ECHO SPOTLIGHT

D2.2 ECHO MULTI-SECTOR ASSESSMENT FRAMEWORK

A key objective of the ECHO project is to develop and demonstrate a comprehensive ECHO Multi-sector Assessment Framework (E-MAF), providing the means to analyse transversal and inter-sectoral challenges and opportunities and supporting the development of cybersecurity technology roadmaps.

The E-MAF aims to provide a structured method for multi-dimensional analysis and development of management processes for cybersecurity risks and takes into consideration the needs/requirements from typical threats, vulnerabilities, affected assets and countermeasures in the domain under inspection as well as on inter-sector and transversal needs, challenges and opportunities. It sets the foundation for an implementation which focuses on all of them. The development methodology is based on a continuous iteration-based process, enabling a tight collaboration between several tasks of WP2.

The envisaged framework will mix a new methodology based on the introduced logical and architectural models together with aspects inspired by standardized methodologies for Risk Assessment and scoring that can be tailored to the specific requirements to E-MAF. This deliverable reports on the analysis of challenges and opportunities derived from sector-specific use cases and contributes to the on-going development of the ECHO Risk Assessment Framework, and the ECHO Risk Management Framework, later.The latter will finally evolve in a three-tiered Multi-sector Cybersecurity Framework (the E-MAF).

While presenting the work done, the focus of the document is on horizontal technologies and cybersecurity in selected critical sectors, as well as addressing inter-sector dependencies and transversal security aspects. It provides a snapshot of the methodology and architectural design for the implementation of the multi-sector assessment framework. Subsequent stages of validating and iterating the framework will be pursued actively and these results will be documented in related tasks such as the inter-sector technology roadmaps, Early Warning System, Federated Cyber Range and finally the demonstration cases.

The goal to develop and demonstrate a comprehensive ECHO Multi-sector Assessment Framework, aimed at providing a new way to analyze transversal and inter-sectoral challenges and opportunities and supporting the development of cybersecurity technology roadmaps, is too ambitious to be fully addressed in just a few months at the beginning of the project. For this reason, the project schedule spreads activities all along the project timeline. So, the requirements coming from other tasks was faced by defining a modular architecture enabling an iterative development and implementation methodology as well as the set-up of virtuous cycles of innovation. Moreover, it does worth to be said that these initial top-down and bottom-up analysis are pillars for the full architecture; they were absolutely needed to start and fundamental to be defined.

In this aim, the foreseen initial assessment activities focused on Risk Assessment and Risk Management frameworks with main interest into Risk Assessment Methodologies while all methods for general risk governance (COBIT, Basel II for example) or high-level reference documents have been excluded by default. The analysis methodology for methods/frameworks took into account a set of parameters strictly related to Risk Assessment process. Then how these frameworks have been applied in real systems in the ECHO-domains (health care, energy, maritime, defense and space), in an inter-sectoral and transversal way was inspected, also through the analysis of domain specific threats, vulnerabilities, affected assets, and countermeasures for cyber risk governance (where possible, with huge restriction in defense domain). Also, outcomes provided by previous EU funded projects, their architecture and logical models were inspected, as well as the foreseen outputs of currently running projects.

At the end, the main goal of the final development of a multi-sector cybersecurity framework, with focus on EU specificities and policy targets, compatible with Member States' policies and regulations and which takes into account cross-border risks, will be reached. It will be a very amazing activity devoted to follow a sort of yet unexplored path, the team will walk in an enthusiastic manner.