Title	European network of Cybersecurity centres and competence Hub for innovation and Operations
Acronym	ECHO
Number	830943
Type of instrument	Research and Innovation Action
Topic	SU-ICT-03-2018
Starting date	01/02/2019
Duration	48
Website	www.echonetwork.eu

D2.2 ECHO MULTI-SECTOR ASSESSMENT FRAMEWORK

Work package	WP2 Multi-sector Needs Analysis
Lead author	Marco PAPPALARDO (CIRM)
Contributors	Riccardo Delpopolo Carciopolo, Gabriella Trombino (CIRM), Mascia Toussaint (ENQ), Barbara Angelucci, Consuelo Colabuono, Raffella Condoleo (RHEA), Nikolai Stoianov (BDI), Maria Vittoria Marabello (EXP), Kirsi Aaltola (LAU), Raniero Rapone (AON), Daniele Cristofori (ZP), Giuseppe Chechile (FC), Jari Räsänen (LAU), Kristine Hovhannisyan, Andrew Roberts (TUT), Alessandro Cantelli-Forti (LCU), Oleg Illiashenko (KHAI), Todor Tagarev (IICT).
Peer reviewers	Matteo MERIALDO (RHEA), Tiago NOGUEIRA (VISIONSPACE), Barbara ANGELUCCI, Maria Vittoria MARABELLO (EXPRIVIA).
Version	V2.4
Due date	18/06/2020
Submissiondate	18/06/2020

Dissemination level

X	PU: Public
	CO: Confidential, only for members of the consortium (including the Commission)
	EU-RES.Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)
	EU-CON. Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)
	EU-SEC. Classified Information: SECRET UE (Commission Decision 2005/444/EC)

The work described in this document has been conducted within the ECHO project. This project has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830943

Version history

Revision	Date	Editor	Comments
0.1	02/07/2019	Marco Pappalardo (CIRM)	Draft ToC and initial assignment of contributions
0.1	08/07/2019	Marco Pappalardo (CIRM)	Changing contributions. ENQ from 4.1.1 to 4.5.3 and 4.5.7.
0.2	30/07/2019	Marco Pappalardo (CIRM)	Added contributions to Section 2.2
0.3	19/08/2019	Marco Pappalardo (CIRM)	Updated ToC
0.4	21/09/2019	Marco Pappalardo (CIRM)	Added contributions from Section 2.3 to 2.5.4
0.5	9/10/2019	Marco Pappalardo (CIRM)	Added contributions to Section 4.3.2
0.6	17/10/2019	Marco Pappalardo (CIRM)	Added contributions to Sections from 3.1 to 3.4
0.7	30/10/2019	Marco Pappalardo (CIRM)	Added contributions to Sections from 4.1 to 4.3
0.8	04/11/2019	Marco Pappalardo (CIRM)	Adjusted the references styles
0.9	08/11/2019	Marco Pappalardo (CIRM)	Added contribution to Section 3.5
1.0	12/11/2019	Marco Pappalardo (CIRM)	Revised section 4. Finalization.
2.0	31/05/2020	Marco Pappalardo (CIRM)	Moved and improved section 4 to section 5. Added the new section 4. Full revision and alignment of the document with updated goals and timelines. Partially edited section 3.5.
2.1	10/06/2020	Tiago Nogueira (VisionSpace)	QA checks. Format and textcorrections.
2.2	12/06/2020	Marco Pappalardo (CIRM)	Minor updates after QA.
2.3	15/06/2020	Harri Ruoslahti (LAU)	Full check of cross references after QA.
2.4	18/06/2020	Matteo Merialdo (RHEA)	Final checks and document closed

List of contributors

The list of contributors to this deliverable are presented in the following table:

Section	Author(s)
All	CIRM
2	RHEA, ENQ, LAU, AON, EXP, FC, Z&P
3	RHEA, AON, EXP, FC, NAU KHAI, Z&P
4	CIRM
5	RHEA, BDI, IICT
6	CIRM

Keywords

E-MAF, ECHO MULTI-SECTOR ASSESSMENT FRAMEWORK, FRAMEWORK, RISK ASSESSMENT, RISK MANAGEMENT, TRANSVERSAL, INTER-SECTOR, MULTI-SECTOR, MULTI-TIER, LAYER, TECHNOLOGICAL, CHALLENGES AND OPPORTUNITIES, ROADMAPS.

Disclaimer

of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

Executive summary

A key objective of the ECHO project is to develop and demonstrate a comprehensive ECHO Multi-sector Assessment Framework (E-MAF, previously E-MSAF, see Introduction), providing the means to analyse transversal and inter-sectoral challenges and opportunities and supporting the development of cybersecurity technology roadmaps. This report describes the outcomes of analysis and design activities leading to the architectural design of ECHO Multi-sector Assessment Framework.

This objective is implemented in activity T2.2 (Derivation of ECHO Multi-sector Assessment Framework) that will develop and adopt the Multi-sector Assessment Framework. The E-MAF aims to provide a structured method for multi-dimensional analysis and development of management processes for cybersecurity risks; it will also provide:

- leveraging to guide actions and provide confidence on program and actions taken;
- help to benchmark initiatives;
- an effective cybersecurity educational portfolio and training programmes;
- a shared definition of the transversal and cross-sectoral skills and qualifications needed by cyber-security actors.

While providing the outcomes listed above, T2.2 activities refer to several fundamental sources like:

- Contents and analyses from task T2.1 StoryLines and Use Cases;
- Frameworks, Standards and Regulations currently used by key actors in the observed sectors;
- Existing frameworks/practices adopted by organisations within and outside the ECHO ecosystem;
- Other EU funded projects focused on similar goals.

This report describes the methodologies involved in the definition of the E-MAF architectural design:

- Risk Assessment (RA) and Risk Management (RM) methodologies;
- Methodology to analyse existing Cybersecurity Frameworks in the inspected domains;
- Methodology for the design and implementation of E-MAF.

This architectural design 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 (see Section 5) and scoring that can be tailored to the specific requirements to E-MAF. As part of T2.2, 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 (M18 official release of first prototype), 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 this document is on horizontal technologies and cybersecurity in selected critical sectors, as well as addressing inter-sector dependencies and transversal security aspects. This is a living document, delivered at the early stages of the project, in order to provide information to related key tasks in WP2 and built constructive synergies between several different ECHO activities. This deliverable

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 (WP4), Early Warning System (WP5), Federated Cyber Range (WP6) and finally the demonstration cases (WP8).

The structure of the document is in line with its scope, i.e. to deliver the methodology and the foreseen outcomes of the first iteration for the E-MAF.

This deliverable (D2.2 v.2.4) is an updated of the former D2.2 v.1 subsequently to the Review and the request for resubmission. The whole document has been aligned with the new timeframes and with the work done on architecture in the last months. Major changes occurred in the following sections:

- Section 4: new section dealing with assessment of methodologies/framework used in EU funded projects;
- Section 5 (former section 4): new 5.3 section added, other sections (5.1, 5.2, 5.4, 5.6 respectively former 4.1, 4.2, 4.3, 4.5) aligned with recent improvements in design and renumbered;
- Section 3.5: domain-specific assessment for defence and space improved;
- Section 6: updated.

