ERMIS

Newsletter

2025 - Issue No 4

In this Issue

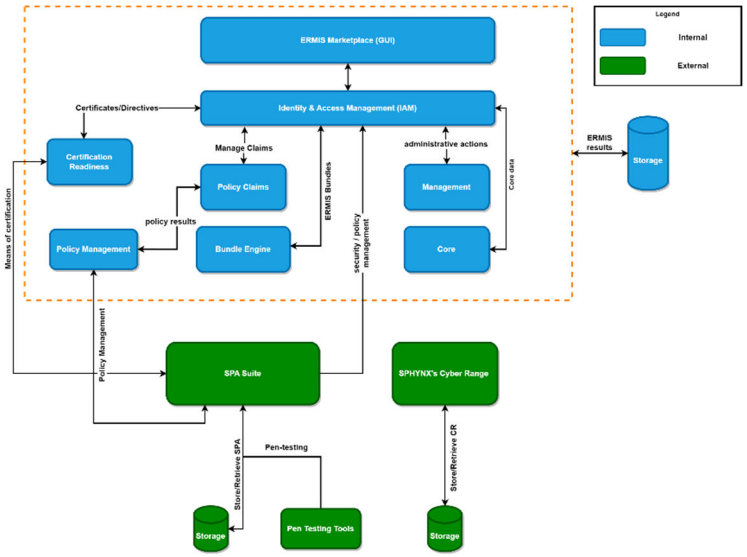

Figure 1 ERMIS High-level architecture

Over the last several months, the ERMIS consortium has made significant progress in the design, development, and partial deployment of the ERMIS Proof of Concept (PoC), with key contributions across Work Packages. Within WP3, the focus has been on the cybersecurity assurance and insurance marketplace. The initial technical specifications and architecture were successfully delivered as part of Milestone 4 (M10), followed by a more robust and mature version that incorporates both functional and non-functional requirements. Significant development efforts were directed towards the creation of the Graphical User Interface (GUI) and backend components, particularly on the supply side and selected demand-side scenarios, enabling the initial execution of Use Case (UC) owner activities. A first limited integrated version of the marketplace has been extracted and tested, while its architectural components are being finalised.

In parallel, WP4 has focused on establishing the certification, risk, and cyber insurance framework that underpins the marketplace's value proposition. The framework is structured around three core, interlinked components: certification readiness, risk assessment, and cyber insurance. These components are embedded into iterative processes that allow for dynamic evaluation and real-time adaptation. Notably, the ERMIS Certification Readiness Model was developed to offer targeted insights into certification preparedness, with ISO/IEC 27001:2022 serving as the foundational standard. The risk assessment models integrate certification and insurance perspectives, offering a comprehensive view of an organisation's cyber posture. Additionally, bundled cyber insurance models have been introduced to align pricing structures with cybersecurity solution deployment. WP5 contributed by delivering and customising the necessary tools that support the cyber risk assessment and certification readiness mechanisms within the ERMIS marketplace. The consortium reached Milestone 7 at M14, having developed and deployed several key components. A real-life case study on the UC owner allowed for asset modelling and initial cybersecurity assessments using the tools developed. Work is also underway to establish a seamless linkage between these cybersecurity tools and the marketplace's cyber insurance and certification frameworks. Furthermore, the deployment environment for collecting and analysing operational evidence has been initiated.

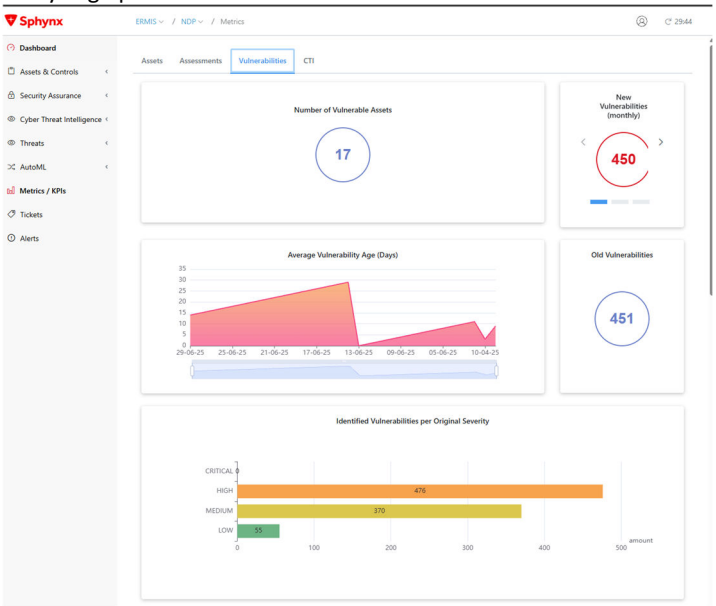

Figure 2 Pilot initial statistics

In WP6, real-life demonstration scenarios have been detailed, including both supply-side and demand-side flows, resulting in the documentation of multiple individual scenarios. These scenarios are instrumental for shaping UC activities, and an evaluation methodology has been defined to support structured assessment and iterative feedback as the platform moves towards its MVP stage. In the coming months, ERMIS will continue to refine its system architecture, integrate and validate components, and transition to the development of a functional MVP to support broader demonstration and engagement efforts.

