Information & Security

K. Jakimoski et al.
vol. 55, no. 1 (2024): 32-43
https://doi.org/10.11610/isij.5539

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

A Scalable and Adaptable Asset-Based Cyber Risk Assessment Tool for All Types of Organisations

Kire Jakimoski, (✉) *Mitko Bogdanoski,*[1] *Aleksandar Risteski,*[2] *Dimitar Bogatinov,*[1] *and Goce Stevanoski* [1]

[1] *Military Academy "General Mihailo Apostolski," Skopje, Republic of North Macedonia, https://ma.edu.mk/en*

[2] *Faculty of Electrical Engineering and Information Technologies, Ss. Cyril and Methodius University in Skopje, Republic of North Macedonia, https://feit.ukim.edu.mk*

ABSTRACT:

In today's complex cybersecurity landscape, effective risk management is crucial. This involves fulfilling cyber security controls according to established standards like ISO/IEC 27001, ISO/IEC 27005, the Center for Internet Security's CIS v8.1, etc. Many organisations, particularly smaller ones, lack dedicated cyber risk teams. Therefore, streamlined and automated processes are essential. By implementing a robust Cyber Risk Management Policy, companies can gain a comprehensive understanding of their vulnerabilities. This requires a tool that can efficiently assess risks and identify necessary security controls. The authors of this paper have developed an asset-based tool that precisely evaluates risks based on the status of existing security measures for all types of institutions – from the smallest to large ones.

The proposed tool offers a fast and efficient approach to cyber risk assessment, enabling organisations to proactively mitigate threats and protect their valuable assets. It was developed as a web application that generates precise risk levels according to the answers provided on the status of the implemented cyber security controls. In addition, the tool also gives instructions and suggests safeguards to be implemented.

✉ Corresponding Author E-mail: kire.jakimoski@ugd.edu.mk

ARTICLE INFO:
RECEIVED: 17 Sep 2024
REVISED: 20 Oct 2024
ONLINE: 28 Oct 2024

KEYWORDS:
CIS controls, compliance, cyber risks, risk assessment, security controls, vulnerabilities

Introduction

Cyber Risk Management is very important for all institutions and companies, regardless of size, to protect their reputation and financial stability. Without a solid cyber risk strategy, the probability of unwanted events is increased, and that could negatively impact on the business and reputation of the institutions and companies. Successful cybersecurity risk management produces a systematic approach to the identification, analysis, and assessment of potential threats and vulnerabilities that could compromise information security objectives. Effective protection against cyber security threats can be accomplished only with a thorough understanding of the cyber risks and through the implementation of the appropriate cybersecurity controls.

In the whole concept of cybersecurity risk management, the most important parts are risk assessment and treatment processes. They play an essential role in the implementation and maintenance of a successful ISMS (Information Security Management System). Important world standards that delve into risk assessment and risk treatment processes are ISO/IEC 27001 and ISO/IEC 27005. Organisations should refer to these standards to achieve efficient cybersecurity risk protection and prevent potential cyber threats from materializing. Implementation of consistent, reproducible, and well-defined risk assessment and risk treatment processes is better when following standardized policies and procedures that are well recognized, like the above-mentioned.

One of the key elements of risk treatment is the implementation of security controls. Annex A part of the ISO/IEC 27001 standard[1] gives detailed information about the security controls that should be implemented. CIS (Center for Internet Security) v8.1,[2] also gives detailed information about implementing security controls for different types of organisations and different types of assets. Following the instructions, guidelines, and safeguards of these standards for the implementation of cybersecurity controls improves cybersecurity protection and resilience.

Possessing tools for cybersecurity risk assessment plays essential role in implementing a successful cybersecurity risk management program. In the science community there are already efforts in this field. For example, Benz and Chatterjee [3] suggest cybersecurity assessment tool that is based on the NIST framework. It includes online survey with 35 questions that are based on the five categories in the NIST framework. This tool is focused only on small- to medium-sized enterprises. Santini and coworkers [4] use data-driven approach for cyber risk assessment based on the well-known HTMA (How To Measure Anything) approach including usage of quantitative key risk indicators.