Table of contents

Version history 2
List of contributors 2
Keywords 2
Disclaimer 2
Executive summary 4
Table of contents 6
List of figures 10
List of tables 10

1. INTRODUCTION 12

1.1 PURPOSE AND SCOPE OF THE DOCUMENT 12

1.1.1 Improvements after the first project review 12

1.2 STRUCTURE OF THE DOCUMENT 13

1.3 RELATION TO OTHER WORK IN THE PROJECT 13

1.4 APPLICABLE AND REFERENCE DOCUMENTS 14

1.5 INTELLECTUAL PROPERTY RIGHTS 25

1.6 GLOSSARY OF ACRONYMS 25

2. RISK ASSESSMENT AND MANAGEMENT FRAMEWORKS ANALYSIS 27

2.1 INTRODUCTION 27

2.2 ISO 31000 RISK MANAGEMENT METHODOLOGY 29

2.2.1 Risk Assessment in ISO 31000:2018 32

Risk Identification 33
Risk Analysis 34
Risk Evaluation 34

2.3 TOGAF ENTERPRISE ARCHITECTURE FRAMEWORK 34

2.3.1 TOGAF RA Methodology 38

2.4 NIST RISK MANAGEMENT FRAMEWORK 41

2.4.1 Overview of the SP800-30 Risk Assessment Process 42

2.4.2 Evaluation of NIST SP 800-30 in the context of ECHO 46

2.5 OTHER RISK ASSESSMENT METHODOLOGIES 46

2.5.1 MEHARI Risk Assessment Method 47

Overview of MEHARI Risk Assessment process 47
Business process analysis, malfunction analysis, assets assessment 48
Vulnerability assessment 48
Threat assessment 48
Security measures assessment 48
Risk scenarios assessment 49
Risk treatment 50
Evaluation of MEHARI in the context of ECHO 52

2.5.2 MAGERIT 53

Overview of MAGERIT Risk Assessment process 54
Evaluation of MAGERIT in the context of ECHO 58
2.5.3 OCTAVE 60
Overview of OCTAVE Risk Assessment process 60
OCTAVE Criteria 62
OCTAVE developments 64
OCTAVE-S [41] 64
OCTAVE-Allegro 65
Methodology 65
Evaluation of OCTAVE in the context of ECHO 67
2.6 CONCLUDING REMARKS 68

3. ANALYSIS OF EXISTING CYBER SECURITY FRAMEWORK ADOPTION IN THE SECTORS OF INTEREST 71
3.1 ANALYSIS METHODOLOGY AND CRITERIA 71
3.2 HEALTH CARE SECTOR 72
3.2.1 NIST Cyber Security Framework 74
3.2.2 HITRUST Common Security Framework 74
3.2.3 CIS Critical Security Controls 75
3.2.4 ISO 27000 75
3.2.5 COBIT 75
3.2.6 ECHO healthcare scenarios: weaknesses and potential mitigation actions 76
3.2.7 Conclusions 80
3.3 ENERGY SECTOR 81
3.3.1 MEHARI 84
3.3.2 MAGERIT 85
3.3.3 ISO 31000 85
3.3.4 OCTAVE 86
3.3.5 NIST 86
3.3.6 ISO 27001 86
3.3.7 COBIT 87
3.3.8 ECHO energy scenarios: weaknesses and potential mitigation actions 87
3.3.9 Conclusions 89
3.4 MARITIME SECTOR 89
3.4.1 IMO guidance 90
3.4.2 Guidelines on Cyber Security on board Ships 90
3.4.3 Cyber security resilience management for ships and mobile offshore units in operation 91
3.4.4 ISO27001 92
3.4.5 TOGAF 92
3.4.6 ECHO maritime scenarios: weaknesses and potential mitigation actions 92
3.4.7 Conclusions 96

3.5 DEFENCE AND SPACE SECTORS 97
3.6 INTER-SECTOR AND TRANSVERSAL ASPECTS 101
3.6.1 State of the art and transversal/inter-sector factors 101
3.6.2 Transversal challenges and opportunities 102
3.6.3 Industrial analysis of inter-sector dependencies 108
HEALTHCARE 108
ENERGY 110
DEFENSE/MARITIME 111
SUMMARY OF INTER SECTOR DEPENDENCIES 113
3.6.4 Transversal and inter-sectoral needs addressed in E – MAF and in ECHO 114
4. ANALYSIS OF METHODOLOGIES FROM OTHER EU PROJECTS 117
4.1 ANALYSIS METHODOLOGY AND CRITERIA 117
4.2 OTHER PILOT PROJECTS TO PREPARE THE EUROPEAN CYBERSECURITY COMPETENCE NETWORK 117
4.2.1 SPARTA 118
NeSSoS Risk Assessment Tool 120
IDS and SIEM Assessment Tool 120
Risk Assessment for Cyber-physical Interconnected Infrastructures (MRA) 121
4.2.2 CONCORDIA 122
4.2.3 CyberSec4Europe 124
BadGraph 126
BowTiePlus 126
CORAS 126
HERMES 126
OFMC/AIF 126
PLEAK 127
SEMCO 127
SOBEK 127
SYSVER 127
VEREFOO 127
IDMP 128
4.3 EU FUNDED PROJECTS 128
4.3.1 CYSM 128
4.3.2 MEDUSA 132
4.3.3 MITIGATE 135
Step 1: Boundary Setting 140
Step 2: SCS Cyber Threat Analysis 140
Step 3: SCS Vulnerability Analysis 140
Step 4: SCS Impact Analysis 141
Step 5: SCS Risk Estimation 141
Considerations on MITIGATE Methodology 141
4.3.4 Other Projects from Cyberwatching Radar 142

AEGIS 142
CANVAS 142
CertMILS 143
COMPACT 144
CS-AWARE 146
DEFeND 147
DISCOVERY 147
PROTECTIVE 148
4.4 Concluding Remarks 150

5. THE ECHO MULTI-SECTOR ASSESSMENT FRAMEWORK 154
5.1 Methodology for design and implementation of E-MAF 154
5.2 Architectural Design of the Multi-sector Assessment Framework 162
5.3 Logical Model for ECHO Risk Management 167
5.3.1 Risk Assessment 169
5.3.2 Threats Identification 170
5.3.3 Vulnerabilities Identification 172
5.3.4 Consequences 174
5.3.5 Risk Estimation 174
5.3.6 Risk mitigation 175
Measures 176
Decisions on measures to be implemented 176
Application of measures 176
5.3.7 Implementation of the E-MAF Logical Model 177
5.4 Delivery of E-MAF 179
5.5 E-MAF Taxonomy 183
5.5.1 ECHO Cybersecurity Framework Taxonomy 183
5.5.2 ECHO Cybersecurity Framework Vocabulary 187
5.5.3 ECHO Cybersecurity Framework Semantics 200
5.6 Roadmap for E-MAF implementation 202

6. CONCLUSIONS 205
ANNEXES 207
Annex 1 – T2.2 Framework and Methodologies Analysis Questionnaires 207
Annex 1.1 – ISO31000 207
Annex 1.2 – TOGAF 211
Annex 1.3 – NIST SP800-30 213
Annex 1.4 – MEHARI 215
Annex 1.5 – MAGERIT 218
Annex 1.6 – OCTAVE 225
Annex 1.7 – HITRUST 229
Annex 1.8 – CYSM 232

