STATEMENT REPORT

under the procedure for acquisition of the educational and scientific degree "Doctor" on the topic "The impact of regulation (eu) 2019/881 (Cybersecurity act) on the expansion of cybersecurity certifications"

by candidate Racheli Menda Shabat

in the scientific field 4. Natural Sciences, Mathematics and Informatics

professional field 4.6. "Informatics and Computer Sciences"

Faculty of Social, Economic and Computer Sciences, Doctoral program "Information Systems and Technologies, Informatics and Computer Sciences", Varna Free University "Chernorizets Hrabar"

The statement report has been prepared by Prof. Dr. Vladimir Todorov Dimitrov, professor in professional filed 4.6. Informatics and Computer Sciences, at the Faculty of Mathematics and Informatics of Sofia University "St. Kliment Ohridski", as a member of the scientific jury for the defense of this DSc Thesis according to Order 256/30.04.2026 of the Rector of the Varna Free University "Chernorizets Hrabar".

1. General characteristics of the dissertation thesis and the presented materials

The documents submitted by the candidate comply with the requirements of ADASRB and RAADASRB for this procedure.

The submitted dissertation is 213 pages long. It consists of an introduction, three chapters, a conclusion, a list of references and appendix. The text is written in English. It is illustrated by 29 tables and 21 figures. The references

include 187 sources in English, 123 of which are available via Internet including these with DOI.

At the end of each chapter, the author draws conclusions and summaries on the topic under consideration.

Chapter one is dedicated to the topic of certifications in the field of cybersecurity, the regulatory framework in the EU and the place of private certification bodies. In conclusion, the author defends the thesis that the regulatory framework in the EU provides for the presence of private certification bodies, which would improve the scalability of the certification process.

Chapter two analyzes models for evaluating certification schemes: HoQ, FAHP and MPSBM. Based on the analysis, the author proposes PSF - a model for evaluating certification schemes offered by CAB, as well as a model for selecting a PSS certification scheme. The two models are integrated and are the author's original development.

Chapter three is dedicated to the implementation of the proposed PSF and PSS models. The application of the models is illustrated.

The conclusion describes in detail the characteristics of the two integrated models at the micro and macro levels and provides a reasoned answer to the research tasks. The contributions of the dissertation are presented.

After the verification, I find that the candidate meets the minimum national requirements for acquiring a PhD degree in professional field 4.6. "Informatics and Computer Sciences".

2. Evaluation of the candidate's results and contributions

The research problem for the study is formulated in the dissertation with the following questions:

1. Quality Assurance – Can private CABs ensure the same level of rigorous evaluation as public schemes?
2. Regulatory Compliance – Does this shift increase the risk of non-compliance with cybersecurity regulations?
3. Harmonization – How can private and public schemes be aligned to ensure mutual recognition within the EU?
4. Legitimacy and Trust – How can private schemes be recognized without undermining government authority?
5. Market Adoption and Scalability – How can the growth of certified IoT products be supported while addressing concerns that cybersecurity compliance may reduce product performance and detain their development and market adoption?
6. Decision Making for CAB selection: In light of the challenges outlined above, which criteria and methodological approaches should guide the decision to engage a private CAB, so as to ensure the successful completion of the certification process?

The aim of the dissertation is "to develop scientifically grounded, harmonized models that facilitate the prediction of successful integration of private certification schemes within the broader certification ecosystem. Furthermore, the dissertation aims to formalize these models into a robust decision-making framework for Conformity Assessment Body (CAB) selection".

The research tasks set for the dissertation are:

1. Evaluate quality and effectiveness – compare the assurance levels, impartiality, and cost-effectiveness of private versus public certifications, assessing the influence of commercial incentives.
2. Analyze regulatory impact – investigate the implications of expanding private CAB involvement and propose measures to ensure alignment with CSA, RED, and CRA requirements.
3. Develop harmonization strategies - explore mechanisms for integrating public and private schemes within a coherent, EU-wide certification ecosystem.
4. Investigate trust mechanisms - identify methods to strengthen stakeholder confidence through transparency, oversight, and accountability frameworks.
5. Assess market adoption and scalability - analyze how private certifications influence uptake of secure IoT products without hindering innovation or performance.
6. Formulate a CAB decision-making model - define structured selection criteria, balancing competence, impartiality, cost, and regulatory compliance.

The author's thesis is that the recognition of private certification bodies (CABs) within the EU as legitimate entities for cybersecurity certification of IoT products (CABs under the CSA/RED/CRA regulation) can increase the scalability and efficiency of the certification process without compromising the quality, productivity or harmonization of products.

The contributions of the study are formulated at three levels – macro level and micro level and integration as follows:

Macro-level Contribution: Private Scheme Forecasting (PSF) Model

1. An original model for assessing the reliability of private cybersecurity certification schemes has been developed.
2. The PSF model identifies three key conditions for effective private certification: innovative risk-based assessment strategies; realistic scenario building that balances comprehensiveness and plausibility; and systemic integration of technological and methodological components.
3. A high level of compliance does not have to undermine competitiveness, the PSF model presents certification as a simultaneous factor for building trust and good market performance.

Micro-level Contribution: Private Scheme Selection (PSS) Model

4. An algorithmic model has been developed to assist IoT device manufacturers in selecting a Conformity Assessment Body (CAB). The PSS model integrates fuzzy logic and optimizes it through the Fuzzy Prioritization Method (FPM) to transform expert linguistic assessments into robust quantitative priorities. In this way, the model accounts for uncertainty and subjectivity more effectively than conventional Analytic Hierarchy Process (AHP) methods.
5. Six structured steps are defined, criteria definition, pairwise comparisons, fuzzy transformation, geometric mean optimization, fuzziness removal, and decision-making application. The PSS model creates a transparent, reproducible, and validated process for CAB selection, with trust and enforcement as the dominant criteria.
6. The PSS model is implemented through a simple Excel-based tool.

Integrated contribution: linking PSF and PSS

7. A strategy is proposed for harmonizing private and public schemes within the European Union framework. Through a two-perspective framework that links strategic forecasting (PSF) with operational execution (PSS), a closed system is formed in which macro-level forecasting supports micro-level decision-making, and micro-level methodology validates macro-level assumptions.

The contributions of the dissertation are described and defended in the relevant chapters of the dissertation.

I find the obtained results to be original achievements of the author.

3. Critical notes and recommendations

The presentation of the material is verbose. It is possible to shorten the text without losing content.

One of the main reasons for avoiding cybersecurity certification and even ignoring cybersecurity itself in IoT devices is the increase in the cost of the product. Adding this factor to the study would fill in the picture. The focus here is on functionality and speed, but adding price to the study can improve the content of the study.

4. Conclusion

Having become acquainted with the dissertation work presented in the procedure and the accompanying scientific results and based on the analysis of their significance and the scientific and scientifically applied contributions contained therein, I confirm that the scientific achievements meet the requirements of ADASRB and RAADASRB for the candidate to acquire the the educational and scientific degree "Doctor" in the scientific field 4. Natural

Sciences, Mathematics and Informatics and professional field 4.6 Informatics and Computer Sciences. In particular, the candidate meets the minimum national requirements in the professional field and no plagiarism has been established in the scientific works presented in the procedure.

Based on the above, I recommend that the scientific jury award **Racheli Menda Shabat** the educational and scientific degree "Doctor" in the scientific field 4. Natural Sciences, Mathematics and Informatics and professional field 4.6 Informatics and Computer Sciences.

Sofia, 31 May 2026

Sign:

(Prof., Dr. Vladimir Dimitrov)