implemented in the organization (q14) Regulations and rules from the risk management domain have been implemented (q15) An internal audit/supervision of compliance with prescribed procedures is conducted (q16) Continuous efforts are made to improve safety in the company (q17) Security management is carried out through outsourcing
ID3 - Development of the process dimension **(ISO 31000:2018)**	Respondents express their level of agreement with the statements (ISO 31000:2018) on a Likert scale from 1 to 5. A higher total score means that the company has successfully implemented the process dimension of risk management in accordance with ISO 31000:2018. (q18) There is clear communication and coordination of risk management at all levels within the company (q19) The organization carries out risk context determination (risk assessment) (q20) The organization conducts risk evaluation (q21) The organization has a plan for responding to risk occurrences (q22) Risk monitoring is carried out
Security risk management (SRM) - The variable and its corresponding subdimensions will be measured through statements from validated scales taken from existing literature. Respondents will express their agreement with only one statement from the model by Tubis and Werbińska-Wojciechowska (2021) shown in Table 1.	

Source: Author

The research instrument employed in this study was a survey questionnaire distributed online. It was developed based on relevant scientific literature, with adjustments made to align with the selected research topic. The questionnaire consists of a set of statements that allowed respondents to express the intensity of their agreement or disagreement.

The first part of the research instrument measured the degree of implementation of the ISO 31000:2018 standard (variable ID), specifically its main provisions. Using a Likert scale, the implementation of the standard's fundamental principles (ID1), the implementation of the structural dimension (ID2), and the development of the process dimension (ID3) were assessed within the companies included in the research. A higher level of agreement indicated a higher degree of implementation of the ISO 31000:2018. The second part of the research instrument measured the maturity of the security risk management process (variable SRM) in companies from the national critical infrastructure sector of the Republic of Croatia.

The research targeted individuals holding senior management positions or those with primary responsibility for overseeing security risk management within their respective companies. The sample was compiled using data obtained from the Digital Chamber of Commerce and the FINA Financial Agency platform, which yielded a dataset comprising 241 medium-sized and 89 large enterprises. Of the total 330 companies initially targeted by the research, 125 valid responses to the survey questionnaire were included in the sample, of which 64% percent were top management level executives, 30.4% are middle management security specialists, and 5.6% of the respondents were neither of the above. The composition of the sample reflected a modest predominance of respondents from large companies (N = 70) in comparison to those from medium-sized companies (N = 53). The research sample was composed of respondents representing a diverse range of sectors within the national critical infrastructure of the Republic of Croatia. A total of 125 participants contributed to the study, with the largest proportion drawn from the food sector (N = 42; 32%), followed by representatives from the energy sector (N = 24; 19.2%) and the transportation sector (N = 18; 14.4%). Additional representation included respondents from the water management sector (N = 16; 12.8%), the information and communication infrastructure sector (N = 15; 12%), the finance sector (N = 6; 4.8%), and the health sector (N = 4; 3.2%). This distribution ensured comprehensive sectoral coverage and facilitated a more nuanced understanding of security risk management practices across the critical infrastructure landscape.

For the descriptive analysis of the collected data, the arithmetic mean and standard deviation were used for interval scale variables, while the median and interquartile range were employed for ordinal scale variables. The distributions were further examined by determining the minimum and maximum values, as well as the coefficients of skewness and kurtosis. The normality of the distributions was tested using the Kolmogorov-Smirnov test. As all distributions significantly deviated from normality, the median and interquartile range were used as measures of central tendency and dispersion.

For the institutional provisions of the ISO 31000:2018 standard, the factor structure of the employed scales was examined through principal component analysis, as the scale was specifically variableed for this research. Prior to conducting the factor analysis, the inter-correlations between the variables included in the analysis were determined using Pearson's correlation coefficient. To determine the number of dimensions underlying the measured variables, the Kaiser-Guttman criterion was used, which selects the number of dimensions with eigenvalues greater than one. Additionally, a Scree test was employed, based on the criterion of the largest drop in the eigenvalue values.

The overall results for the employed scales were determined as the average of the responses to the items comprising the scale, and the reliability of the scale was assessed using Cronbach's α coefficient of internal consistency. For determining the maturity of security risk management, the total score was calculated using the weights defined by Tubis and Werbińska-Wojciechowska (2021).

4. RESEARCH RESULTS

4.1. Institutional dimension of ISO 31000:2018 - variable ID

The arithmetic means and standard deviations of the items intended to measure the aspects of the institutional provisions of the ISO 31000:2018 standard are presented in Table 4.

Table 4 Arithmetic Means and Standard Deviations

		M	*SD*
ID	**Institutional dimension**	3,72	1,25
ID1	Basic principles of the standard	3,91	1,13
ID2	Structural dimension	3,64	1,27
ID3	Process dimension	3,62	1,37

Source: Author

The descriptive statistics for the items measuring the application of the fundamental principles of risk management (ID1) are presented in Table 5. All items, except for one, covered the full range of the applied scale; however, the distributions of results were skewed towards the higher values and significantly deviated from a normal distribution.