Annex 1.9 – COMPACT *234*
Annex 1.10 – PROTECTIVE *236*

List of figures

Figure 1: Risk Management process in ISO 31000:2018 [19]. 33
Figure 2: Essential Security and Risk concepts in TOGAF Enterprise Architecture [34]. 36
Figure 3: TOGAF RA Hierarchical Structure [31]. 39
Figure 4: Heat map of risks for TOGAF. 40
Figure 5: SP 800-30 Risk assessment procedure [24]. 42
Figure 6: MEHARI Risk Assessment procedure 47
Figure 7: Risk Scenario estimation process 50
Figure 8: XML grammar 56
Figure 9: Example of treat definition [105]. 58
Figure 10: OCTAVE phases [14]. 62
Figure 11: OCTAVE ALLEGRO Phases and steps [41]. 66
Figure 12: Dependencies on common factors in transversal cybersecurity challenges and opportunities. 104
Figure 13: The CYSM system architecture [100]. 131
Figure 14: The MEDUSA architecture [100]. 134
Figure 15: MITIGATE general architecture [100]. 137
Figure 16: PROTECTIVE Cyber Situational Awareness Model (adopted from Mitre15) [109]. 149
Figure 17: ECHO Risk Management high-level design. 156
Figure 18: The first iteration between E-MAF and other tasks of WP2 and ECHO. 159
Figure 19: The Architectural Design of the ECHO Multi-sector Assessment Framework. 163
Figure 20: The Logical Model of the ECHO Multi-sector Assessment Framework. 169
Figure 21: General definition of the Agari Threat Taxonomy [106]. 171
Figure 22: ECHO E-MAF Vulnerability Taxonomy. 173
Figure 23: Information sharing process between the elements of E-MAF Analytical Model. 181
Figure 24: ECHO Cyber Security Ontology. 201

List of tables

Table 1: Applicable documents 15
Table 2: Reference documents. 25
Table 3: Glossary of acronyms, initialisms and abbreviations. 26
Table 4: Risk Assessment frameworks/methods survey parameters 28
Table 5: Pros and Cons of ISO 31000:2018 30
Table 6: The Risk Classification Scheme [33]. 38
Table 7: Risk Identification and Mitigation Assessment Worksheet [33]. 38

Table 8: Threat characterization 44
Table 9: MEHARI Risk acceptability Table. 51
Table 10: The history of OCTAVE. 60
Table 11: OCTAVE Principles and Attributes [40]. 63
Table 12: OCTAVE Outputs [40]. 64
Table 13: Description of threat trees [41]. 67
Table 14: ECHO Requirements coverage matrix. 69
Table 15: Most used Security frameworks in USA [42]. 74
Table 16: Cyber-attacks in the Healthcare sector[1]. 80
Table 17: Cyber attacks in the Energy sector[1]. 88
Table 18: Cyber-attacks in the Maritime sector[1]. 96
Table 19: Cyber-attacks in the Defence and Space Sectors[1]. 101
Table 20: Risk category identified from the use cases in D2.1[1]. 108
Table 21: Dependency of the Healthcare sector on Telecommunications services. 109
Table 22: Dependency of the Energy sector on Telecommunications services. 110
Table 23: Dependency of the Maritime sector on satellite services. 113
Table 24: Summary of inter sector dependencies. 114
Table 25: SCRA main blocks and sub-steps. 139
Table 26: Comparison between CYSM, MEDUSA, and MITIGATE methodologies. 152
Table 27: Sharing of information between elements of E-MAF. 178
Table 28: Example structure of the E-MAF Analytical Model. 182
Table 29: Sectors and subsectors proposed for ECHO Cybersecurity Taxonomy. 185
Table 30: Complementary sectors and subsectors for ECHO Cybersecurity Taxonomy. 187

1. Introduction

1.1 Purpose and scope of the document

This document presents the architectural design of the ECHO Multi-sector Assessment Framework (E-MAF). The overall goal of the activity is to foster the development and adoption of a Multi-Sector Assessment Framework, aiming to provide a structured method for multi-dimensional analysis and development of management processes for cybersecurity risks, leverage to guide actions and provide confidence on program and actions taken, help benchmark initiatives, provide an effective cybersecurity educational portfolio and training programmes, provide a shared definition of the transversal and cross-sectoral skills and qualifications needed by cyber-security actors. The framework employs a standardised methodology for risk assessment and scoring that can be tailored to the specific requirements as identified for the ECHO MAF making the framework "*certifiable and assurable*" (cit. **[GA]**).

Because of the demanding activities in the project which are very eagerly waiting for a first prototype of the E-MAF, a choice was made in order to provide a highly modular architecture which enables development cycles.

The E-MAF we refer to in these pages is the same Assessment Framework whose name was abbreviated by "E-MSAF" in the Grant Agreement (where "MS" was a short form for "Multi-sector"). Being for us "multi-sector" a single word indicating a very complex meaning and wanting to make the acronym pronunciation easier, ***from now on the ECHO Multi-sector Assessment Framework will be shortly indicated*** (in this document and in all the following ones) **as "E-MAF"**.

1.1.1 Improvements after the first project review

After the first project review (November 2019), the following reviewers' comments were received. As general comment it was stated that the "*Use Cases are sufficient to demonstrate the usefulness of the overall approach/model. They are indicative per sector, which is enough for the scope of the project at the moment. If these Use Cases prove and justify the correctness of the whole model (Governance, Cyber Challenges, Risk Assessment, Certification, EWS and FCR) then in practice every case (as much detailed as possible) could be used in the future.*". From the first version of this document, it was stated that UseCases will be the validation bench for E-MAF. As described in Section 5, they are used since the first (development) iteration cycle. They will feed (and validate) the prototypes and results will be used both to improve the E-MAF itself and to provide useful information to other tasks and WPs in the project (see Section **5.2**).

Another general comment has been: "*Previous work based on other EU projects must be taken into consideration and build upon this. For example there are already several 'Risk Assessment and Management' models, and methodologies that can be found in ENISAs' repository and also proposed by various EU Projects (e.g. CYSM, MEDUSA, MITIGATE)*". The models and methodologies in ENISA's repository were already analyzed in the first version of this deliverable where it was already stated that some of them had been assessed and others discarded (see Section **2.5** and Table **4**). The new Section **4** assesses three different sources:

- the other 3 pilots projects funded in 2018 Horizon 2020 cybersecurity call "Establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap" (see Section **4.2**).
- other EU funded projects (Section **4.3**). Among these, there will be: CYSM (Section **4.3.1**), MEDUSA (see Section **4.3.2**), MITIGATE (Section **4.3.3**) and a number of other projects (Section **4.3.4**).

Moreover, "The new proposed ECHO methodology should be assessed against the existing ones and explain the advancements". This architectural document reads that E-MAF takes inspiration from a list of strength points from the assessed solutions.

The expectation is that "*At the end, the ECHO project must be able to demonstrate the 'added value' on the already existing similar risk assessment methodologies and tools*". This is the final goal of T2.2 which will be clearly discussed in D2.11 (M45) together with the assessment of the methodology discussed above.

As D2.2 specific comments, the reviewers requested that D2.2 be revised before the following review meeting. The comment reads as follows:

"*The elements that needed revision are:*

1. *Multi-sector framework (T2.2.): Explain the who/why/what of the framework.*
2. *It is not clear in what format Figure 14 will be delivered. How will future users be able to use this framework? What is the tool? What is the methodology?*
3. *Also take into account the electronic communications networks infrastructure parameters (e.g. network failure, etc.).*"

The points 1 and 2 in the list are addressed in Section 5 (especially in Sections **5.1**, **5.2**, **5.3**, and **5.4**), point 3 in Section **5.3** since taxonomies and security controls will take into consideration communication networks.