Sukumar, Mahdiraji, and Jafari-Sadeghi proosed a novel approach for cyber risk assessment [5] for SMEs (Small and Medium-sized Enterprises) in online retailing. In their research, 28 cyber-oriented risks are identified specifically for e-tailing SMEs. Hence, this approach is limited only to small e-tailors, and it cannot be applied to other types of SMEs or larger institutions. Russo, with co-authors, [6] proposed a software platform for cyber risk management focused on micro and small enterprises based on the NIST 800-30 standard.

A framework for risk assessment and risk management utilising a decision-analysis-based approach is proposed by Ganin et al.[7] This framework could be complex for organisations that have limited expertise in risk management. Some elements of this framework, like assigning weights to criteria, can include subjective judgments.

A cybersecurity decision-support framework that considers the cost of the cybersecurity breach for the targeted company, the uncertainty in the time needed to exploit a vulnerability, and the optimization of the mitigation measures is proposed by Tsiodra and her co-authors.[8] They presented use cases from the real world utilising the 2020 CWE top 25 software weaknesses as well as Center of Internet Security (CIS) controls.

Carías and coworkers developed the CR-SAT (Cyber Resilience Self-Assessment Tool) for SMEs.[9] This is a valuable tool limited to small and medium-sized companies for assessment of their cybersecurity resilience. It identifies vulnerabilities, prioritizes risks, and includes mitigation strategies.

Ahmed et al.[10] are focused on assessing the risks related to APTs (Advanced Persistent Threats) and supporting informed cyber risk evaluation and characterization. In this context, the MITRE repository is used with known adversarial TTPs (Tactics, Techniques, and Procedures) to define the attack probability and likelihood. Performed assessment is supported by a case study implemented on a health care organisation.

Niemiec and co-authors [11] designed an architecture of the ECHO Multi-sector Assessment Framework that is applicable in many sectors, such as healthcare, energy, maritime transportation, or defence. It evaluates cybersecurity risks in trans-sectoral and inter-sectoral contexts and supports actions for mitigation and resource allocation.

This article is a continuation of our previous research work.[12] In it, Jakimoski et al. presented a tool for cyber risk assessment for small to medium-sized companies considering the types of assets. The application used 20 generic cyber risks mapped with CIS v8 security controls, and it achieved a relatively simple way to assess the cyber risks and map them to well-known security controls in CIS v8. There are also instructions that give information on which security controls from CIS v8 are to be implemented after identifying the risk levels. Furthermore, the cyber risk assessment application visualised the compliance and mapped the presented tool with standards like CIS v8 and ISO/IEC 27001 Annex A Controls.

In this research work, the authors developed a cyber risk assessment tool to serve any type of company, from the smallest to the largest one. It is based on

the CIS v8.1 standard, and it provides fast and accurate cyber risk assessment for each type of asset and company. Considering internationally recognized cybersecurity controls like CIS v8.1, the authors created an application for effective and fast cybersecurity risk assessment that is asset-based and includes every possible type of organisation, from the smallest to the largest one. It also gives a more accurate assessment of the risk levels in comparison to our earlier tool,[12] which gives three—instead of two—options when answering questions.

The remainder of this paper is organized as follows. Section 2 presents the methodology used for developing the cyber risk assessment application. In section 3, the cyber risk assessment application is described in detail. Section 4 concludes this paper.

Methodology for the Design of the Application

Cybersecurity controls and measures are often neglected by many organisations, especially by the small ones that do not employ cybersecurity staff. Usually, system administrators are also handling cybersecurity challenges in the organisations without cybersecurity staff. This oversight often introduces significant vulnerabilities and cyber risks for the companies. A good starting point for this type of organisations that do not have solid cyber defence is to be familiarized with the cyber risks. Having a cyber risk assessment tool that will detect and prioritize cyber risks in these organisations is of great importance for them.