Table 5 Descriptive Statistics of Items Intended for Measuring the Fundamental Principles of ISO 31000:2018

					K-S test	
	min	*max*	*M*	*SD*	*z*	*p*
q1	2	5	4,65	0,57	0,42	< 0,001
q2	1	5	3,98	1,09	0,31	< 0,001
q3	1	5	3,86	1,15	0,30	< 0,001
q4	1	5	3,92	1,08	0,31	< 0,001
q5	1	5	4,03	1,26	0,28	< 0,001
q6	1	5	3,42	1,35	0,27	< 0,001
q7	1	5	3,59	1,26	0,29	< 0,001
q8	1	5	3,63	1,37	0,25	< 0,001
q9	1	5	4,09	1,07	0,27	< 0,001

Source: Author

The results indicate that respondents generally held a positive attitude towards risk management and believed it added value to the organization ($M = 4.65$, $SD = 0.57$, $p < 0.001$). While all responses were affirmative regarding risk management, the lowest scores were observed for statements related to the transparency and inclusiveness of the process ($M = 3.59$, $SD = 1.26$, $p < 0.001$), as well as the consideration of human and cultural factors ($M = 3.42$, $SD = 1.35$, $p < 0.001$).

To examine the dimensionality of the items designed to measure the application of the core principles of the ISO 31000:2018 standard, Pearson's correlation coefficient was initially used to determine the intercorrelations between the items. The high intercorrelations suggest the existence of a single underlying dimension in the items used. These findings align with those of Olechowski et al. (2016), who conducted a study on the effectiveness of the ISO 31000 standard and demonstrated a statistically significant relationship among the core principles. Similar to Olechowski et al., all intercorrelations between the items intended to measure the core principles of the standard were significant.

The dimensionality of the application of the core principles (ID1) was tested through exploratory factor analysis, specifically principal component analysis. According to the Kaiser-Guttman criterion, only one dimension was extracted, as it had an eigenvalue greater than 1. The appropriateness of extracting a single dimension was further supported by the Scree test, which showed a clear drop in the eigenvalues after the first dimension. The extracted dimension accounted for 75.66% of the variance in the variables included in the analysis. All

factor loadings were high, indicating the suitability of all items for measuring the application of the core principles of the ISO 31000:2018 standard. The internal consistency reliability, assessed using Cronbach's α coefficient, was 0.96. The range of responses varied from 1.33 to 5.0, with a mean of 3.91 and a standard deviation of 0.99. The distribution of results was positively skewed, significantly deviating from a normal distribution (Kolmogorov-Smirnov $z = 0.15$, $ss = 125$, $p < 0.001$). Due to the skewed distribution, the median and interquartile range were used as measures of central tendency and dispersion, yielding a median of 4.11 and an interquartile range from 3.28 to 4.67.

Descriptive statistics for the items measuring the implementation of the structural dimension (ID2) of the ISO 31000:2018 standard are presented in Table 6. Nearly all items spanned the full range of the scale; however, the distributions of responses significantly deviated from a normal distribution, with mean values slightly above the theoretical average, indicating a skew toward higher values. The highest mean was observed for the item "q13: In my company, general regulations and rules related to security have been implemented" ($M = 4.22$, $SD = 1.01$, $p < 0.001$), while the lowest mean was recorded for the item "q17: My company has outsourced security risk management to an external contractor" ($M = 2.58$, $SD = 1.51$, $p < 0.001$).

Table 6 Descriptive Statistics of Items Intended for Measuring the Implementation of the Structural Dimension (ID2) of the ISO 31000:2018 Standard

					K-S test	
	min	*max*	*M*	*SD*	*z*	*p*
q10	1	5	4,00	1,28	0,29	< 0,001
q11	2	5	4,02	1,10	0,28	< 0,001
q12	1	5	3,09	1,33	0,27	< 0,001
q13	1	5	4,22	1,01	0,28	< 0,001
q14	1	5	3,63	1,35	0,30	< 0,001
q15	1	5	3,63	1,38	0,24	< 0,001
q16	1	5	3,92	1,23	0,26	< 0,001
q17	1	5	2,58	1,51	0,25	< 0,001

Source: Author

The intercorrelations between the items were relatively high, suggesting the presence of a single underlying dimension. The dimensionality was subsequently examined through principal component analysis. The analysis

revealed that only one principal component had an eigenvalue greater than one, confirming the retention of a single dimension. This conclusion was further supported by a clear drop in the eigenvalues. The extracted dimension accounted for 71.34% of the variance in the variables included in the analysis. All factor loadings were sufficiently high to justify the inclusion of all items in the overall result. The internal consistency reliability, measured using Cronbach's α coefficient, was 0.94. The range of responses varied from 1.38 to 5.0, with a mean of 3.64 and a standard deviation of 1.06. The distribution of results significantly deviated from a normal distribution (Kolmogorov-Smirnov $z = 0.15$, $ss = 125$, $p < 0.001$). The median (interquartile range) was 4.00 (2.69–4.56).

