CYBERFORT QUALITY MANAGEMENT FRAMEWORK

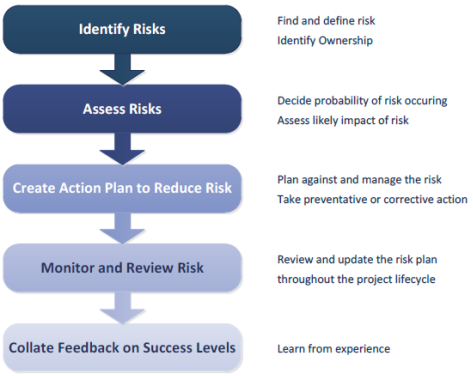
8th September 2025, Stefan-Andrei SIMA

The CYBERFORT Consortium successfully submitted the Project Quality, Risk Assessment, Research, Control & Innovation Management Plan, a key strategic document that ensures all project activities are executed at the highest quality standards, with robust risk monitoring and a strong focus on innovation. This deliverable is an essential tool in the project's internal governance and supports CYBERFORT's wider mission: to equip European SMEs with trusted, open-source cybersecurity solutions that meet the requirements of the Cyber Resilience Act (CRA). Funded by the European Commission under the Digital Europe Programme, the project brings together expert partners from Romania, Cyprus, and Greece to ensure secure, compliant, and impactful results.

The Quality Plan acts as a key internal governance document, building upon the foundation set by the Project Management Handbook. It defines the essential processes and shared responsibilities that allow CYBERFORT to deliver results in a consistent, secure, and transparent manner. It ensures that all project partners align on how outputs are prepared, reviewed, and improved throughout the project's implementation.

A strong emphasis is placed on quality assurance and collaborative coordination. The document outlines procedures for documentation workflows, standard naming conventions, peer-review processes, and version control measures. These internal mechanisms enable efficient teamwork and streamline the preparation of deliverables, software, and public materials. Each Consortium Partner has appointed a Quality Assurance Contact Point to monitor compliance locally and maintain consistency across the board.

The Plan also introduces clear development and testing procedures to ensure technical outputs are robust and secure. Agile development methodologies, secure code practices, multi-level testing phases (unit, integration, and system), and corrective actions for non-conformities are all described in detail. A dedicated section addresses risk management through the FERMA model, guiding partners in how to detect, evaluate, and respond to technical, legal, and strategic risks using a shared Risk Register and escalation channels.



The implementation of the Project is led by an international Consortium that brings together diverse areas of expertise under a shared mission. Funded by the European Cybersecurity Competence Centre (ECCC) through the Digital Europe Programme, CYBERFORT officially launched on 1st December 2024. The Consortium is composed of 8 Partner Organisations from Cyprus and Romania, combining strengths across cybersecurity, legal, energy, and digital innovation fields. The Project is coordinated by I-ENERGYLINK (RO), in collaboration with BOLTON TECHNOLOGIES (CY), CLONE SYSTEMS (CY), COLUMBIA SHIPMANAGEMENT (CY), DEALIO LIMITED (CY), the ROMANIAN NATIONAL CYBERSECURITY DIRECTORATE (RO), ELIAS NEOCLEOUS (CY), and EXIMPROD ENGINEERING (RO).

CYBERFORT presents a comprehensive approach designed to strengthen the cybersecurity defenses of SMEs. It offers an integrated strategy to improve SMEs' cybersecurity by implementing the CRA requirements. The project emphasizes creating and sharing tailored compliance tools, best practices, and educational resources to help SMEs tackle the challenges posed by cybersecurity threats.

The Project aims to introduce innovative ideas for various energy stakeholders across Europe, particularly in Southeastern Europe. CYBERFORT will develop free, open-source tools to support the internal compliance process in line with the CRA. Throughout the project's implementation, workshops, hackathons, and conferences will be organized to share results and outcomes.

This Project has received funding from the European Union's Digital Europe Programme under Grant Agreement no. 101190281

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE