REVIEW

by Prof. Dr. Eng. Naiden Valkov Nenkov
Shumen University "Bishop Constantine of Preslav"
regarding: Dissertation for the award of the educational and scientific degree "DOCTOR" **to Raheli Menda Shabat**
on the topic: **"Impact of Regulation (EU) 2019/881 (Cybersecurity Act) on the expansion of cybersecurity certifications"**

Professional field: **4.6 "Informatics and Computer Science" Doctoral Program: "Information Systems and Technologies, Informatics and Computer Science"**

1. Introductory information about the doctoral student and the procedure

The presented dissertation was developed by **Raheli Menda Shabat**, a doctoral student in independent training at the Department of Computer Science of the VFU "Chernorizets Hrabar". Scientific supervisors are Assoc. Prof. Dr. Galina Mileva and Assoc. Prof. Dr. Zlatogor Minchev. The dissertation was successfully discussed and sent for defense before a scientific jury.

I do not know Racheli Menda Shabat personally, but from the documents provided to me, the curriculum vitae (CV), I can note her active presence and participation in the field of the topic considered in the dissertation work as a practical expert and specialist.

The PhD candidate states that she has been involved in cybersecurity certification for over 30 years on semiconductor projects and more than 20 years in the development, testing and certification of cybersecurity products. She is currently the Vice President of Cybersecurity Certification at Winbond Corporation, leading product certification programs in compliance with global standards and regulatory requirements for security and safety. She is an active contributor to international standards and regulatory frameworks (ISO/IEC), participating in committees and working groups shaping regulations for cybersecurity, secure connectivity and product resilience.

She also participates as a technical expert member of the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC) contributing to the security requirements for the Radio Equipment Directive (RED) and the Cyber Resilience Act (CRA). She has been involved in security standardization since 2000, including early definitions of Trusted Platform Modules (TPM). She also holds leadership positions at Eurosmart and GlobalPlatform, leading technical groups that advance cybersecurity standards and regulatory readiness.

2. Relevance and importance of the topic

The topic is extremely relevant for the IoT (Internet of Thinks - Internet of Things) sector, which is growing exponentially every year with the inclusion of many new devices for smart homes, cities and machines. The international standard **ISO/IEC 15408** is known as **Generic Criteria for Information Technology Security Assessment** , which assesses the security of their products by checking whether they meet specific, recognized security criteria. The standard faces difficulties in serving this large market due to its dependence only on public authorities. The research in the dissertation highlights the critical gap in the literature on the integration of **private conformity assessment bodies (CABs)** under the new EU regulatory architecture (CSA, RED, CRA).

The previously mentioned "first-hand" expertise of the doctoral student transforms the analysis of standards such as **EN 18031** in the dissertation from a theoretical overview into a professional assessment with high applied value.

3. General characteristics and structure of work

218 pages long , structured in an introduction, three chapters, a conclusion and appendices. The scientific apparatus includes **29 tables, 21 figures and a bibliography of 187 literary sources**. The structure is logical and consistent, leading from theoretical analysis to the development of innovative models and their empirical verification.

4. Research methodology

The author applies a multidisciplinary methodology combining regulatory analysis, case studies, and advanced quantitative modeling. The selected methods – **multiphase scenario modeling** (for the macro level) and **Fuzzy Prioritization Method (FPM)** for the micro level – are high-tech tools adequate for managing uncertainty and subjectivity in complex cybersecurity systems.

5. Analytical assessment of the content of the work

Chapter one examines the regulatory environment and standards, providing a detailed classification of **20 international and regional standards** (including SESIP and EN 18031).

The analysis of the inclusion of private schemes in the European cybersecurity certification framework marks a key and controversial regulatory change. This is driven by the need for scalability, flexibility, and industry coherence in rapidly evolving sectors such as IoT. The main challenges are analyzed and ways to address them are shown. The main conclusion is that the EU is moving towards **a hybrid ecosystem**, in which private Conformity Assessment Bodies (CABs) become vital due to the capacity constraints of state structures. The value here lies in identifying trust and legitimacy as central issues in their establishment.

Chapter two: A model for successful micro- and macro-level adoption in private schemes – evaluation of alternative models and development of a new model. Two original tools are proposed. **PSF (Private Scheme Forecasting** - Private Scheme Forecasting), represents a significant macro-level innovation in the dissertation work offering a scientifically sound framework for predicting the systemic success of the adoption of private certification schemes in the IoT ecosystem. The predictive value of the PSF model is expressed in several critical directions that are essential for the industry and regulators: **identification of viable certification paths** where the cross-compatibility analysis (CCM) shows that about 20% (65 scenarios) of the theoretically possible combinations are

practically plausible; **technological prioritization** where the model predicts that high levels of security require a transition to hardware-oriented architectures such as nanotechnology and embedded software, supported by an independent third-party assessment; **revealing hidden risks** through 3D modeling of the dimensions in "Key Protection" and "Secure Storage" are identified as falling into the "critical zone" and **validating market viability** .