The descriptive statistics for the items measuring the development of the process dimension (ID3) of the ISO 31000:2018 standard is presented in Table 7. Although all items covered the full range of the utilized scale, as was the case with the previous two dimensions (ID1 and ID2) of institutional provisions, the result distributions significantly deviated from normality. In this case, the arithmetic means were above the midpoint of the scale, indicating that the result distributions were skewed towards the higher values of the scale.

Table 7 Descriptive Statistics of Items Intended for Measuring the Development of the Process Dimension (ID3) of the ISO 31000:2018 Standard

					K-S test	
	min	*max*	*M*	*SD*	*z*	*p*
q18	1	5	3,40	1,42	0,25	< 0,001
q19	1	5	3,56	1,43	0,23	< 0,001
q20	1	5	3,26	1,48	0,23	< 0,001
q21	1	5	4,16	1,08	0,28	< 0,001
q22	1	5	3,72	1,42	0,27	< 0,001

Source: Author

The highest arithmetic mean ($M = 4.16$) was recorded for the statement "q21: My company has a plan for managing risks." All correlations were relatively high, indicating that a single dimension underlies the responses to these items. Factor analysis revealed that only one principal component had an eigenvalue greater than one, thus confirming the existence of a single dimension. This was further supported by the decline in eigenvalue magnitudes. The internal consistency reliability, expressed through Cronbach's α coefficient, was 0.96. The range of results varied from 1.00 to 5.00, with a mean of 3.62 and a standard deviation of 1.27. The distribution of results significantly deviated from normality,

as indicated by the Kolmogorov-Smirnov test ($z = 0.19$, $ss = 125$, $p < 0.001$). The median was 4.20, with an interquartile range of 2.40–4.80.

The analysis indicated that, according to the Kaiser-Guttman criterion, two dimensions could be identified behind the responses to all items. However, the first eigenvalue was significantly higher than the next, suggesting the existence of only one dimension, which explained 71.40% of the variance in the items included in the analysis. The results led to the conclusion that only one factor is present. The reliability of the overall result, expressed through Cronbach's α coefficient, was 0.98. The range of results varied from 1.32 to 5.00, with a mean of 3.74 and a standard deviation of 1.04. The distribution of results significantly deviated from normality, as indicated by the Kolmogorov-Smirnov test ($z = 0.12$, $ss = 125$, $p < 0.001$). The median was 4.05, with an interquartile range of 2.77–4.70.

4.2. Maturity of security risk management - variable SRM

The statistical analysis of the collected data regarding risk management is presented in Table 8. The medians for knowledge, identification, and response to security risks were high, while for the remaining two aspects, the medians were somewhat lower.

Table 8 Medians and Interquartile Range - SRM

	C	*IQR*
Knowledge about security risks	4,00	2,00-5,00
Identification and analysis of security risks	4,00	2,00-5,00
Response to security risks	4,00	2,00-5,00
Security risk monitoring	3,00	2,00-5,00
Cooperation	3,00	2,00-5,00

Source: Author

The overall result representing the level of security risk management was determined according to Tubis and Werbińska-Wojciechowska (2021), as described in the previous chapter. Each aspect was multiplied by its respective weight, and the results were then summed. The weights were as follows: 0.1 for knowledge, 0.3 for identification and analysis, 0.3 for response to security risks, 0.1 for monitoring, and 0.2 for collaboration. The results ranged from 1 to 5, with a mean of 3.33 and a standard deviation of 1.35. However, the distribution of results was skewed towards higher values and significantly deviated from a normal

distribution (Kolmogorov-Smirnov z = 0.12, ss = 125, p < 0.001). Therefore, both the median and interquartile range were used as measures of central tendency. The median was 3.50, and the interquartile range ranged from 2.00 to 4.75.

4.3. Intercorrelation between variables and subdimensions

To examine the interrelationships between the variables under investigation, correlation coefficients were calculated, as presented in Table 9. Statistically significant positive correlations were found between all the variables tested. A higher expression of the institutional dimension, both at the overall level and at the subdimension level, particularly the subdimension of adopting the fundamental principles of ISO 31000:2018, was associated with more pronounced security risk management. This was observed both at the total result level (ID/SRM = 0.92, p < 0.001) and at the subdimension level (ID1/SRM = 0.88, p < 0.001; ID2/SRM = 0.90, p < 0.001; ID3/SRM = 0.91, p < 0.001).

