



PROJECT DURATION
01/03/2024 - 31/08/2026



ERDF
1,927,889.60 €



TOTAL BUDGET
2,409,862.00 €



Improving the Cyber RESilience and Security of Adriatic PORTs

| Brochure N°3



INTRO

The project marks the crucial shift from the phase of technological experimentation to **the consolidation of a structural and permanent resilience**.

In an interconnected global ecosystem, cybersecurity is not merely a technical requirement, but the fundamental pillar for operational continuity and for the competitiveness of commercial traffic in the Adriatic Sea. CRESPOINT's efforts align with the recommendations of the **World Bank report "Cybersecurity in Ports: Shifting from Risk to Resilience,"** turning data protection into a driver of macroeconomic stability. Theory is now supported by tangible evidence: **cybersecurity is the engine of secure economic growth** for the entire cross-border area.



WP2 ACTIVITIES COMPLETED IN COOPERATION:



RAVENNA AND ANCONA

Digitalisation of processes and implementation of advanced systems for secure operational tracking.



VENICE

Validation of operational efficiency through rigorous testing of the scheduling tool.



PLOČE

Evolution of the Data Center infrastructure and enhancement of server security.



TRIESTE

Strengthening of active monitoring through the activation of a dedicated Security Operations Center (SOC).



DUBROVNIK

Structural modernisation through targeted upgrades of hardware and software components.



RIJEKA

Increased perimeter protection with the installation of new next-generation firewalls.

These local improvements across the seven Adriatic Ports involved are not isolated, but converge into a **collective defence system** that drastically reduces the vulnerability of the entire Adriatic logistics chain. To function in synergy, these technologies require a **framework of common rules**.



THE ARRANGEMENT BEYOND PROJECT'S END

✓ ✓ ● WP3

Objective:

*To sign MoU for creating
a cross boarder cooperation
beyond the project's end.*



WP3

THE “COMMON LANGUAGE” OF RESILIENCE

“Cross-border Strategy for Improving Cyber Resilience and Security of Adriatic Ports”: the partnership starts working on defining the minimum technical and functional requirements for hardware, software, cloud services, and the ship-port interface. These guidelines constitute the **“common language” of resilience**: standardisation is the only viable strategy for effectively managing cross-border data exchange, ensuring that interoperability becomes a strength rather than a weakness.





BOARD CONTRIBUTIONS

Role of the Board:

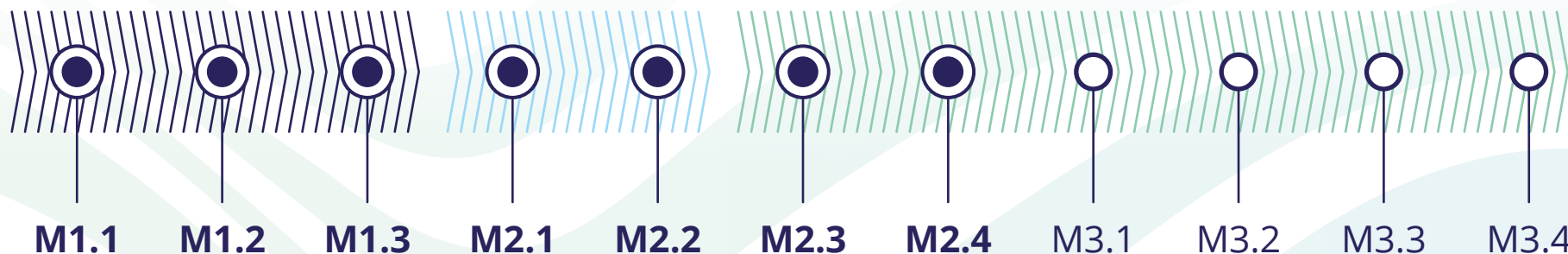
1. Technical support to pilot actions.
2. Validation of methodologies and results.
3. Independent expert feedback.
4. Sharing of real-world experiences related to cyber incidents in critical infrastructures.

Milestones achieved:

2024

2025

2026



Find out more

www.italy-croatia.eu/web/cresport/library



CONCLUSION

A SHARED VISION FOR SAFER PORTS

CRESPORT is developing a concrete and transferable model for enhancing Port Cyber Security, built on:

A strategic path that will strengthen **the resilience of Adriatic ports** and prepare them for **the future challenges of digitalisation**.

REAL-WORLD TESTING ON CRITICAL INFRASTRUCTURE



Port of Ravenna Authority

Area Pianificazione, Sviluppo, Promozione e Progettazione UE
Servizio Promozione e Progettazione Europea



www.italy-croatia.eu/web/cresport/partners

Contacts:

Via Antico Squero, 31 - 48121 Ravenna Italy
anna.esposito@port.ravenna.it
+39 0544 608880