The PSS (**Private Scheme Selection**) model reforms the perception of certification, presenting it not as an obstacle to competitiveness, but as a tool for building trust, which is validated through real products (Winbond W75F, etc.) and confirms the prognostic assumptions - certified products achieve higher security without degrading performance. The doctoral student concludes that these models eliminate the subjectivity of expert judgment.

Chapter three titled: A model for successful adoption of a private scheme in a micro and macro system - realization of the model and implementation of the results. Here is a step-by-step description of the two models proposed by the doctoral student: Private Scheme Forecasting Model (PSF) and the Private Scheme Selection Model (PSS). The two models described are built on the same theoretical aspects and mathematical foundations. The use of fuzzy set theory and its application in this work leaves an incredibly good impression. The verification and validation of the models use practical examples from the good experimental work of the doctoral student with real IoT components. The results are shown with tables and graphs for each model. The comparative analysis of certified products such as Winbond W75F against non-certified analogues in the three selected IoT categories shows that these results are statistically significant ($p < 0.001$) and prove that certification increases security without degrading performance. This provides empirical evidence that refutes the main market barrier to this type of certification.

6. **Major scientific and applied scientific contributions.**

Development of a PSF model (Macro level).

The model is based on 324 scenario combinations, of which only **20% are identified as practically plausible** . **3D sensitivity analysis** maps risks, revealing hidden threats in areas such as “Key Protection” and “Secure Storage”, which are critical for system resilience.

Mathematical justification of the PSS model (Micro level) .

The use of triangular fuzzy numbers (TFN) and the centroid method allow the transformation of subjective opinions into specific weights: **Trust (38%)** , Enforcement (23%), Legitimacy (16%), Quality (11%) and Efficiency (11%). The mathematical reliability is proven with a Consistency Coefficient **CR = 0.0195** (significantly below the threshold of 0.10).

Integrated macro-micro framework: A closed system is created in which strategic foresight informs operational decisions for CAB selection, serving as a roadmap for harmonizing private and public schemes in the EU.

7. **Personal contribution and publication activity**

Rahel Menda-Shabbat's personal contribution is undeniable, based on her leadership roles in **Eurosmart and GlobalPlatform**. Publication activity includes **seven (**7) **publications** in Springer, BISEC, and AdComSys. The scientometric indicators of the doctoral student fully meet the minimum national and university requirements.

8. **Evaluation of the extended abstract**

The abstract has been prepared in accordance with the requirements and **accurately reflects** the main content and contributions of the dissertation work. It may be supplemented with a little more information reflecting the theoretical models themselves and their relationship to the results shown.

9. Critical notes and questions

My note to the abstract is that there is an opportunity to show in more detail some of the theoretical justifications of the developed models and their connection with the results. This way, the doctoral student's theses in the dissertation will be even more convincingly justified and defended before the readers of this short form.

It would be good to avoid some inaccuracies in the layout of tables and text when moving it between pages.

I recommend that in future work, the doctoral student explore in more detail the impact of **artificial intelligence** on automated certification processes, identified in the paper as a potential threat or opportunity.

Question for the PhD student: How can the proposed **PSF** and **PSS** models adapt to the concept of "continuous security monitoring" throughout the product lifecycle, required by the Cyber Resilience Act (CRA)?

10. Opinion on the presence of plagiarism

I do not find any plagiarism in the dissertation . The author has strictly observed ethical norms and has correctly cited the sources used.

11. Conclusion

Racheli Menda Shabat's dissertation represents an independent, complete, innovative, and scientifically sound study with a significant applied effect for European certification practice. The critical remarks do not belittle the achieved results and their relevance.

All this gives me full reason to propose to the esteemed scientific jury to evaluate the dissertation with **a POSITIVE EVALUATION** and to award Raheli Menda Shabat the educational and scientific degree **"DOCTOR"** in professional field 4.6 "Informatics and Computer Science".

Date: 05.06.2026 **Reviewer:** NAYDEN VALKOV NENKOV Digitally signed by NAYDEN VALKOV NENKOV Date: 2026.06.05 10:19:12 +03'00'

Prof. Dr. Eng. Naiden Nenkov