Table 9 Interrelationship between variables expressed through Pearson's correlation coefficient

	ID	ID1	ID2	ID3	SRM	SRM1	SRM2	SRM3	SRM4	SRM5
ID	-									
ID1	0,97	-								
ID2	0,98	0,91	-							
ID3	0,97	0,91	0,94	-						
SRM	0,92	0,88	0,90	0,91	-					
SRM1	0,89	0,84	0,87	0,88	0,93	-				
SRM2	0,89	0,85	0,87	0,90	0,97	0,90	-			
SRM3	0,88	0,84	0,86	0,87	0,96	0,88	0,92	-		
SRM4	0,88	0,84	0,87	0,87	0,94	0,85	0,90	0,90	-	
SRM5	0,89	0,84	0,87	0,87	0,97	0,90	0,92	0,90	0,89	-

Source: Author

In other words, the results show that a higher degree of implementation of the fundamental principles is associated with higher levels of knowledge, identification and analysis, response, monitoring, and collaboration, thus confirming Hypothesis 1. This is elaborated in greater detail by the elements used to assess the maturity of security risk management, and a statistically significant correlation between the implementation and application of the fundamental

principles of the ISO 31000:2018 standard and all the elements used for evaluating the maturity of security risk management is evident. Furthermore, a higher degree of implementation of the structural dimension of security risk management was statistically significantly correlated with higher levels of knowledge, identification and analysis, response, monitoring, and collaboration. Similar to the previous institutional provisions of the ISO 31000:2018 standard, a statistically significant positive correlation was found between the development of the process dimension and all aspects of security risk management. In other words, a higher development of the process dimension of the ISO 31000:2018 standard was associated with higher levels of knowledge, identification and analysis, response, monitoring, and collaboration.

4.4. Analysis of differences between medium and large organisations

In large companies, compared to medium-sized ones, there was a statistically significantly higher level of implementation of the fundamental principles of security risk management, the implementation of the structural dimension of security risk management, and the development of the process dimension of risk management. On the overall level of institutional dimension development, large companies showed a statistically significantly higher level of development than medium-sized companies, as presented in Table 10.

Table 10 Analysis of differences between medium-sized and large companies

	Medium		Large			
	M	*SD*	*M*	*SD*	*t(ss)*	*p*
ID1	3,23	1,00	4,43	0,61	-7,78(80,7)	< 0,001
ID2	2,82	0,92	4,26	0,70	-9,57(94,2)	< 0,001
ID3	2,60	1,05	4,41	0,78	-10,54(92,7)	< 0,001
SRM	2,24	1,03	4,18	0,91	-11,13(121)	< 0,001

Source: Author

The difference between medium and large companies in the subdimensions of security risk management was also examined. Due to the ordinal measurement scale, the median and interquartile range were used as measures of central tendency and dispersion, while the non-parametric Mann-Whitney U test was applied for comparison. All aspects of security risk management were statistically significantly more pronounced in large companies than in medium-sized ones, as presented in Table 11, which confirmed Hypothesis 2.

Table 11 Analysis of subdimension of SRM variable

	Medium		Large			
	C	*IQR*	*C*	*IQR*	*M-W U*	*p*
Knowledge	2,00	1,00-3,00	5,00	3,75-5,00	500,00	< 0,001
Identification and analysis	2,00	2,00-3,00	5,00	4,00-5,00	375,50	< 0,001
Response	2,00	2,00-3,00	5,00	4,00-5,00	456,50	< 0,001
Monitoring	2,00	1,00-3,00	4,00	3,75-5,00	377,00	< 0,001
Cooperation	2,00	1,00-3,00	4,00	3,75-5,00	420,50	< 0,001

Source: Author

5. DISCUSSION OF KEY FINDINGS AND IMPLICATIONS

In this article, in support of confirming or refuting Hypothesis 1, the relationship between the degree of implementation of the ISO 31000:2018 standard and the maturity of security risk management was explored. The results of the conducted research, in which statistical data processing encompassed the entire sample (both medium and large companies), show a significant positive impact of the implementation of the institutional provisions of the ISO 31000:2018 standard on security risk management (ID/SRM, $r=0.90$, $p<0.001$). The application of the fundamental principles of the standard ($M=3.91$, $SD=1.13$, $p<0.001$) is statistically significantly associated with all aspects of security risk management. Specifically, the results show that a higher degree of implementation of the fundamental principles of the standard is associated with higher levels of knowledge ($r=0.84$), identification and analysis ($r=0.85$), response ($r=0.84$), monitoring ($r=0.84$), and collaboration ($r=0.84$), which are key aspects of the maturity evaluation model for security risk management.