1.2 Structure of the document

- Section **2** summarizes the assessment of Risk Management (RM) and Assessment Methodologies (RA) and Frameworks with the focus on providing a comparative analysis able to evaluate their suitability to play the role of a starting block for the E-MAF.
- Section **3** describes the analysis of existing Cyber Security Framework adopted in the sectors of interest (health care, energy, maritime, defense and space) and summarizes the outcomes with respect to the goals of this Architectural Design Document by highlighting inter-sectoral and transversal challenges and opportunities.
- Section **4** assesses a number of current and completed projects funded by EU; these projects focus on similar goals than T2.2 or provide outcomes that T2.2 should monitor, replicate or integrate into T2.2. The section will start by analysing the other 3 pilots projects funded in 2018 Horizon 2020 cybersecurity call “Establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap". Assessment will then move to other EU funded projects dealing with cyber-risk assessment and management as well as other cybersecurity issues.
- Section **5** depicts the methodology outlined to produce the Architectural Design of the E-MAF and introduces the abovementioned design implementation by describing all the elements foreseen for the final implementation of E-MAF (tiers, layers, modules). In order to achieve this, it presents the architectural design and the underlying logical model of E-MAF and the roadmap for its implementation. This section also describes the ECHO Taxonomy, Vocabulary, and Semantics. It also describes the architectural design of the E-MAF, its logical model and implementation, the E-MAF taxonomy and vocabulary, the roadmap for the E-MAF implementation.
- Section **6** concludes the document by summarizing the main findings and way ahead.
- Annexes includes
    - T2.2 Framework and Methodologies Analysis Questionnaires limited to useful methodologies.

1.3 Relation to other work in the project

Within the scope of the ECHO project, the E-MAF is an important asset related to many elements and activities in ECHO on a twofold manner. In fact, from one side the E-MAF takes as inputs several contributions and, for this reason, closely follows fundamental activities (as T2.1, T2.3, T2.4, T2.5, see below and Section **5** for

deeper details). On the other side, it provides its outcomes as input to a long list of tasks and WPs. As an example, the ECHO consortium is prepared to include additional technology roadmaps developed in WP4 as may be identified through the application of the ECHO Multi-sector Assessment Framework.

In order to detail the contribution of E-MAF in the project, it can be pointed out that E-MAF builds on information related to:

- **Transversal aspects** produced by the detailed analysis of transversal cybersecurity challenges that appear prevalent independent of the industrial sector and identify common challenges and opportunities (T2.3).
- **Technological challenges and opportunities** provided by the application of the technology-based approach to ensure inter-sector cybersecurity and which raises both opportunities and challenges (T2.4).
- **Multi-sector dependencies** from analysis of inter-sector cybersecurity challenges on multiple sectors (T2.5).
- **StoryLines and UseCases** to use to provide results on its adoption in the domains of interest (T2.1).

Likewise, E-MAF's outputs feed into ECHO research in several ways:

- the E-MAF output is used in the **Governance Model definition** activities (WP3);
- the E-MAF output is an input to the analysis of transversal technical cybersecurity leading to a shared vision on the current and emerging technical cybersecurity challenges for the definition and the implementation of **Inter-sector Technology Roadmaps** (WP4);
- the E-MAF feeds the activities of **EWS Research, Development and Implementation** (T5.2);.
- the E-MAF contributes to **FCR (the Federated Cyber Range) Research, Development and Implementation** (T6.2);.

Moreover, the outputs produced by E-MAF application will be the input and will improve whole project outcomes in terms of:

- **Transversal aspects** by fostering the transversal cybersecurity challenges and opportunities definition through the enhancement of detailed analysis process applied to prevalent transversal cybersecurity challenges (T2.3).
- **Technology challenges and opportunities** to enhance activities ensuring inter-sector cybersecurity methodologies and improve outcomes of its application (T2.4).
- **Multi-sector dependencies** by feeding and enhancing analysis of inter-sector cybersecurity challenges prevalent and touch on multiple sectors (T2.5).
- **Cyberskills** by providing key information to develop learning-outcome based competence framework for professionals in the cyber security domain (T2.6).
- **Cybersecurity certification scheme** by fostering the matching of the diverse needs of sector specific and inter-sector issues in the development of the E-CCS (T2.7)

1.4 Applicable and reference documents

The following documents contain requirements applicable to the generation of this document:

Reference	Document Title	Document Reference	Version	Date
[GA]	Grant Agreement 830943 – ECHO	-	1.0	02/04/2019
[PH]	D1.1 Project Handbook	ECHO_D1.1_v1.41	1.41	02/05/2019
[PQP]	D1.3 Project Quality Plan	ECHO_D1.3_v1.1	1.1	31/05/2019

Table 1: Applicable documents

The following documents have been consulted for the generation of this document:

Reference	Document Title	Document Reference	Version	Date
[1]	ECHO Deliverable D2.1 - SECTOR SCENARIOS AND USE CASE ANALYSIS		1.0	31/10/2019
[2]	ECHO Deliverable D2.3 - Transversal Cybersecurity Challenges and Opportunities		1.0	31/10/2019
[3]	ECHO Deliverable D2.4 - Inter-sector Technology Challenges and Opportunities		1.0	31/10/2019
[4]	ECHO Deliverable D2.5 - Multi-sector Requirements Analysis and Definition of Demonstration Cases		1.0	31/10/2019
[5]	ECHO Deliverable D2.6 - Derivation of ECHO Cyberskills Framework and Related Trainings		1.0	31/01/2021
[6]	ECHO Deliverable D2.7 - Derivation of ECHO Cybersecurity Certification Scheme		1.0	31/01/2021
[7]	Yalcin, Nursel & Kılıç, Berker. (2019). Information Security Risk Management and Risk Assessment Methodology and Tools.	https://www.researchgate.net/publication/330170264_Information_Security_Risk_Management_and_Risk_Assessment_Methodology_and_Tools		10/2019
[8]	Agrawaln (2015) A Comparative Study on Information Security Risk Analysis Methods	http://www.jcomputers.us/vol12/jcp1201-06.pdf		30/12/2015
[9]	Ionita, Hartel, Pieters , Wieringa (2014) Current established risk assessment methodologies and tools.	https://www.researchgate.net/publication/308887387_Current_Established_Risk_Assessment_Methodologies_and_Tools		2014
[10]	Austrian IT Security Handbook	https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_au_it_security_handbook.html	2.2	11/2004
[11]	CORAS	http://heim.ifi.uio.no/~ketils/coras/index.htm http://coras.sourceforge.net		N/A
[12]	CRAMM (CCTA Risk Analysis and Management Method)	https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-	5	2003

		inventory/rm-ra-methods/m_cramm.html		
[13]	Dutch A&K Analysis	https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_dutch_ak_analysis.html	1.01	07/1996
[14]	ISAMM	https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_isamm.html	N/A	N/A
[15]	ISO27001:2013	https://www.iso.org/isoiec-27001-information-security.html		2013
[16]	ISO/IEC 27005:2018	https://www.iso.org/standard/75281.html	3	2018
[17]	ISO/IEC 27008:2019	https://www.iso.org/standard/67397.html		2019
[18]	ISO31000:2010	https://www.iso.org/iso-31000-risk-management.html		2010
[19]	ISO31000:2018	https://www.iso.org/iso-31000-risk-management.html		2018
[20]	MAGERIT	https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en	3	10/2012
[21]	Marion	https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_marion.html	N/A	1998
[22]	MEHARI	http://meharipedia.x10host.com/wp/download-mehari-2010/on-line-documents/		
[23]	MIGRA	https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_migra.html	2.1	09/2006
[24]	NIST SP800-30	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf	R1	09/2012