To implement a successful Information Security Management System – ISMS, regular risk assessments and treatments are more than needed in each type of organisation and company. That is why nowadays, every organisation, from small to large, should have solid cyber risk management to identify the risks and take actions with appropriate security controls.

As it was mentioned above, this research is continuation and improvement of our previous work.[12] In this work, a cyber risk assessment tool was developed integrating the risks defined in the well-known risk management platform [13] and CIS controls v8 defined by the Center of Internet Security.[2] In the first phase mapping was done between the risks defined by SimpleRisk [13] and security controls for Implementation Group 1 defined by the Center for Internet Security.[2] So, the user first selects the asset type and then answers the questions for that asset type. Answers were designed with simple “Yes” or “No” options related to the adequate risks and security controls for that asset. After answering the questions, details for the cyber risks and their levels were automatically generated for the appropriate security controls for that specific asset.

The next phase of development of the cyber risk assessment tool involved the design of instructions on what to be done by the user for every risk to decrease the risk level.[12] These instructions were related to the CIS safeguards [2] for the appropriate security controls. In this way, users, in a very user-friendly manner, can review the safeguards that can decrease the generated levels of cyber risks.

In this work, the above methodology is extended. Here the questions, risks and instructions are generated not only for Implementation Group 1, but also

for Implementation Groups 2 and 3 from CIS v8.1. Hence, the application of cyber risk assessment in this research covers not only small but also large and complex organisations and companies.

Furthermore, a novelty in this work is that questions are designed to be answered with "Yes," "No," and "Partially." Answering three options creates better granularity and precision for the cyber risk evaluation. Answers with the option "Partially" have half the weight of the answers with the option "No" when assessing the risk level. By giving three options, we are also not complicating too much this cyber risk assessment process in this research, which aims to produce user-friendly and fast initial cyber risk assessment for all types of companies and institutions.

In the application developed in this research, users first choose the type of organisation (small, medium, or large) and then choose the type of asset. Then, they answer questions for the appropriate type of organisation and asset. The application is developed in a way that all answers must be answered before generating the response. The generated response gives the appropriate risks for that asset with an accurate risk level, as well as instructions and safeguards that should be implemented to decrease the generated risks.

A web application for the cyber risk assessment tool has been developed in this research to increase the user-friendliness of the clients who will use this tool. It uses a combination of popular web technologies. The foundation of the application is formed by HTML, and then CSS is used to style the elements, perform visual presentations, and create a consistent user interface. Dynamic functionality is obtained by JavaScript, which enables interactive features. Furthermore, Bootstrap framework is also used, offering pre-built components and utility classes.

This development methodology gives the tool the power to efficiently generate different risk levels according to the answers to the sets of questions and offer safeguards for solving the risks. The methodology used for developing this tool also relates the tool to the CIS v8.1 standard. So, the instructions and safeguards offered in this tool automatically make the organisation that is using this tool compliant with the CIS v8.1 standard. On the other hand, CIS v8.1 standard is well-mapped with ISO/IEC 27001 standard, so this tool is also in compliance with the ISO/IEC 27001 standard.[14]

Results Obtained with the Cyber Risk Assessment Tool

The risk Matrix presented in Table 1 is used as a basis for defining the risk levels [15] for the developed cyber risk assessment application in this work. It is based on ISO/IEC 27005 standard, and it is widely used for cyber risk management. Risk levels are defined from Very Low (Insignificant) to Very High.