As in the case of the fundamental provisions of the ISO 31000:2018 standard, the results showed that a higher degree of implementation of the structural dimension, i.e., those principles that have been implemented into the organizational structure of the company ($M=3.64$, $SD=1.27$, $p<0.001$), as well as the development of the process dimension, i.e., those principles that have been implemented into the business processes of the company ($M=0.62$, $SD=1.37$, $p<0.001$), have positive and statistically significant effects on security risk management, i.e., on all aspects of the maturity evaluation model for security risk management. Empirically, the existence and strength of the correlation has been proven, and causality can also be assumed. In other words, it can be hypothesized that the fact that certain companies have a higher level of maturity in security risk management is a consequence of their higher degree of implementation of the ISO 31000:2018 standard. Additionally, the results indicate that, in the context of the fundamental provisions

of the standard, the lowest measured mean response given by respondents on the Likert scale was M=3.42, with SD=1.35, and p<0.001. This result pertains to the consideration of human and cultural factors in the security risk management process, which represents one of the areas that companies could focus on to improve the effectiveness of implementing the standard and, consequently, security risk management.

In the context of the process dimension of the standard, the lowest result (M=2.58, SD=1.51, p<0.001) was recorded for reliance on external partners (outsourcing). However, this result should not be seen as a potential shortcoming, as it likely indicates the existence of in-house organizational structures that are responsible for security risk management within the companies included in the study. In the context of the structural dimension of the standard, the lowest recorded result concerns the sufficiency of allocated resources for security risk management (M=3.09, SD=1.33, p<0.001). This is not surprising given the fact that research and practices show that companies often struggle with making decisions about resource allocation for risk management, which may or may not occur, to the detriment, for example, of reinvesting in new business opportunities.

The implementation of the ISO 31000:2018 standard must involve a equally dedicated application of all provisions of the standard, meaning putting the standard into practice. Furthermore, achieving a higher level of maturity resulting from the implementation and internalization of the ISO 31000:2018 standard can lead to the optimization of all business processes, a higher level of security in all segments exposed to various forms of security risks, and a more effective integrated risk management process. This comprehensive approach involves assessing risks at all levels within the organization with the goal of minimizing potential negative impacts on the company's operations. Furthermore, the results of the research on the maturity of risk management show that risk management is statistically significantly more mature in large companies (M=4.18, SD=0.91, p<0.001) compared to medium-sized companies (M=2.24, SD=1.03, p<0.001) within the national critical infrastructure segment of the Republic of Croatia. The difference between medium and large companies in the sub-dimensions of risk management was also examined, and it was found that all aspects of risk management were statistically significantly more pronounced in large companies than in medium-sized ones.

Of the total 125 respondents from 125 companies in the national critical infrastructure segment, 28% reported that their company has implemented a comprehensive system of indicators used for monitoring the effectiveness of business processes and their compliance with security procedures. However, 11.2% of the companies stated that they do not have a developed system of indicators for monitoring the effectiveness and efficiency of business processes.

When measuring factors related to knowledge about security risks in medium and large companies within the national critical infrastructure segment, it was found that 20% of respondents believe that their companies lack knowledge about security risks and their potential consequences, while 35.2% of respondents indicated the highest level of knowledge about security risks in their company.

Identification and analysis of security risks was also one of the factors in the model used to assess the maturity of risk management in this article. A total of 24% of respondents stated that risks are assessed using qualitative tools and communicated only to company management. A significant number of respondents (31.2%) indicated that risk assessments are based on expert opinions from responsible individuals, and that the results of the analysis are communicated to all areas of the company, corresponding to the highest level of process maturity.

The risk management maturity model also considers how companies respond to security risks. Those companies that base their business processes on the results of security risk assessments and that have developed not only reactive but also preventive measures to protect critical business processes, as well as scenarios for managing the consequences of security events, are considered to have reached the highest level of maturity in this segment. The research revealed that 30.4% of respondents have reached this level of maturity. Cooperation within companies, as well as the exchange of data on security risks with partners, is an indicator of a high level of risk management maturity, and this was detected in 23.2% of companies. Lower levels of cooperation, indicating a complete or significant lack of communication about security risks within the company, were detected in 43.2% of companies.

The results show that in large companies ($M=4.43$, $SD=0.61$), compared to medium-sized companies ($M=3.23$, $SD=1.00$), there is a statistically significantly higher implementation of the fundamental principles of security risk management, the implementation of the structural dimension of risk management, and the development of the process dimension of risk management. The largest difference was observed in the process dimension, i.e., those aspects of the ISO 31000:2018 standard implemented in the company's business processes, where the results for medium-sized companies ($M=2.60$, $SD=1.05$, $p<0.001$) were significantly lower than for large companies ($M=4.41$, $SD=0.78$, $p<0.001$).

