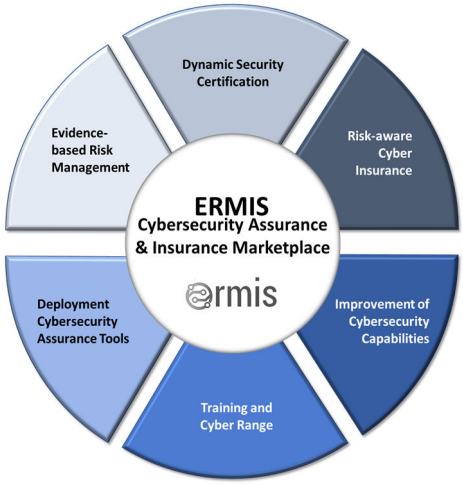
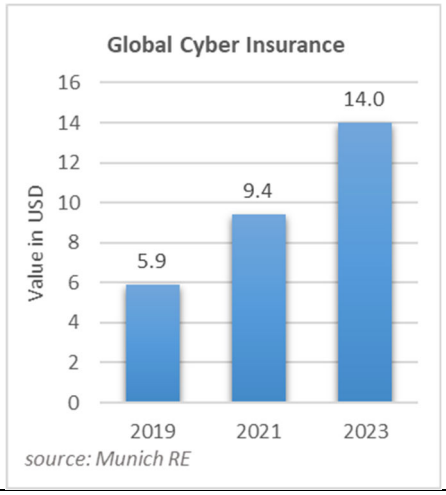
ERMIS Newsletter

April 2024 - Issue No1

In this Issue

The ERMIS concepts and the marketplace contents





Overview

ERMIS (CybERsecurity Market assurance and Insurance-as-a-Service) is a European Union project under the DIGITAL-ECCC-2022-CYBER-03 work programme, launched in November 2023. ERMIS has 3-years duration and aims at developing of a cyber security assurance and insurance as-a-service, by integrating mechanisms, services, and tools in an innovative marketplace platform.

The ERMIS marketplace aims to support the adoption of innovative cybersecurity solutions by providing end-to-end support for cyber risk assessment, security certification, and cyber insurance processes. It aims to strengthen cybersecurity capabilities for EU SMEs and public organizations, while also empowering the cyber insurance market to assess the potential of the European digital ecosystem to eliminate the impact of security incidents and improve business continuity strategies. In particular, the ERMIS marketplace:

- Integrates tools for supporting the implementation of cybersecurity protection services, with the aim to collect and analyse operational evidence, using ML algorithms;
- Hosts services and tools for providing auditing on cybersecurity resilience of open-source projects and libraries and other software components through risk-aware security certification mechanisms;
- Supports security testing service components, including static-analysis code scanning tools, penetration testing tools and vulnerability analysis tools;
- Will deliver software components, services, and tools for the monitoring and analysis of security incidents, the investigation of cybersecurity threats and the management of incident response strategies and cyber threat intelligence information;
- Will support various stakeholders' groups and communities by providing cyber ranges and training for experts in the use of mechanisms and tools for improving cybersecurity capabilities and enhancing cyber resilience towards more accurate management of cyber insurance policies.

Goals

- Deliver Cyber security Assurance and Insurance as-a-Service in an innovative marketplace platform;
- Integrate and deploy mechanisms, services, and tools from partners portfolios;
- Offer end-to-end support for cyber risk assessment, security certification, and cyber insurance;
- Promote adoption and deployment of market-ready cybersecurity solutions.

Cyber insurance Market Trends

The increasing number of cyber-attacks and data leaks is the leading factor driving the growth of the cybersecurity and cyber insurance market. Ransomware, business communication and email compromise (BEC & BCC), data breaches and supply chain vulnerabilities are the major loss drivers in cyber insurance.