The starting screen of the web-based tool for cyber risk assessment proposed in this work is presented in Figure 1. Here, the user should choose the type of the organisation. As we can see in the starting screen, three options are available: Implementation Group 1 (IG-1), Implementation Group 2 (IG-2), and

Table 1. Cyber Risk Matrix [15]

Risk Matrix		Likelihood Level				
		Very Unlikely - 1	Unlikely - 2	Moderate - 3	Likely - 4	Very likely - 5
Impact Level	Very High - 5	5	10	15	20	25
	High - 4	4	8	12	16	20
	Medium - 3	3	6	9	12	15
	Low - 2	2	4	6	8	10
	Very Low - 1	1	2	3	4	5

Risk Levels:

Very Low (Insignificant)

Low

Medium

High

Very High

Implementation Group 3 (IG-3), representing small (IG-1), medium (IG-2) and large (IG-3) organisations appropriately.

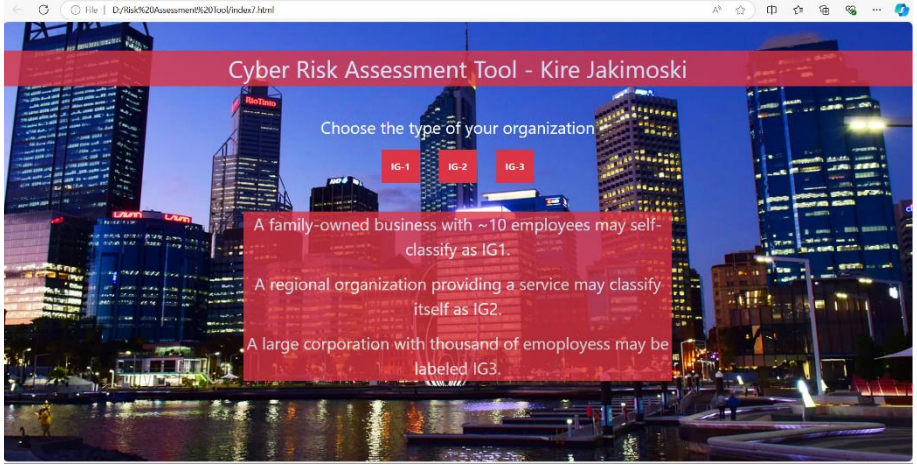

Figure 1: Cyber Risk Assessment Tool: A Starting Screen.

Once the organization type is selected, the user is requested to select the asset type to evaluate the risks. Asset types are classified according to the CIS v8.1 classification: **Devices, Software, Data, Users, Network, and Documentation**. For example, if the client chooses IG-1 type of organization in Figure 1, the next thing presented by the proposed tool is the asset types (Figure 2). In this step, the client selects the asset type that wants to evaluate.

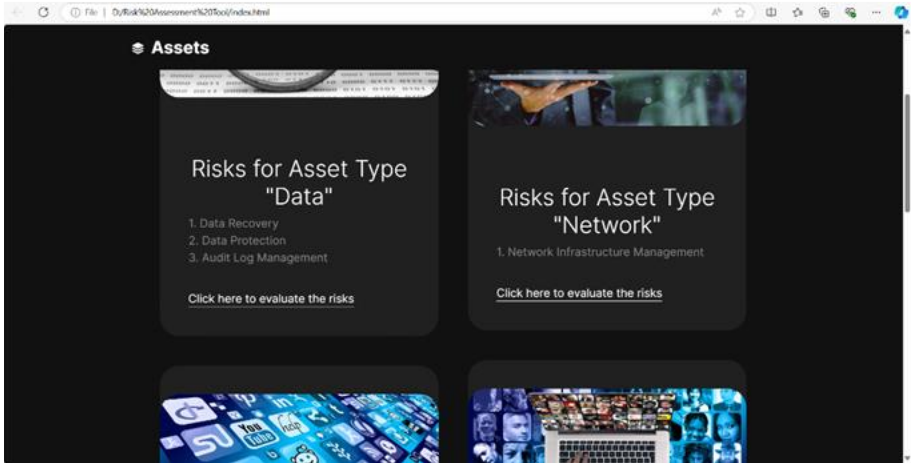

Figure 2: Selecting the Asset Type for Cyber Risk Assessment.

