Neapolis University Pafos, Cyprus
AI-2-TRACE-CRIME
Jean Monnet Center of Excellence
Co-funded by the European Union

# Policy Brief

*Strengthening Cybersecurity:*

*A European Common Criteria-based Certification Scheme*

NUP Jean Monnet / UNESCO Policy Briefs

22/2024

With the support of the Erasmus+ Programme of the European Union

Neapolis University Pafos
UNESCO Chair in Human Development, Security & the Fight against Transnational Crime and Illicit Trafficking in Cultural Property

unesco Chair

The NUP Jean Monnet / UNESCO working papers and policy briefs can be found at:

https://www.nup.ac.cy

Publications in the Series should be cited as:

AUTHOR, TITLE, NUP UNESCO/JEAN MONNET WORKING PAPER or POLICY BRIEF NO. x/YEAR [URL]

Copy Editor: G. Pavlidis

Neapolis University Pafos, School of Law

Pafos, 8042, Cyprus

*Frontpage picture: Generated with AI (Bing Image Creator)*

*The support of the European Commission and of UNESCO for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors; the European Commission and UNESCO cannot be held responsible for any use which may be made of the information contained therein.*

# *Strengthening Cybersecurity:*

# *A European Common Criteria-based Certification Scheme*

**Executive Summary:**

*This policy brief outlines the new European regulation implementing a cybersecurity certification scheme based on the EU Common Criteria (EUCC). This scheme aligns with the existing European cybersecurity certification framework established in Regulation (EU) 2019/881. The EUCC builds upon the existing Mutual Recognition Agreement (MRA) for IT security certificates, leveraging the Common Criteria, its procedures, and related documents. The European Cybersecurity Certification Group will play a key role in maintaining the scheme, collaborating with the private sector and developing specialized working groups to address evolving cybersecurity needs.*

**Keywords**

*Cybersecurity, cybersecurity certification, Regulation (EU) 2019/881, Mutual Recognition Agreement, European Cybersecurity Certification Group.*

## Background

The Commission Implementing Regulation (EU) lays down rules for the application of the European Common Criteria-based cybersecurity certification scheme (EUCC). It provides detailed guidelines and requirements for the adoption and implementation of the EUCC as specified in Regulation (EU) 2019/881. The implementing regulation aims to enhance cybersecurity across the European Union (EU) by establishing a standardized certification scheme for information and communication technologies (ICT) products. It outlines the roles, responsibilities, evaluation standards, assurance levels, and methods for certifying ICT products under the EUCC framework. Additionally, the implementing regulation emphasizes the retention, disclosure, and protection of information related to certification processes and certificates.

## The Importance of Common Standards

**1) Protection Against Cyber Threats:** Cybersecurity measures help safeguard against a wide range of cyber threats, including malware, phishing attacks, data breaches, and ransomware. By implementing robust cybersecurity practices, organizations can mitigate risks and protect sensitive information.

**2) Maintaining Trust and Confidence:** Common cybersecurity standards provide a baseline for organizations to follow, ensuring a consistent level of security across different sectors. Adhering to these standards helps build trust among stakeholders, customers, and partners, demonstrating a commitment to security and data protection.

**3) Facilitating Interoperability:** Common standards promote interoperability among systems and devices, enabling seamless communication and data exchange. This is particularly important in today's interconnected world where various technologies need to work together securely.

**4) Regulatory Compliance:** Many industries and regions have specific cybersecurity regulations and requirements that organizations must comply with. Common standards help organizations meet these regulatory obligations efficiently and effectively.

**5) International Cooperation:** Common cybersecurity standards facilitate international cooperation and information sharing. When organizations, governments, and industries adhere to the same standards, it becomes easier to collaborate on cybersecurity initiatives and respond to global cyber threats.

**6) Risk Management:** By following established cybersecurity standards, organizations can better identify, assess, and manage cybersecurity risks. This proactive approach helps prevent security incidents and minimizes the impact of potential breaches.

