Vilniaus
universitetas

Vilniaus
universitetas

Oleksii Chalyi
First Year Part-Time Student
Start year – 2025.10.01. End year – 2031.09.30

Artificial Intelligence-Based Solution for Improving Cybersecurity Risk Management

Supervisor: Doc. Dr Kęstutis Driaunys

Table 1. Doctoral study plan

Vilniaus universitetas

Year of study	Exams	
	Plan	Completed
I (2025/2026)	**1**	
II (2026/2027)	1	
III (2027/2028)	2	
IV (2029/2030)		
Total:	4	0

Table 1. Doctoral study plan

Vilniaus universitetas

Year of study	Participation in conferences				Publications					
	International		National		With citation index			Without citation indicator		
	Plan	Completed	Plan	Completed	Plan	Completed	Condition	Plan	Completed	Condition
I (2025/2026)	**1**				**1**	**1**	**Published**			
II (2026/2027)	1				1					
III (2027/2028)					1					
IV (2029/2030)					1					
Total:	2				4	1				

Table 2. Reporting semester of studies

Vilniaus universitetas

Exams 2025/2026 (1st semester)		
Plan	**Credits (ECTS)**	**Condition**
Introduction to Research Data Management	0.15	Completed, waiting for certificate in autumn 2026
The FAIR Data Principles	0.55	Completed, waiting for certificate in autumn 2026
Data Repositories and Data Papers	0.4	Completed, waiting for certificate in autumn 2026
Getting started with the MIDAS Archive	0.4	Completed, waiting for certificate in autumn 2026
Preparing a Data Management Plan	0.5	Completed, waiting for certificate in autumn 2026
Scientific Information Retrieval: Databases and AI Tools	0.2	Completed, waiting for certificate in autumn 2026

Publications 2025/2026 (First semester)			
Plan	**Completed**	**Condition**	**Publication type**
Electronics	Chalyi, O., Driaunys, K., Grigaliūnas, Š., & Brūzgienė, R. (2026). Standard-Oriented	submitted (first reviews received): date 2026.03.03	Research Article. JIF: 2.6

Table 2. Reporting semester of studies

Vilniaus universitetas

Publications 2025/2026 (First semester)			
Plan	**Completed**	**Condition**	**Publication type**
Electronics	Chalyi, O., Driaunys, K., Grigaliūnas, Š., & Brūzgienė, R. (2026). Standard-Oriented Architecture for AI-Powered Information Security Risk Management. *Electronics, 15(6)*, 1282. https://doi.org/10.3390/electronics15061282	Published	Research Article. JIF: 2.6

Table 3. Stages of research and dissertation preparation

Vilniaus universitetas

Job title		Fulfilment period		Notes
		From	To	
1.	Review and analysis of scientific research related with the theme of doctoral thesis (in Lithuania and abroad):			
1.1.	Analysis of international standards for information security risk management.	2025 y. IV quarter	2026 y. I quarter	An analysis and comparison of eight international standards for ISRM was prepared
1.2.	Review of previous approaches to automating information security risk management.	2025 y. IV quarter	2026 y. III quarter	An review of previous approaches to automating ISRM was prepared

Research Object, Aim and Objectives

Vilniaus universitetas

The research **object** of this study is the process of Information Security Risk Management (ISRM) and the methodologies for its automation.

The main **aim** of this research is to develop a novel solution for the automation and semi-automation of Information Security Risk Management utilizing artificial intelligence, specifically to enhance the efficiency and accuracy of the risk assessment and risk treatment processes.

To achieve this aim, the following **objectives** were formulated:

1) To analyze related works and existing approaches concerning the automation and semi-automation of ISRM.
2) To conduct a comparative analysis of international ISRM standards to establish a foundational framework for the proposed solution.
3) To design the architecture of the proposed automated (or semi-automated) ISRM system.
4) To develop a Multi-LLM decision-making module integrated into the risk management workflow.
5) To implement a prototype of the proposed ISRM system.
6) To test and validate the proposed system, evaluating its performance and results against traditional ISRM methods.