Once the asset type is selected, the user is challenged with sets of questions that should be answered in this phase. For example, if the client selects the asset type Data, the proposed tool presents questions for IG-1 type of organisation for the selected asset type Data (Figure 3).

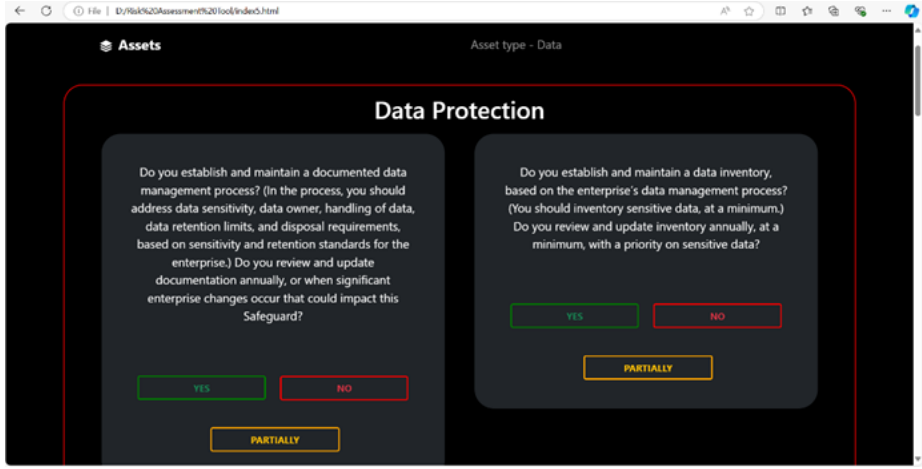

Figure 3: Set of Questions for the Asset Type Data for IG-1.

In the proposed tool, questions could be answered with three options: "Yes," "Partially," or "N," having one option more compared with our previous tool.[12] So, the answer "Partially" is evaluated with weight between the weights of "Yes" and "No" answers. Hence, the results are more accurate for the clients that have partial implementation of the safeguards for the appropriate security control.

For the selected asset type **Data** in Figure 3, according to the IG-1 group in CIS v8.1 standard, there are safeguards for the security controls: "Data Recovery, Data Protection, and Audit Log Management." Hence, the proposed tool presents a set of questions for these three security controls. Part of the questions for the security control Data Protection can be seen in Figure 3. In this example, the client answers the questions with "Yes," "Partially," or "No." After answering all questions for all three security controls in this example for the asset type "Data," the appropriate three risks will be automatically generated. One of these risks is presented in Figure 4 for the security control "Data Protection."

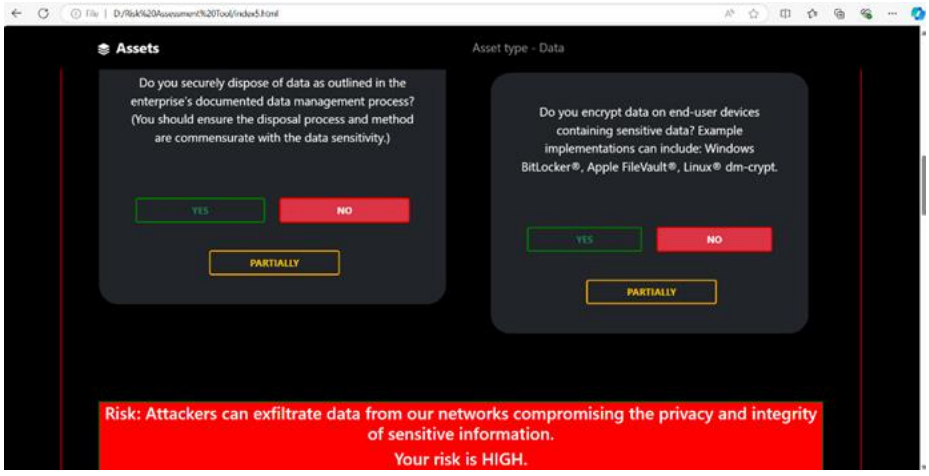

Figure 4: Risk Generation after Answered Questions.