[25]	NIST 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems	https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final	R2	12/2018
[26]	NIST SP 800-82	https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final	REV 2	05/2015
[27]	NIST Cyber Security Framework - "Framework for Improving Critical Infrastructure Cybersecurity"	https://www.nist.gov/cyberframework/framework	1.1	04/2018
[28]	"Managing Information Security Risks: The OCTAVE Approach", C.J. Alberts and A.J. Dorofee, Addison-Wesley Pub Co	http://www.cert.org/octave/	1	09/09/2002
[29]	The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology	http://www.cert.org/octave/	2	05//2007
[30]	TOGAF Risk Assessment (based on FAIR)	https://publications.opengroup.org/c182	9.2	16/04/2018
[31]	Risk Taxonomy Standard (O-RT)	https://publications.opengroup.org/c13k	2.0	18/10/2013
[32]	Harmonized Threat Risk Assessment	https://www.h-tra.ca	N/A	N/A
[33]	Integrating Risk and Security within a TOGAF® Enterprise Architecture	https://publications.opengroup.org/g152		01/04/2019
[34]	"Risk Management: Multiservice Tactics, Techniques, and Procedures for Risk Management", Air Land Sea Application Center, FM 3-100.12, MCRP 5-12.1C, NTTP 5-03.5, AFTTP(I) 3-2.30			02/2001
[35]	"Air Force Pamphlet 90-902", "Operational Risk Management (ORM) Guidelines and Tools			12/2000
[36]	Federal Office for Information Security (BSI). "IT Baseline Protection Manual"	http://www.bsi.de/gshb/english/etc/index.htm		10/2003
[37]	"The Vulnerability Assessment and Mitigation Methodology", P.S. Antón et al., RAND National Defense Research Institute, MR-1601-DARPA	https://www.rand.org/pubs/monograph_reports/MR1601.html		2004
[38]	Common Criteria framework	https://www.commoncriteriaportal.org		
[39]	Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework	https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=13473	1.0	09/1999
[40]	Christopher J. Alberts; Audrey J. Dorofee; James F. Stevens; Carol Woody; *Introduction to*	https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=51546		08/2003

	the OCTAVE Approach. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.			
[41]	Richard A. Caralli; James F. Stevens; Lisa R. Young; William R. Wilson; *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process (CMU/SEI-2007-TR-012, ESC-TR-2007-012)*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.	https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf		05/2007
[42]	HIMSS Cybersecurity Survey	https://www.himss.org/2018-himss-cybersecurity-survey		2018
[43]	HITRUST CSF	https://hitrustalliance.net/csf-license-agreement/	9.3	15/10/2019
[44]	CIS 20 Controls	https://learn.cisecurity.org/cis-controls-download	7	03/2018
[45]	COBIT framework	http://www.isaca.org/cobit/pages/default.aspx	5	04/2012
[46]	Guidelines on high-level recommendations on maritime cyber risk management	http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx		05/07/2017
[47]	Cyber security resilience management for ships and mobile offshore units in operation	http://www.gard.no/Content/21865536/DNVGL-RP-0496.pdf		09/2016
[48]	IEC 62443 (ISO 62443-3-3 System security requirements)	https://webstore.iec.ch/publication/7033		2013
[49]	HEALTHCARE SECTOR REPORT Cyber security for the healthcare sector	https://ecs-org.eu/documents/publications/5ad7266dc1cba.pdf		03/2018
[50]	Cybersecurity Report issued by the High Level Advisory Group of the EC Scientific Advice Mechanism	https://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf		03/2017
[51]	European Cybersecurity Centres of Expertise Map, JRC Technical Report, Definitions and Taxonomy	https://publications.jrc.ec.europa.eu/repository/bitstream/JRC111441/taxonomy_final.pdf		2018
[52]	Tabansky, L. (2011). Basic Concepts in Cyber Warfare. Military and Strategic Studies 3 (1): 75–92.			2011
[53]	Wiener, N. (1948). Cybernetics or Control and Communication in the Animal and the Machine. Cambridge, MA: The MIT Press.			1948
[54]	Kaplan, F. (2016). Dark Territory: The Secret History of Cyber War. London: Simon & Schuster.			2016

[55]	Collins, J., and Futter, A. (2015) Reassessing the Revolution in Military Affairs: Transformation, Evolution and Lessons Learnt. London: Palgrave.			2015
[56]	Futter, A. (2016) Cyber Threats and Nuclear Weapons – New Questions for Command and Control, Security and Strategy. London: RUSI.			2016
[57]	Aviad A., Węcel K., Abramowicz W. (2015): The Semantic Approach to Cyber Security. Towards Ontology Based Body of Knowledge. Proceedings of the 14th European Conference on Cyber Warfare and Security (ECCWS).			2015
[58]	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union			06/07/2016
[59]	Cyber Threats to the Energy Industry	https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/ib-energy.pdf		
[60]	Papastergiou, S., & Polemi, D., MITIGATE: A dynamic supply chain cyber risk assessment methodology. World conference on smart trends in systems, security and sustainability (WS4 2017), Springer Computer Science proceedings, 15–16 Feb 2017, London.			2017
[61]	Papastergiou, S., & Polemi, D., Securing maritime logistics and supply chain: The Medusa and MITIGATE approaches. 1st NMIOTC conference on cyber security in the maritime environment, NATO Maritime Interdiction Operational Training Centre, 4–5 Oct 2016, Chania, Crete.			2016
[62]	Kalogeraki, E. M., Polemi, N., Papastergiou, S., & Panayiotopoulos, T. , Modeling SCADA attacks. World conference on smart trends in systems, security			2017

	and sustainability (WS4 2017), Springer Computer Science proceedings, 15–16 Feb 2017, London.			
[63]	Specification for security management systems for the supply chain (ISO 28000:2007): International Standardization Organization (ISO/IEC), Geneva, Switzerland			2007
[64]	Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance (ISO/IEC 28001): International Standardization Organization, Geneva, Switzerland			2007
[65]	Information security risk management (ISO/IEC 27005): International Standardization Organization, Geneva, Switzerland			2011
[66]	Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC 27001:2013): International Standardization Organization, Geneva, Switzerland			2013
[67]	Information technology — Security techniques — Code of practice for information security controls 2nd ed. (ISO/IEC 27002:2013): International Standardization Organization, Geneva, Switzerland			2013
[68]	Polemi, N., & Kotzanikolaou, P., Medusa: A supply chain risk assessment methodology. In Cyber security and privacy: Vol. 530. Communications in computer and information science. Cham: Springer			2015
[69]	Papastergiou, S., Polemi, D., & Papagiannopoulos, I., Business and threat analysis of ports' supply chain services. Special session on "innovative risk management methodologies and tools for critical information			2015

	infrastructures (CII)" within the 6th international conference on digital human modeling and applications in health, safety, ergonomics and risk management (HCI International 2015), 2–7 Aug 2015, Los Angeles, CA.			
[70]	Polemi, N., Kotzanikolaou, P., & Papastergiou, S., Design and validation of the MEDUSA supply chain risk assessment methodology and system. International Journal of Critical Infrastructures. Inderscience Publishers			2017
[71]	Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, p. 75–82.	http://data.europa.eu/eli/dir/2008/114/oj		2008
[72]	Joint Systems and Analysis Group, "Guide to Capability-Based Planning," The Technical Cooperation Program.	https://www.hsdl.org/?view&did=461818		2004
[73]	Sharon L. Caudle, "Homeland Security Capabilities-Based Planning: Lessons from the Defense Community", Homeland Security Affairs, vol. 1, no. 2 (2005).	https://www.hsaj.org/articles/178		2005
[74]	Todor Tagarev, "Capabilities-based Planning for Security Sector Transformation," Information & Security: An International Journal 24 (2009): 27-35,.	https://doi.org/10.11610/isij.2404		2009
[75]	"Capability-Based Planning," The TOGAF® Standard, Version 9.2, Chapter 28,.	https://pubs.opengroup.org/architecture/togaf9-doc/m/chap28.html	9.2	16/04/2018
[76]	Dan Shoemaker, Anne Kohnke, Ken Sigler, *A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce 2.0* (Boca Raton, FL: CRC Press)			2016
[77]	"Integrating the Disaster Risk Management Cycle," in *Science for DRM 2020: Acting Today, Protecting Tomorrow*. Disaster Risk Management Knowledge Centre, in Press.			2020