Furthermore, the overall development of the institutional dimension in large companies ($M=4.37$, $SD=0.66$) was significantly higher than in medium-sized companies ($M=2.94$, $SD=0.92$). Analyzing the interrelationships between the institutional provisions of the ISO 31000:2018 standard and risk management, a positive and statistically significant correlation was found in medium-sized companies (IDmedium/SRMm $r=0.70$, $p<0.05$), but it was statistically more significant in large companies (IDlarge/SRMv $r=0.85$, $p<0.001$). A significantly smaller correlation was observed between the institutional provisions of the ISO 31000:2018 standard at all subdimension levels, and the security risk management provision related to risk monitoring in medium-sized companies (IDmedium/SRM4medium, $r=0.57$, $p<0.001$), compared to large companies (IDlarge/SRM4large, $r=0.84$, $p<0.001$). This result, besides generally indicating a lower maturity of security risk management in medium-sized companies, shows that the monitoring mechanisms for the effectiveness of business processes and risk assessment indicators are significantly less developed in medium-sized companies than in large companies in the national critical infrastructure segment of the Republic of Croatia.

6. CONCLUSION

This article positions itself by building upon recently published research addressing organizational resilience in response to crises and security threats (Đokić et al, 2023, Aliyono et al., 2023), process maturity (Milanović Glavan, 2023; Jambor & Nagy, 2023) as well as advancing the scholarly understanding of risk management and security practices (Laine et al., 2023; Aliyono et al., 2023). By empirically examining the relationship between the implementation of the ISO 31000:2018 standard and the maturity of security risk management in national critical infrastructure companies, the article offers a concrete contribution to ongoing discussions on institutionalizing resilience through formalized risk governance frameworks. It extends prior research by integrating a maturity model approach to evaluate the depth and effectiveness of security risk management systems, thereby aligning with the journal's thematic focus while providing novel insights into the operationalization of international standards in high-risk and strategically vital organizational environments.

Through theoretical analysis and empirical research, the article has provided insight into how companies from the national critical infrastructure sector in the Republic of Croatia perceive, implement, and apply the ISO 31000:2018 standard, and how these components influence the maturity of security risk management. This research may be of significance for enhancing the processes of managing security risks in companies, as well as for risk management in general - both within this specific sector and beyond.

The research thoroughly examined the correlation between the implementation of the ISO 31000:2018 standard and the maturity of security risk management in companies that are part of the national critical infrastructure sector in the Republic of Croatia. The findings provide robust empirical evidence supporting the hypothesis that a higher degree of implementation of the standard - particularly its fundamental principles, as well as its structural and process dimensions - positively correlates with more advanced levels of risk management maturity. These results suggest that ISO 31000:2018 serves as a valuable framework for enhancing risk-related practices and organizational preparedness in critical infrastructure entities.

Furthermore, the research highlights that large companies exhibit significantly greater maturity in security risk management than medium-sized enterprises, across all measured dimensions. This discrepancy may reflect differences in resource availability, organizational capacity, and strategic prioritization of security practices. Notably, weaknesses identified in areas such as the integration of human and cultural factors, reliance on external partners, and the allocation of dedicated resources for risk management point to specific opportunities for improvement, especially among medium-sized companies.

It is a known fact that not all companies have adequate human and material resources to allocate to security risk management tasks. However, considering the legal obligations, medium and large companies within the national

critical infrastructure sector of the Republic of Croatia provide an appropriate sample for studying this issue. Furthermore, it is important to recognize that, depending on their level of technological development, the industry they operate in, or their geographic location, not all companies are equally exposed to all forms of security risks. Therefore, it is expected that the systematization of security risks will not be identical across companies, and consequently, the development or maturity of security risk management will vary accordingly.

The implications of these findings are twofold. First, they underscore the need for a more systematic and comprehensive application of the ISO 31000:2018 standard to maximize its impact on organizational resilience. Second, they emphasize the importance of tailored support and capacity-building strategies for medium-sized enterprises to enable them to reach comparable levels of maturity observed in larger organizations. Future research should further investigate causality through longitudinal designs and explore the role of contextual factors, such as sector-specific risk profiles and regulatory environments, in shaping the effectiveness of standard implementation. Ultimately, this study affirms the central role of structured risk management frameworks in safeguarding critical infrastructure and ensuring national security.

Author Contributions: Conceptualization, T.L., I.P.; Methodology, I.P., T.L.; Formal Analysis, I.P.; Writing – Original Draft, I.P.; Resources, I.P., T.L., Review & Editing, T.L.

Funding: The research presented in the manuscript did not receive any external funding.

Conflict of interest: None.

Acknowledgment: This article is based on research conducted as part of a doctoral dissertation entitled "*Determinants of Security Risk Management in Medium and Large Companies within the National Critical Infrastructure Sector of the Republic of Croatia in Accordance with the ISO 31000:2018 Standard.*"

REFERENCES

Alberts, C. J., & Dorofee, A. J. (2003). *Managing information security risks: the OCTAVE approach*. Addison-Wesley Professional.

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2003). *Introduction to the OCTAVE approach.* Carnegie Mellon University, Pittsburgh. https://doi.org/10.21236/ADA634134

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*.