At the same time, instructions are automatically generated under the generated risk with its appropriate level (Figure 5). Instructions are very valuable source of information, because the client gets in the same time risk with its appropriate level, and instructions what safeguards to be implemented to decrease the risk level. Usually, risk appetite for this high level of risk is mitigation, so for high risks it is very important users to start mitigating them as soon as possible.

Therefore, this web application is user-friendly with a solid graphical interface, and it gives comfort and simple control to users who want to make fast and accurate cyber risk assessments. It is of great benefit for all types of organisations that want to implement successful cyber risk management.

Furthermore, this tool is well-mapped with internationally recognized standards like CIS Controls [2] and ISO/IEC 27001 standard.[1] So, it is of great benefit for organisations that want to be compliant with CIS v8.1 and ISO/IEC 27001 standards.

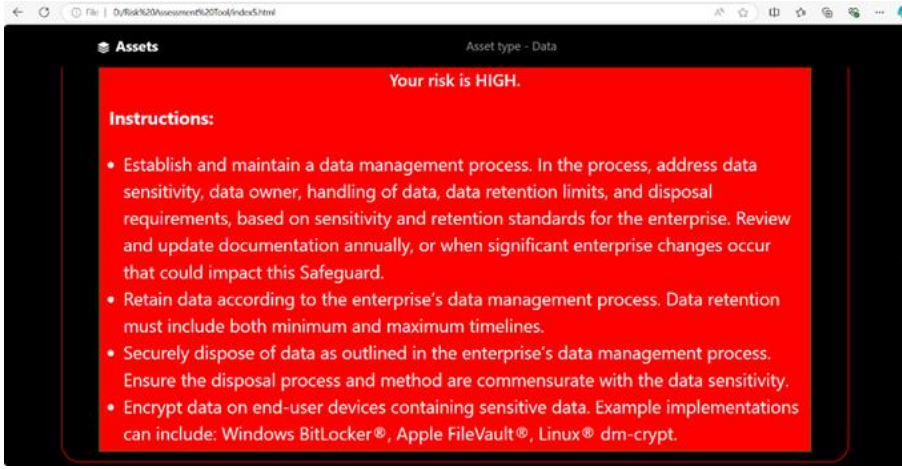

Figure 5: Generation of Instructions under the Generated Risk.

Conclusions

Cyber Risk Management is a very important area nowadays for each type of organisation and company that wants to be well protected from cyberattacks. Cyber risk assessment is one of the crucial parts of the process of cyber risk management. This paper proposes a cyber risk assessment tool built in a web application style for fast and accurate cyber risk assessment based on CIS v8.1 security controls. It can help organisations and companies to familiarise themselves with the potential cyber security dangers in a user-friendly way.

The proposed cyber risk assessment tool gives two types of very important information regarding cyber risk management. First, it gives information about the cyber risks classified by asset types and their appropriate risk levels. Then, it also gives information on which safeguards to be taken to decrease the level of the risk. This tool is designed to be adapted for all types of organisations – from small ones to large corporations. It is of great benefit for cyber security teams in organisations that deal with cyber risk management. It is also of special benefit for organisations that do not have cyber security teams on their staff and want to understand the dangers of cyberattacks for them.

What makes this proposed cyber risk assessment application unique is the asset-based approach when assessing cyber risks. Generated risks are classified by asset type, so users of this tool gather information about cyber risks with accurate risk levels just for that particular asset type. For example, if they want to know the risks for the asset type **Software**, they will choose this asset type in the proposed application before answering the questions and get the risks with appropriate risk levels and instructions just for that asset type.