## Key Takeaways

**1) Establishment of EUCC Framework:** The regulation sets out rules for the application of the EUCC within the European cybersecurity certification framework established by Regulation (EU) 2019/881.

**2) Roles and Obligations:** It specifies the roles, rules, and obligations of stakeholders involved in the EUCC, including national cybersecurity certification authorities, conformity assessment bodies, and certification bodies.

**3) Certification Process:** The regulation outlines the certification process for ICT products under the EUCC, emphasizing third-party conformity assessment by accredited bodies to ensure a high level of trust and assurance.

**4) Certified Protection Profiles:** Certified protection profiles are included in the EUCC conformity and compliance monitoring by national cybersecurity certification authorities, with a focus on ensuring a high level of cybersecurity for ICT products.

**5) Common Criteria and Evaluation Methodology:** The regulation references the Common Criteria for Information Technology Security Evaluation and the Common Evaluation Methodology as the basis for evaluating protection profiles and ICT products.

**6) State-of-the-Art Documents:** State-of-the-art documents, including evaluation methodologies and technical guidelines, play a crucial role in the certification process and are endorsed by the European Cybersecurity Certification Group.

**7) European Cybersecurity Certification Group:** This group plays a significant role in maintaining the EUCC scheme, endorsing state-of-the-art documents, and providing recommendations for certification activities.

## Challenges for the Implementation of the New Scheme

**1) Complexity and Compliance Burden:** Compliance with new certification requirements and standards can be complex and resource-intensive for organizations, especially smaller businesses with limited cybersecurity expertise and resources.

**2) Lack of Awareness:** Stakeholders may lack awareness of the new certification scheme, its requirements, and the benefits it offers, leading to slow adoption and implementation.

**3) Interoperability Issues:** Ensuring interoperability between different ICT products and systems certified under the EUCC scheme may pose challenges, particularly if there are variations in certification criteria or interpretations.

**4) Resource Constraints:** Conformity assessment bodies and certification bodies may face resource constraints in terms of expertise, capacity, and funding to meet the demands of the certification process effectively.

**5) Harmonization and Consistency:** Achieving harmonization and consistency in certification processes and criteria across EU member states can be challenging, especially if there are divergent interpretations or implementations.

**6) Cybersecurity Risks:** Despite certification, ICT products may still be vulnerable to emerging cyber threats and attacks, highlighting the need for ongoing monitoring, updates, and adaptation of certification requirements.

**7) Legal and Regulatory Challenges:** Adapting to evolving legal and regulatory frameworks, both at the EU level and internationally, may present challenges in ensuring compliance and alignment with changing cybersecurity requirements.

**8) International Recognition:** Ensuring international recognition and acceptance of EUCC certifications outside the EU may require alignment with global cybersecurity standards and frameworks, which could be a complex process.

**9) Data Privacy Concerns:** Balancing the need for robust cybersecurity with data privacy and protection requirements, such as those outlined in the General Data Protection Regulation (GDPR), can be a challenge for organizations seeking certification.

**10) Adoption and Trust:** Building trust and encouraging widespread adoption of the EUCC scheme among stakeholders, including consumers, businesses, and government entities, may require effective communication, education, and demonstration of the scheme’s benefits.

## Conclusion

The Commission Implementing Regulation (EU) lays down rules for the application of the European Common Criteria-based cybersecurity certification scheme (EUCC). It provides detailed guidelines and requirements for the adoption and implementation of the EUCC as specified in Regulation (EU) 2019/881. The regulation aims to enhance cybersecurity across the European Union by establishing a standardized certification scheme for information and communication technologies (ICT) products. It outlines the roles, responsibilities, evaluation standards, assurance levels, and methods for certifying ICT products under the EUCC framework. Additionally, the document emphasizes the retention, disclosure, and protection of information related to certification processes and certificates.

## Further Reading

- Implementing Regulation on the adoption of a European Common Criteria-based cybersecurity certification scheme (link)