Scientific results obtained during the semester

Vilniaus universitetas

Table 4. Summary of Related Works

Reference	Approach	Key Findings & Limitations
D. G. Jakka et al. (2022)	AI adoption survey	+ Showcased corporate demand for AI cyber risk frameworks. - Lacks practical deployment or technical models.
M. Yazdi et al. (2024)	LLMs vs. Human specialists	+ Evaluated AI precision in risk assessment vs. humans. - Misses human nuance; ignores algorithmic bias and accountability.
A. Bhardwaj et al. (2024)	ML (SVM, PCA, Neural Networks)	+ Strong predictive precision for financial vulnerabilities. - Lacks applicability to information security contexts.
S. S. Dasawat & S. Sharma (2023)	Theoretical AI integration	+ Highlighted AI for faster threat identification. - Purely theoretical; missing concrete architectural propositions.
M. Sterbak et al. (2021)	ISO/IEC 2700x automation	+ Pinpointed specific risk management phases suitable for automation. - Full automation fails without AI (struggles with IT asset discovery).
I. Hamid & M. Rahman (2025)	AI/ML/DL review	+ Articulated the necessity of human-in-the-loop AI integration. - Lacks actionable blueprints for standard-aligned AI.
N. Mohamed (2023)	Statistical survey	+ Revealed algorithm opacity and bias as primary adoption hurdles. - Offers no governance mechanisms for ethical, unbiased models.

Scientific results obtained during the semester

Vilniaus universitetas

Conclusions of Related Works Analysis

Generic AI Limitations: While AI is vital, general LLMs (e.g., ChatGPT-4) still lack the precision and nuance of human experts in core risk estimation.

The Cybersecurity Gap: Current AI methods predominantly target financial risks; reliable, practical implementations specifically for InfoSec are missing.

Barriers to Full Automation: End-to-end automation remains unfeasible due to AI "transparency deficits," potential biases, and the need for manual oversight.

Study Motivation: These fragmented efforts drive the need for the unified, standard-oriented automation architecture proposed in this work.