Future work for this research should be an evaluation of the asset value because not all assets in one asset type have the same value for the organisation. Some of these assets store or process more highly classified information, and

some – lower level ofclassified information. This results in different asset values that could impact the potential risk level of the assets that belong to the same asset type.

Acknowledgment

The completion of this research paper would not have been possible without the support of Red Piranha Limited, Australia's leading developer, manufacturer, and exporter of cutting-edge cybersecurity solutions.

References

[1] ISO, "ISO/IEC 27002: 2022 Information security, cybersecurity and privacy protection – Information security controls," Edition 3, 2022, https://www.iso.org/standard/75652.html.

[2] CIS (Center for Internet Security), "Critical Security Controls, Version 8.1," https://www.cisecurity.org/controls/, accessed August 30, 2024.

[3] Michael Benz and Dave Chatterjee, "Calculated risk? A cybersecurity evaluation tool for SMEs," *Business horizons* 63, no. 4 (2020): 531-540, https://doi.org/10.1016/j.bushor.2020.03.010.

[4] Paolo Santini, Giuseppe Gottardi, Marco Baldi, and Franco Chiaraluce, "A Data-Driven Approach to Cyber Risk Assessment," *Security and Communication Networks* 2019, no. 1 (2019): 6716918, https://doi.org/10.1155/2019/6716918.

[5] Arun Sukumar, Hannan Amoozad Mahdiraji, and Vahid Jafari-Sadeghi, "Cyber Risk Assessment in Small and Medium-Sized Enterprises: A Multilevel Decision-making Approach for Small e-Tailors," *Risk Analysis* 43, no. 10 (2023): 2082-2098, https://doi.org/10.1111/risa.14092.

[6] Pietro Russo, Alberto Caponi, Marco Leuti, and Giuseppe Bianchi, "A Web Platform for Integrated Vulnerability Assessment and Cyber Risk Management," *Information* 10, no. 7 (2019): 242, https://doi.org/10.3390/info10070242.

[7] Alexander A. Ganin, Phuoc Quach, Mahesh Panwar, Zachary A. Collier, Jeffrey M. Keisler, Dayton Marchese, and Igor Linkov, "Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management," *Risk Analysis* 40, no. 1 (2020): 183-199, https://doi.org/10.1111/risa.12891.

[8] Maria Tsiodra, Sakshyam Panda, Michail Chronopoulos, and Emmanouil Panaousis, "Cyber Risk Assessment and Optimization: A Small Business Case Study," *IEEE Access* 11 (2023): 44467-44481, https://doi.org/10.1109/ACCESS.2023.3272670.

[9] Juan Francisco Carías, Saioa Arrizabalaga, Leire Labaka, and Josune Hernantes, "Cyber Resilience Self-assessment Tool (CR-SAT) for SMEs," *IEEE Access* 9 (2021): 80741-80762, https://doi.org/10.1109/ACCESS.2021.3085530.

[10] Mohamed Ahmed, Sakshyam Panda, Christos Xenakis, and Emmanouil Panaousis, "MITRE ATT&CK-driven Cyber Risk Assessment," In *Proceedings of the 17th*

International Conference on Availability, Reliability and Security, 2022, pp. 1-10, https://doi.org/10.1145/3538969.3544420.

[11] Marcin Niemiec, Salvatore Marco Pappalardo, Maya Bozhilova, Nikolai Stoianov, Andrzej Dziech, and Burkhard Stiller, "Multi-sector Risk Management Framework for Analysis Cybersecurity Challenges and Opportunities," In *International Conference on Multimedia Communications, Services and Security* (Cham: Springer International Publishing, 2022), 49-65.

[12] Kire Jakimoski, et al, "Cyber Risk Management Tool for Improving the Cybersecurity Maturity in the Companies," *13th International Conference on Applied Internet and Information Technologies, Bitola, Republic of North Macedonia,* 2023, pp. 30-36.