[78]	Ganin A.A., Quach P., Panwar M., Collier Z.A., Keisler J.M., Marchese D., Linkov I., "Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management," *Risk Analysis*, vol. 40, no. 1: 183-199.			2020
[79]	National Research Council, *Review of the Department of Homeland Security's Approach to Risk Analysis* (Washington, DC: The National Academies Press), Chapter 5.	https://doi.org/10.17226/12972.		2010
[80]	For additional considerations, see Chris Simmons, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Qishi Wu, AVOIDIT: A Cyber Attack Taxonomy, Technical Report CS-09-003, University of Memphis.			August 2009
[81]	ENISA's Threat Taxonomy, updated in September 2016.	https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view		2016
[82]	See "Common Language security incident taxonomy," (accessed 28 April 2020).	https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/figure11.png/view		28/04/2020
[83]	Angelo Corallo, Mariangela Lazoi, Marianna Lezzi, "Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts," *Computers in Industry* 114: 103165.	https://doi.org/10.1016/j.compind.2019.103165		2020
[84]	Maria Bada, Jason R. C. Nurse, "The Social and Psychological Impact of Cyber-Attacks," In *Emerging Cyber Threats and Cognitive Vulnerabilities*, ed. Vladlena Benson, John McAlaney (London: Academic Press), 73-92.			2020
[85]	Michel Rademaker, "National Security Strategy of the Netherlands: An Innovative Approach," *Information & Security: An International Journal*, vol. 23, no. 1: 51-61,	https://doi.org/10.11610/isij.2305		2009

[86]	Amin Z., "A practical road map for assessing cyber risk," *Journal of Risk Research*, vol. 22, no. 1: 32-43,	https://doi.org/10.1080/13669877.2017.1351467		2019
[87]	Humza Naseer, *A Framework of Dynamic Cybersecurity Incident Response to Improve Incident Response Agility*, PhD Dissertation. School of Computing and Information System, The University of Melbourne.			October 2018
[88]	George Sharkov, "From Cybersecurity to Collaborative Resiliency," 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig '16), pp.3-9,	https://doi.org/10.1145/2994475.2994484		2016
[89]	Benjamin Gittins, Ronald Kelson, "Input to the Commission on Enhancing National Cybersecurity,"	https://www.nist.gov/system/files/documents/2016/09/16/synaptic_rfi_advances-idmckm.pdf		16/09/2016
[90]	Sessika Siregar, Kuo-Chung Chang, "Cybersecurity Agility: Antecedents and Effects on Security Incident Management Effectiveness," Twenty-Third Pacific Asia Conference on Information Systems (PACIS 2019), China,	http://www.pacis2019.org/wd/Submissions/PACIS2019_paper_307.pdf		July 2019
[91]	Phil Lester, Sean Moore, "Responding to the Cyber Threat: A UK Military Perspective," *Connections: The Quarterly Journal*, vol. 19, no. 1: 39-44,	https://doi.org/10.11610/Connections.19.1.04		2020
[92]	Ludwig Leinhos, "Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr," *Connections: The Quarterly Journal*, vol. 19, no. 1: 9-19,	https://doi.org/10.11610/Connections.19.1.02		2020
[93]	Ryan Black, "WannaCry, NotPetya, and Cyberwarfare's Threat to Healthcare," IncideDigitalHealth,	https://www.idigitalhealth.com/news/wannacry-notpetya-and-cyberwarfares-threat-to-healthcare		11/06/2018
[94]	S. Gourisetti, M. Mylrea, H. Patangia, "Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis," *Future Generation Computer Systems* 105: 410-431,	https://doi.org/10.1016/j.future.2019.12.018		2020

[95]	Tang M., Alazab M., Luo Y., Donlon M., "Disclosure of cyber security vulnerabilities: Time series modelling," *International Journal of Electronic Security and Digital Forensics*, vol. 10, no. 3:255-275.	https://doi.org/10.1504/IJESDF.2018.093018		2018
[96]	Radanliev, P., De Roure, D.C., Page, K., Van Kleek, M., Cannady, S., et al., "Artificial intelligence and cyber risk super-forecasting," pre-print	https://doi.org/10.13140/RG.2.2.34704.56322		
[97]	Yu, M.; Zhuge, J.; Cao, M.; Shi, Z.; Jiang, L. "A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices," *Future Internet*, vol. 12, no. 2, 27,	https://doi.org/10.3390/fi12020027		2020
[98]	Ceccarelli A., Zoppi T., Vasenev A., Mori M., Ionita D., Montoya L., Bondavalli A., "Threat Analysis in Systems-of-Systems: An Emergence-Oriented Approach," ACM Transactions on Cyber-Physical Systems, vol. 3, no. 2, article 18,	https://doi.org/10.1145/3234513		2018
[99]	Griffy-Brown, C., Miller, H., Zhao, V., Lazarikos, D., Chun, M., "Making better risk decisions in a new technological environment," *IEEE Engineering Management Review*, vol. 48, no. 1: 77-84,	http://doi.org/10.1109/EMR.2020.2969121		2020
[100]	Polemi, N., Papastergiou, S., Assessing the Risk of Ports and Their Supply Chains: The CYSM, MEDUSA, and MITIGATE Approaches Springer International Publishing AG in E.G. Carayannis et al. (eds.), Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense.	http://doi.org/10.1007/978-3-319-06091-0_53-1		2017
[101]	The Guidelines on cyber security onboard ships.	https://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16		

[102]	CyberSec4Europe - D3.1 Common Framework Handbook 1	https://cybersec4europe.eu/wp-content/uploads/2020/05/D3.1-Handbook-v2.0-submitted.pdf	2.0	2020
[103]	NIST Special Publication 800-53 Revision 4 - Security and Privacy Controls for Federal Information Systems and Organizations	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf	4	2013
[104]	NIST Special Publication 800-53A Revision 4 - Assessing Security and Privacy Controls in Federal Information Systems and Organizations - Building Effective Assessment Plans	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf		2014
[105]	MAGERIT – version 3.0 Methodology for Information Systems Risk Analysis and Management	https://www.pilar-tools.com/doc/magerit/MAGERIT_v_3_%20book_1_method_PDF_NIPO_630-14-162-0.pdf		2014
[106]	AGARI Threat Taxonomy for cyber attacks	https://www.agari.com/email-security-blog/threat-taxonomy-framework-cyber-attacks/		
[107]	Open Threat Taxonomy	https://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a.pdf		
[108]	A Proposal for a European Cybersecurity Taxonomy	https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf	v.2	2019
[109]	Protective Project Overview	https://protective-h2020.eu/wp-content/uploads/2018/09/PROTECTIVE-Overview-Presentation-v3.0.pdf		

Table 2: Reference documents.