Scientific results obtained during the semester

Vilniaus universitetas

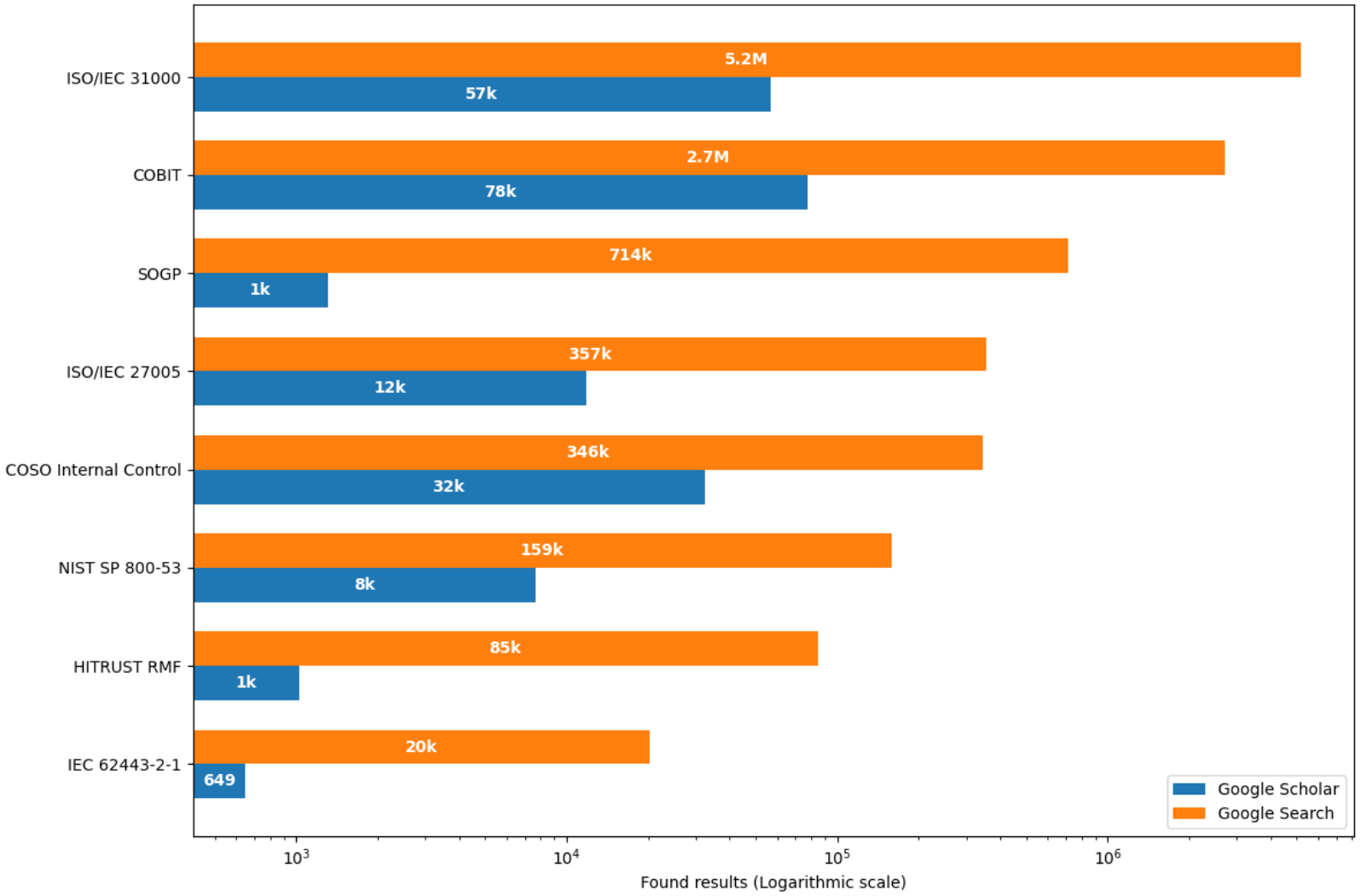

Figure 1. Popularity of risk management frameworks based on google scholar and search results.

Scientific results obtained during the semester

Vilniaus universitetas

Table 5. Comparative evaluation of ISRM standards by key criteria.

Framework	Structural Granularity	Domain Relevance	Potential for Automation	Lifecycle Completeness	Compliance and Audit Support	Final score
COBIT 2019	3	3	2	5	5	3,6
ISO/IEC 27005	5	5	4	5	4	4,6
ISO 31000	3	3	4	5	5	4
SOGP	1	3	2	3	2	2,2
NIST SP 800-53	4	4	3	5	5	4,2
IEC 62443-2-1	3	4	3	4	3	3,4
COSO IC-IF	4	3	2	4	3	3,2
HITRUST RMF	4	3	3	4	3	3,4

Scientific results obtained during the semester

Vilniaus universitetas

Clear Winner: ISO/IEC 27005 achieved the highest overall score (4.60), demonstrating maximum structural detail, ISRM focus, and process lifecycle coverage.

AI & Automation Ready: It is the most technically actionable framework (Automation Readiness score of 4), making it uniquely suited for algorithm-driven implementation.

Runners-Up Limitations: While NIST SP 800-53 (4.20) and ISO 31000 (4.00) excel in compliance, they lack the specific technical granularity and automation readiness required for AI-driven generative reasoning.

Final Conclusion: ISO/IEC 27005 provides the optimal balance of methodology and technical adaptability, making it the perfect baseline for the proposed AI-driven ISRM architecture.

Work plan for the next semester

Vilniaus universitetas

During the upcoming semester, the research will focus on the architectural design and functional specifications of the proposed automated (or semi-automated) ISRM system. The planned activities include:

- Investigating and comparing various types of information security risks to determine specific approaches for their evaluation.
- Defining the precise data inputs and outputs required for the integration and training of the Multi-LLM decision-making module.
- Preparing and submitting a conference paper based on these architectural findings to the International Conference on Information and Software Technologies (ICIST) 2026.

Vilniaus
universitetas

Vilniaus
universitetas

CONTACTS

Oleksii Chalyi
oleksii.chalyi@knf.vu.lt