Global cyber insurance market was valued at 14bn USD in 2023 a nearly 50% increase compared to 2021 totaling 9,4 bn USD, and almost triple the last five years, driven by the strong commitment of reinsurers and the recent interest in cyber risks shown by the capital markets. The insurance gap remains the main concern of the insurers, highlighting the imperative of achieving greater insurance penetration for cyber risks in a dynamic digital landscape and ensuring that insurance coverage is both adequate and provided on a sustainable basis.

(source: Munich RE, Cyber Insurance: Risks and Trends 2024, 04.04.2024)

Pilot Business Scenarios

Through the ERMIS project, the marketplace will implement cyber security assurance and certification mechanisms that will be made available to multiple stakeholders' groups. These will be ranging from cybersecurity experts and analysts, being responsible for internal and/or external auditing of the applied measures in a cyber environment, to cyber insurance policy facilitators and decision makers seeking for certified, flexible and intuitive ICT-enabled solutions to assess the cyber insurance risks related to the digital assets of complex supply chains and maintain relevant cyber insurance policies in a more accurate manner. To this end, ERMIS will be validated in two realistic business cases:

Pilot 1

ERMIS employs innovative SMEs in the technology field that will benefit from the marketplace capabilities by providing improved cybersecurity services for their products and their customers. In the light of the new EU NIS2 directive and the Cyber Security and Resilience Acts, and to respond to customer requests for an integrated and end-to-end security solution for their business services, such SMEs can register into the ERMIS Marketplace to validate the security and privacy properties of their cybersecurity solutions. They will be also able to certify the adopted security mechanisms to monitor and analyse the security incidents of their customers, towards reaching better and more affordable insurance policies.

Through ERMIS, the participating SMEs will be able to maintain a trusted profile of a security solution provider in the European market and enhance the cybersecurity capabilities of the product portfolio and the relevant skills of the staff to address the cyber security challenges of the customers and deliver reliable and certified security assurance services. To this end, KAR and relevant cyber insurance agencies can develop more appropriate and less costly insurance policies for these SMEs and relax the (technological and economic) barriers for these organisations to build and maintain their certified security profile towards enhanced cyber resilience.

Pilot 2

In this pilot, an ICT SME, which develops and deploys IT software for the healthcare domain by providing qualitative tools and services focusing on integrated healthcare solutions in the wider context of predictive, individualized, preventive and participatory medicine. Such solutions are deployed to various health service providers (including hospitals, primary care centres, regional health authorities) and they process and manage sensitive data, which poses strict security and privacy requirements. The relevant ICT SMEs should, then, seek to establish cyber insurance contracts that will safeguard key security, privacy and dependability requirements for their e-health providers. The latter include the preservation of privacy, confidentiality and integrity of medical records in-transit and at-storage, the preservation of privacy, confidentiality and integrity of prescription and financial data in-transit and at storage, and the preservation of a high degree of the e-health platform availability.

A cyber insurance agency that has ICT SMEs as customers for issuing insurance contracts on their digital solutions when they are deployed and operate in healthcare environments. As such, the agency requires to have a continuous understanding and assessment of the security maturity for the products of these SMEs to be able to specify the cyber insurance policies in an accurate and reliable way.

In that respect, this agency will register into the ERMIS marketplace and validate the provided capabilities to:

i) define the cyber insurance policies that are highly relevant for the digital infrastructure of NDP and other SMEs that are engaged in ERMIS, subject to iterative risk assessment and security certification activities for the deployed and running products of these SMEs, and

ii) continuously collect and analyse evidence from the operational environment of these running products and adapt the cyber insurance policies, based on the current risk exposure of the ICT SME's products and the related analysis of the observed threats.

Kick-off Meeting

The Kick-off Meeting of ERMIS was held in Athens on November 21st, 2023.

Contact

Project Coordinator: Zelus, General inquiries: info@dep-ermis.eu

ERMIS

http://dep-ermis.eu/

#DEP-Ermis

EP-Ermis

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 Cybersecurity Authority and is aligned with the Hellenic Cyber Security Strategy.