By Dr. Michalis Smyrlis, SPH

Figure 3 CRIRM 2025 - More information: https://www.ieee-csr.org/crirm/

CSR CRIRM: ERMIS, together with SecAwarenessTruss and CyberUnity, is organising the 2025 IEEE CSR Workshop on Cyber Range, Insurance, and Risk Management (CRIRM), taking place on 5 August 2025 in Chania, Crete, as part of the IEEE Conference on Cyber Security and Resilience. The workshop will feature seven peer-reviewed papers highlighting advances in cybersecurity training, risk assessment, and cyber insurance.
MIDTERM REVIEW: ERMIS has successfully completed the 1st review meeting on the 12th of June, which affirmed the consortium's solid progress and direction.

ERMIS marketplace Cyber Insurance and Assurance bundles

What are Bundles? ERMIS bundles are integrated packages combining cybersecurity solutions with cyber insurance policies, offering SMEs a comprehensive "one-stop solution" for both security protection and financial coverage.

How are Bundles Formed? Insurance and assurance providers register their insurance policies and tools and opt in for bundling. The ERMIS platform then analyses compatibility between security solutions and insurance policies, using powered matching to suggest optimal bundle combinations to the end users.

End-users seeking cyber insurance and Assurance solutions: End-users looking for cyber insurance and assurance solutions can explore their own tailored bundle catalogue equipped with filtering options based on cost, coverage, industry, and company size (see Figure 4). Each bundle includes a detailed view outlining terms, prerequisites, and the required cybersecurity solutions (see Figure 5). Users can also utilise comparison tools to evaluate bundles side by side. Additionally, assessment results provide real-time insights into the current security posture of their infrastructure.

Expression of Interest and Customization: For the initial interest and assessment, end-users seeking cyber insurance and assurance solutions select a tailor-made proposed bundle and submit interest requests, approving data sharing with insurance providers. The ERMIS marketplace performs an initial cybersecurity assessment. End-users can now receive an exact quotation with specific services (insurance and assurance), with a discount and without having to run through the complex questionnaire as is currently required.

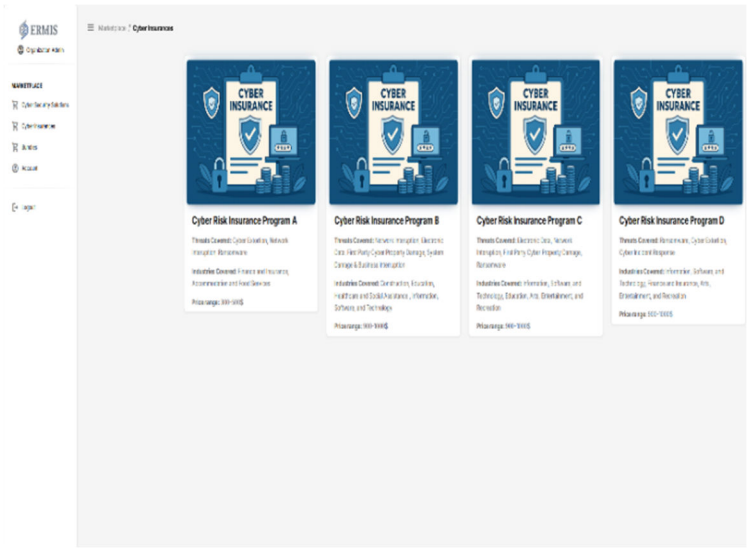

Figure 4 End-user view of the bundle catalogue interface

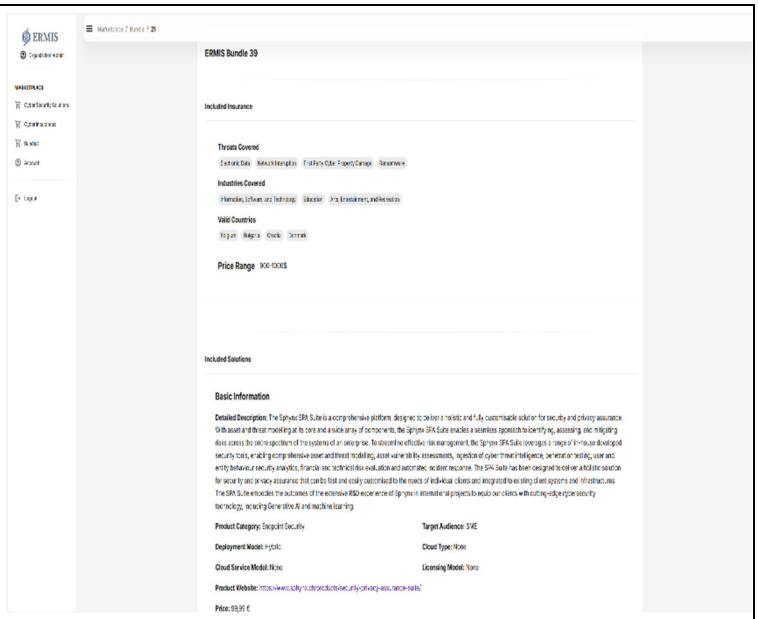

Figure 5 Detailed bundle view displaying terms, prerequisites and requirements.

By George Bolpasis & Elli Alimperti, ZELUS

Contact **Project Coordinator** Zelus **Inquiries** info@dep-ermis.eu

Disclaimer

The project received funding under Grant Agreement No 101128013, and is supported by the European Cybersecurity Competence Centre.

The project is supported by the Ministry of Digital Governance of Hellenic Republic and the National Cyber Security Authority and is aligned with the Hellenic Cyber Security Strategy.

Consortium Partners