1.5 Intellectual Property Rights

Based on the legal framework provided in the ECHO Grant Agreement and the Consortium Agreement, ECHO specific IPR procedures have been established to protect the innovations and knowledge developed within this deliverable.

1.6 Glossary of acronyms

Acronym	Description
ADM	Architecture Development Method
CI	Critical Infrastructure
CNR	National Research Councilof Italy, Consiglio Nazionale delle Ricerche
CS	Cyber Security
CyPR	Cybersecurity Professional Register
DoS	Denial of Service

Acronym	Description
E-CCS	ECHO Cybersecurity Certification Scheme
E-MAF	ECHO Multi-sector Assessment Framework
E-MAF MIT	ECHO MAF Multi-sector Implementation Tier
E-MAF SAT	ECHO MAF Security Alignment Tier
E-MAF TFT	ECHO MAF Transversal Foundation Tier
E-MAF TFT RA/RM	ECHO MAF Transversal Foundation Tier Risk Assessment/Risk Management
ENISA	European Network and Information Security Agency
ERM	Enterprise Risk Management
FSP	Full-Scale Pilot
GA	Grant Agreement
IoT	Internet of Things
ISF	Internal Security Fund
ISM	Information Security Management
LMT	Latvijas Mobilais Telefons, Mobile Telephone company of Latvia
MRA	Risk Assessment for Cyber-physical Interconnected Infrastructures
NCSRD	National Centre of Scientific Research "Demokritos"
NIST	National Institute of Standards and Technology
OOP	Object Oriented Programming
RA	Risk Assessment
RAT	Remote access tool
RM	Risk Management
RP	Recommended Practice
SC	Supply Chain
SEB	Stakeholders Expert Board
SME	Small- and Medium-sized Enterprises
WP	Work Package

Table 3: Glossary of acronyms, initialisms and abbreviations.

2. Risk Assessment and Management Frameworks Analysis

2.1 Introduction

In order to build the E-MAF, the team analysed existing risk assessment frameworks and methodologies, in order to provide a comparative analysis with the aim to assess their suitability to constitute a starting block for the E-MAF.

The **Risk Assessment** describes the overall process including the activities listed below:

- ***Identify hazards and risk factors*** that have the potential to cause harm (hazard identification);
- ***Analyse and evaluate the risk*** associated with that hazard (risk analysis, and risk evaluation);
- Determine appropriate ways to eliminate the hazard or ***control the risk*** when the hazard cannot be eliminated (risk control).

It will be clarified in Section **4** that RA is part of Risk Management and RM cannot take place without RA. So, in the end, RA can be provided by standalone methodologies and frameworks or can be presented as part of a more comprehensive solution like Risk Management or Enterprise Architecture Frameworks. This section and the following one will analyse several solutions belonging to all these categories. An initial list of frameworks and methods for RA has been generated, taking into consideration the *work*[1] published by the European Network and Information Security Agency (ENISA), the experience of ECHO partners and other comparison initiatives from the literature (Yalcin & Kılıç, 2019 **[7]**; Agrawal, 2015 **[8]**; Ionita et al., 2014 **[9]**). Methods for general risk governance (COBIT, Basel II for example) or high-level reference documents have been excluded by default. The initial list of RA methods was counting:

- Austrian IT Security Handbook **[10]**
- CORAS **[11]**
- CRAMM **[12]**
- Dutch A&K Analysis **[13]**
- ISAMM **[14]**
- ISO/IEC 27005:2018 **[16]**
- MAGERIT **[20]**
- Marion **[21]**
- MEHARI **[22]**
- MIGRA **[23]**
- NIST SP800-30 **[24]**
- OCTAVE **[29]**
- TOGAF Risk Assessment (based on FAIR) **[30]**
- Harmonized Threat Risk Assessment **[32]**

Previously listed methods/frameworks have been analysed by taking into account a set of parameters listed in the following table. Some of these methods have been directly excluded due to the lack of basic requirements, listed with **ID 0** in the following table.

[1] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods

ID	Risk assessment frameworks/methods survey parameters
0.1	Is the Methodology clear, documented and well defined **in the English language**?
0.2	Is the Methodology still in use/updated?
0.3	Is the Methodology used in more than one country?
1	Specific Requirements. Does the Methodology…
1.1.1	... enable improvement of multi-sectoral management processes for mitigation of Cyber Security risks?
1.1.2	... assess transversal and inter-sector opportunities and challenges?
1.1.3	... enable a transversal vision for security countermeasures?
1.1.4	… use/rely on an EU Methodology?
1.1.5	… enable benchmarking initiatives?
1.2	Is the Methodology clear and well defined?
1.3	Is the Methodology open source?
1.4	Are the related Taxonomies well defined?
1.5	Are the related Taxonomies expandable?
2	**Economic factors**
2.1	Does the Methodology include a risk analysis method based on financial factors?
2.2	Does the Methodology support risk financing strategies for the residual risk?
3	**Innovation**
3.1	Towards assessment of the support to the concept of Technology Roadmap one in ECHO, does the methodology …
3.1.1	... enable analysis of a StoryLine or a UseCase from D2.1?
3.1.2	… support the provisioning of a selection of roadmaps of ways (e.g. Controls) to reduce the risk?
3.1.3	… enable/define linkability to tools/ICT products?
3.2	Does it support the concept of Curricula (like defined in ECHO)?
3.3	Does it support the concept of Certification Scheme (like defined in ECHO)?
3.4	Does the methodology identify transversal, inter-sector and specific skills for Curricula?
3.5	Does the methodology provide a basis for Training Programmes?
4	**Qualitative Analysis**
4.1	General Comments on investigated RA Framework.
4.2	Recommendations, specific aspects to be taken into consideration.

Table 4: Risk Assessment frameworks/methods survey parameters

Within the following sections, the most promising RA methods have been further analysed. ISO/IEC 27005:2018 **[16]** has been excluded from further analysis of RA methods since it is better defined as a Risk Management framework, tightly related to ISO 31000:2018 **[19]**,

The principal frameworks/methodologies providing Risk Management/Assessment that will be analysed in these paragraphs can be grouped as follows:

- Risk Management Methodologies (Section **2.2**)
  - **ISO 31000:2018 Standard[19]** which is an international standard related to Risk Management;

- Enterprise Architecture Frameworks (Section **2.3**)
  - **TOGAF [33]**, an open standard, whose main methodology of Risk Assessment is TOGAF RA **[30]** based on FAIR;
- Risk Management Frameworks (Section **2.4**)
  - **NIST Risk Management Framework** (SP 800-37**[25]**), comprising the **NIST Risk Assessment Framework [27]** (SP 800-30**[24]**, strictly bound to SP 800-53 **[103]** and SP 800-53A **[104]**, see Section **2.4**). They are both included in the **NIST Cybersecurity Framework [27]**, open standard to critical infrastructure;
- Other Risk Assessment Methods (Section **2.4**)
  - **MEHARI** Risk Assessment Method **[22]** (Section **2.5.1**);
  - **Magerit[20]** (Section **2.5.2**)
  - **Octave[28] [29]** (Section **2.5.3**)

At the end of this section it will be demonstrated how the framework, methods and methodologies which are assessed in the following subsections can be taken as inspiration for the E-MAF but no one of them can be fully adopted. So, this justified the choice made to implement E-MAF based on a different proprietary methodology.

2.2 ISO 31000 Risk Management Methodology

The UNI ISO 31000 **[18][19]** is the international standard that provides a common approach for the management of any type of risk (from strategic to operational, currency, market, compliance, etc.) and the proactive improvement of the management efficiency of the company through a model which can be integrated into the business management system.