Bjarte, H., Diego, D., Brendryen, J., & Haaga, K. (2020). A simple test for causality in complex systems. *arXiv*: Applications.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, *18* (2), 151-164. https://doi.org/10.1057/ejis.2009.8

Doi, A. (2017). Gerenciamento de riscos corporativos em pequenas e médias empresas: análise de uma empresa nacional no setor de TI. Universidade de São Paulo.

Đokić, I., Rašić, I., & Slijepčević, S. (2023). Inovacije u javnom sektoru: jačanje otpornosti lokalnih i regionalnih jedinica u Hrvatskoj na krizu. *Ekonomska misao i praksa*, *32* (1), 113-132. https://doi.org/10.17818/EMIP/2023/1.6

Fennelly, L. J. (2016). *Effective physical security*. Butterworth-Heinemann.

Fraser, J. R. S. (2013). Message from the chair on introducing enterprise risk management (ERM) to a company. *International Journal of Disclosure and Governance*, *10* (2), 98-104. https://doi.org/10.1057/jdg.2013.12

Hardjomidjojo, H., Pranata, C., & Baigorria, G. (2022). Rapid assessment model on risk management based on ISO 31000:2018. *IOP Conf. Ser.: Earth Environ. Sci.*, *1063* (1), 012043. https://doi.org/10.1088/1755-1315/1063/1/012043

Hemme, K. (2015). Critical Infrastructure Protection: Maintenance is National Security. J*ournal of Strategic Security*, *8* (3), 25-39. https://doi.org/10.5038/1944-0472.8.3S.1471

Hillson, D., & Murray-Webster, R. (2017). *Razumijevanje i upravljanje stavom prema riziku*. Routledge.

Hillson, D., & Murray-Webster, R. (2020). The ISO 31000 Risk Management Standard: How does it align with the Project Management Professional (PMP) credential from the Project Management Institute (PMI)? *International Journal of Project Management.*

Hopkin, P. (2018). *Fundamentals of Risk Management Understanding, Evaluating and Implementing Effective Risk Management*. London Kogan Page Publishers.

Jambor, Z., & Nagy, J. (2023). Resilience of food supply chains. *Ekonomska misao i praksa*, *32* (1), 473-486. https://doi.org/10.17818/EMIP/2023/2.9

Jun, L., Qiuzhen, W., & Qingguo, M. (2011). The effects of project uncertainty and risk management on IS development project performance: A vendor perspective. I*nternational Journal of Project Management*, *29* (7), 923-933. https://doi.org/10.1016/j.ijproman.2010.11.002

Laine, V., Valdez-Banda, O., & Goerlandt, F. (2023). Risk maturity Model for the Maritime authorities: a Deplhi study to design the R-Mare matrix model. *Journal of maritime affairs*, *23* (2), 137-164. https://doi.org/10.1007/s13437-023-00328-z

Lalonde, C., & Boiral, O. (2012). Managing risks through ISO 31000: A critical analysis. *Risk Management*, *14* (4), 272-300. https://doi.org/10.1057/rm.2012.9

Macaulay, T. (2019). The Danger of Critical Infrastructure Interdependency. In Governing Cyberspace during a Crisis in Trust: An essay series on the economic potential – and vulnerability – of transformative technologies and cyber security. Centre for International Governance Innovation, 69-73.

Markova, O. V., Zavalko, N. A., Kozhina, V. O., Panina, O. V., & Lebedeva, O. (2018). Enhancing the quality of risk management in a company, Mejorar la calidad de la gestión de riesgos en una empresa. *Revista Espacios*, *39* (48), 26-37.

Milanović Glavan, Lj. (2023). Procesna zrelost poduzeća u Republici Hrvatskoj. *Ekonomska misao i praksa*, *32* (1), 261-272. https://doi.org/10.17818/EMIP/2023/1.13

Miyazaki, A. D., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer affairs*, *35* (1), 27-44. https://doi.org/10.1111/j.1745-6606.2001.tb00101.x

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.

Oehmen, J., Olechowski A., Kenley, R., & Ben-Daya M. (2014). Analysis of the effect of risk management practices on the performance of new product development programs. *Technovation*, *34* (8), 441-453. https://doi.org/10.1016/j.technovation.2013.12.005

Olechowski, A., Oehmen, J., Seering, W., & Ben-Daya, M. (2016). The professionalization of risk management: What role can the ISO 31000 risk management principles play? *International Journal of Project Managemen*t, *34* (8), 1568-1578. https://doi.org/10.1016/j.ijproman.2016.08.002

Oliva, F. L. (2016). A maturity model for enterprise risk management. *International Journal of Production Economics*, *173* (C), 66-79. https://doi.org/10.1016/j.ijpe.2015.12.007

Rampini, G., Harmi, T., & Berssaneti, F. (2018). Critical Success Factors of Risk Management with the Advent of ISO 31000 2018 - Descriptive and Content Analyzes. *Procedia Manufacturing*, *39*, 894-903. https://doi.org/10.1016/j.promfg.2020.01.400

Rampini, G. H., Takia, H., & Berssaneti, F. (2019). Critical Success Factors of Risk Management with the Advent of ISO 31000 2018 - Descriptive and Content Analyzes. *25th International Conference on Production Research Manufacturing Innovation: Cyber Physical Manufacturing*, August 9-14, 2019. Chicago, Illinois (USA).