[13] SimpleRisk, "Comprehensive GRC Solution," https://www.simplerisk.com/, accessed September 01, 2024.

[14] Center for Internet Security, "CIS Controls v8.1 Mapping to ISO/IEC 27001:2022," https://www.cisecurity.org/insights/white-papers/cis-controls-v8-1-mapping-to-iso-iec-27001-2022, accessed September 04, 2024.

[15] Susana Patiño, Edgar Fernando Solís, Sang Guun Yoo, and Rubén Arroyo, "ICT risk management methodology proposal for governmental entities based on ISO/IEC 27005," In *2018 International Conference on eDemocracy & eGovernment (ICEDEG)*, IEEE, 2018, pp. 75-82.

About the Authors

Kire **Jakimoski,** D.Sc., is a Full Professor with over 22 years of experience in the fields of Computer Networks and Cybersecurity. He has worked in state and private organisations and universities as a signals officer, advisor for accreditation of CIS, advisor for cryptographic systems, research and teaching assistant, assistant professor, associate professor, full professor, expert witness, and Cybersecurity Consultant. He is currently a full professor in the Institute for Cybersecurity and Digital Forensics at the Military Academy "General Mihailo Apostolski"

- Skopje, University Goce Delcev, Stip, Republic of North Macedonia. https://orcid.org/0000-0002-4969-8054

Mitko **Bogdanoski**, D.Sc, Full Professor, Colonel, Dean, is an experienced practitioner with over 24 years in IT and cyber/information security, consultancy, education and training. He holds a doctoral degree in cyber/ information security (covering the areas of IT, cyber/information security, cybercrime, electronic surveillance, and protection of classified information. He regularly engages as a cyber security key/ subject matter expert/ consultant, and contributes to various EU, NATO, DCAF, and RACVIAC projects and activities. Author of many publications, including five books, several book chapters published by international publishers, and more than 100 papers/ articles published in reputable international journals/conference proceedings.
https://orcid.org/0000-0002-8098-1421

Aleksandar **Risteski**, D.Sc, Full Professor, received his B.Sc., M.Sc., and Ph.D. degrees in telecommunications from the University Ss. Cyril and Methodius, Skopje, Macedonia in 1996, 2000, and 2004, respectively. He is currently a professor at the same university's Faculty of Electrical Engineering and Information Technologies. In 2001, 2003 and, 2004, he had several internships at IBM T.J. Watson Research Center, Yorktown Heights, NY, USA, where he worked towards his PhD degree. His research interests are in the fields of cybersecurity, blockchain technologies, ICT for energy efficiency, optical communications, and coding theory. He is an author and co-author of more than 100 journal and conference papers, several book chapters, and one book.
https://orcid.org/0000-0001-9485-6683

Dimitar **Bogatinov**, Dr.Sc., Associate Professor, is a renowned cybersecurity expert with over 15 years of experience in education, cybersecurity, and project management. He currently serves as the Head of the Department for Cyber Security and Digital Forensics Training, a leading national training provider for cybersecurity in North Macedonia. Dr. Bogatinov has led numerous high-impact projects funded by NATO, the European Union, and other international organisations. His work includes developing national cybersecurity strategies, coordinating large-scale cybersecurity exercises, and leading cross-border initiatives to strengthen digital resilience.
https://orcid.org/0000-0001-6263-543X

Goce Stevanoski, M.Sc., Research Associate, worked for the military at the operational level for 18 years in various activities and projects regarding policy development, designing and implementing IT network infrastructures, planning, procurement, and implementation of IT security systems, and training the military personnel. He has participated in many multinational exercises on computer networks and cybersecurity. An author of articles related to computer science and cybersecurity issues. Doctoral student at the Faculty of Electrical Engineering and Information Technologies, Skopje, focusing on Machine Learning for Cyber Security. https://orcid.org/0009-0003-8532-0299