Rinaldi, S. M., Peerenboom, J., & Kelly, T. K. (2002). Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems, IEEE*, *21* (6), 11-25. https://doi.org/10.1109/37.969131

Rosa G., & de Toledo, J. C. (2015). Gestão de riscos e a norma ISO 31000: importância e impasses rumo a um um consenso. *V Congresso Brasileiro De Engenharia De Produção*.

Scolobig, A., Prior, T., Schröter, D., Jörin, J., & Patt, T. (2015). Towards people-centred approaches for effective disaster risk management: Balancing rhetoric with reality. *International Journal of Disaster Risk Reduction*, 12, 202-212. https://doi.org/10.1016/j.ijdrr.2015.01.006

Shaw, M. (2020). Resilience in security risk management: Building adaptable systems. *Journal of Risk and Crisis Managemen*t, *13* (3), 65-77.

Shaw, S., & Smith, N. (2010). Mitigating risks by integrating business continuity and security. *Journal of Business Continuity & Emergency Planning*, *4* (4), 329-337. https://doi.org/10.69554/RTYP8319

Speight, P. (2011). Business continuity. *Journal of applied security research*, *6* (4), 529-554. https://doi.org/10.1080/19361610.2011.604021

Teller, J., Kock, A., & Gemünden, H.G. (2014). Risk Management in Project Portfolios Is More Than Managing Project Risks: A Contingency Perspective on Risk Management. *Project Management Journal*, *45* (4), 67-80. https://doi.org/10.1002/pmj.21431

Thamhain, H. (2013). Managing Risks in Complex Projects. *Project Management Journal*, *44* (2), 20-35. https://doi.org/10.1002/pmj.21325

Torabi, S. A., Giahi, R., & Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. *Safety Science*, 89, 201-218. https://doi.org/10.1016/j.ssci.2016.06.015

Tubis, A. A., & Werbińska-Wojciechowska, S. (2021). Risk Management Maturity Model for Logistic Processes. *Sustainability*, *13* (2), 659. https://doi.org/10.3390/su13020659

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. https://doi.org/10.1016/j.resourpol.2014.10.008

Yuwono, M., & Ellitan, L. (2023). Enhancing Company Performance Through Risk Governance Evaluation Based on ERM ISO 31000:2018. *International Conference on Economy. Management, and Business*, 2030-2040.

Dr. sc. Ivana Pokrajčić

Ministarstvo obrane Republike Hrvatske
Sveučilište obrane i sigurnosti "Dr. Franjo Tuđman"
E-mail: ivpokrajcic@gmail.com
Orcid: https://orcid.org/0009-0001-2223-9122

Dr. sc. Tonći Lazibat

Redoviti profesor
Sveučilište u Zagrebu
Ekonomski fakultet
E-mail: tlazibat@net.efzg.hr
Orcid: https://orcid.org/0000-0002-4806-2652

KORELACIJA IZMEĐU PRIMJENE ISO 31000:2018 I RAZINE ZRELOSTI UPRAVLJANJA SIGURNOSNIM RIZICIMA U PODUZEĆIMA IZ SEKTORA NACIONALNE KRITIČNE INFRASTRUKTURE REPUBLIKE HRVATSKE

Sažetak

Primjena norme ISO 31000:2018 i njezina učinkovitost u segmentu nacionalne kritične infrastrukture Republike Hrvatske nije dovoljno znanstveno istražena unatoč činjenici da je njezina primjena u ovom specifičnom segmentu normativno uređena. Metodom multivarijantne statističke analize ovaj članak empirijski istražuje međukorelaciju između primjene norme ISO 31000:2018 i zrelosti upravljanja sigurnosnim rizicima u poduzećima unutar nacionalne kritične infrastrukture Republike Hrvatske. Rezultati istraživanja pokazuju da razina primjene norme ISO 31000:2018 ima značajan i pozitivan utjecaj na zrelost upravljanja sigurnosnim rizicima. Istraživanjem su se također ispitivale razlike između srednjih i velikih poduzeća u poddimenzijama upravljanja sigurnosnim rizicima, a rezultati ukazuju da je zrelost upravljanja sigurnosnim rizicima veća u velikim poduzećama u odnosu na srednja poduzeća unutar nacionalne kritične infrastrukture.

Ključne riječi: ISO 31000:2018, zrelost rizika, upravljanje sigurnosnim rizikom, nacionalna kritična infrastruktura.

JEL klasifikacija: M10, H56, G32, D81.