This standard, born in 2009 **[18]** and further improved during 2018 **[19]**, provides a complete set of principles and guidelines to help organizations carry out risk assessment and analysis. ISO 31000 is structured according to a new approach to risk-based thinking that is planning and assessing risks in the meaning of “opportunity”. In fact, with the statement “the purpose of risk management is the creation and protection of value”, a high concept of risk management is expressed in order to ensure that the company continues to persist and develop over time. This principle is then completed with the second one: “risk management is an integral part of all organizational activities”, that is it pervades all processes and related managers.

It was developed by a range of stakeholders and is intended for use by anyone who manages risks, not just professional risk managers, to provide best-practice structure and guidance to all operations concerned with risk management for any industry group, management system or subject matter field. The challenge for risk professionals is to rearrange the guidance in ISO 31000 to align with their own approach to implementing a risk management initiative. In other words, ISO 31000 clearly states that risk management is an open-ended process designed to be highly customized and tailored to the individual needs and contexts of the organization implementing it.Table 5enlists a comparison between strength and weak points for the discussed methodology.

N.	Pros	Cons
1	RM is intended to be systematic	Resources are requested to RM operation
2	Iterative evaluation of the level of security	
3	Can model any type of risk, company, sector	Need adaptation in order to assess transversal and inter-sector opportunities
4		Does not describe any type of Risk
5	Does not define taxonomies (reference to external ones)	Does not define taxonomies (reference to external ones)

N.	Pros	Cons
6	Provides general indications for the setup of financial factors	
7	Supports risk financing strategies for the residual risk	
8	Provides a basis for Training Programmes	
9	Supports the concept of Technology Roadmap	It is not evident how it could be linked to the concept of Technology Roadmap in ECHO
10		Does not enable/define step-by-step checklists to implement the RA process.
11		Does not support the concept of Certification Scheme and Curricula
12		Does not identify transversal, inter-sector and specific skills for Curricula.
13		Does not rely on any EU Risk Assessment Methodology
14	Is clear and well defined	Is not open source and only available on purchase

Table 5: Pros and Cons of ISO 31000:2018

Finally, "risk management is and must be systematic, structured and timely", implies that risk management is not conditioned by moods or priorities, but it is a continuous activity, which should not be improvised but designed on a solid foundation.

The emphasis is on the continuous improvement of risk management through setting goals for the organization, measuring, reviewing and subsequently modifying processes, systems, resources, capabilities and skills. The ISO 31010 provides guidance on the selection and application of risk assessment methods in a wide range of situations. Methods are used to assist in decision making when uncertainty exists, to provide information on specific risks and as part of the risk management process[2].

Once the risks have been identified (included cyber security risks), analyzed, and evaluated, the appropriate risk treatment should be applied to reduce, remove, or retain each risk depending on a range of factors. Residual risk should be considered in all cases where a risk has been determined as essential or unavoidable. There may be several options to mitigate risk to reduce the likelihood, consequence, or severity of a risk incident, and these may flow one to another for continuous risk mitigation.

Implementing ISO 31000 also helps organizations see both the positive opportunities and negative consequences associated with risk, and allows for more informed, and thus more effective, decision making, namely in the allocation of resources. It can be an active component in improving an organization's governance and, ultimately, its performance.

ISO 31000 can be modelled on any type of risk, sector and company type, and to be truly effective must be adapted to the organization in order to assess transversal and inter-sector opportunities and challenges helping organizations to increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment[3].

The standard describes the steps, approaches, methods for identifying and assessing risk, but does not describe the types of risks. In fact, this is a plan-to-do-check, which describes the steps to prevent, assess

[2] https://quality.eqms.co.uk/blog/iso-31000-developing-your-risk-treatment-strategy
[3] https://www.4clegal.com/opinioni/standard-iso-31000-nove-anni-dopo

and analyze risk. There are no taxonomies in the standard, but there is an explicit reference to external taxonomies of risks for categories, which can be expanded:

- Business processes;
- Capital infrastructure;
- Communications;
- Conflict of interest;
- Financial management;
- Governance and strategic direction;
- Human resources management;
- Information management;
- Information technology;
- Knowledge management;
- Legal;
- Organizational transformation and change management;
- Policy development and implementation;
- Privacy / Information stewardship;
- Program design and delivery;
- Project management;
- Political;
- Reputational;
- Resource management;
- Stakeholders and partnerships;
- Values and ethics.

Through the use of the proposed guidelines, practitioners any level of expertise can benchmark their risk management organization and practices against a recognized international reference[4].

The methodology also defines a risk analysis method providing general indications for the setup of financial factors though the definition of financial risks arising from market trends, changes in customer and supplier conditions, etc. and makes arguments in terms of economic losses, and supporting risk financing strategies for the residual risk. In fact, the standard examines the organization's external context to include financial factors (*5.4.1* Understanding the organization and its context), proposes to consider the nature and value of assets and resources as a factor for identifying uncertainties that may affect one or more objectives (*6.4.2* Risk identification) and proposes to consider cost as a factor for reporting.

ISO 31000 provides a basis for Training Programmes; in fact in Section 5.4.4 (Allocating resources) is stated that:

- Top management and oversight bodies, where applicable, should ensure allocation of appropriate resources for risk management, which can include, but are not limited to:

    - people, skills, experience and competence;
    - the organization's processes, methods and tools to be used for managing risk;
    - documented processes and procedures;
    - information and knowledge management systems;
    - professional development and training needs.

[4] https://www.riskope.com/2010/11/10/new-iso-31000-risk-management-principles-and-guidelines/

The organization should consider the capabilities of, and constraints on, existing resources[5].

The ISO 31000 supports the concept of Technology Roadmap providing a range of risk treatment options, including but not limited to:

- Remove the risk altogether;
- Change the likelihood (such as move servers to a higher floor to reduce risk of flood damage);
- Change the consequences;
- Share the risk through agreements, partnerships, further insurance etc.;
- Retain and mitigate the risk by informed decision.

Residual risk should be considered in all cases where a risk has been determined as essential or unavoidable. There may be several options to mitigate risk to reduce the likelihood, consequence, or severity of a risk incident, and these may flow one to another for continuous risk mitigation[6].

Applying the ISO 31000 methodology to analyse the situation that occurred in the office described in D2.1 **[2]**, it shows insufficient staff knowledge of security and possible risks. If the provisions of paragraphs on health care, maritime, energy scenarios (see 6.3, 6.4, and 6.5 in D2.1) were met, the consequences of cyberattacks could be avoided and mitigated. When a vulnerability was detected at the first manifestation of an attack, it was necessary to disconnect the router from the power supply, and then take measures to detect malicious actions and eliminate them. Application of the standard would allow creating an action plan in case of various types of attacks, to choose criteria of risks, assess and analyse possible risks.

Unfortunately, the standard does not enable/define step-by-step checklists to actually implement the risk assessment process neither is evident how it could be linked to the concept of Technology Roadmap in ECHO. Moreover, it does not rely on any EU Risk Assessment Methodology, nor support either the concept of Certification Scheme, of Curricula neither identify transversal, inter-sector and specific skills for Curricula. In fact ISO 31000 is a set of guidelines, not requirements. Many ISO standards, like ISO 9001, and ISO 14001, are requirements, which means they compose a strict set of specifications that can be certified to. ISO 31000 is not like that; it is not possible to be certified to. It's simply a set of best practice guidelines[7].

Although not being open source, and only available on purchase8, the standard contains much valuable information and it represents robust, high-level guidelines for the management of risk. Moreover, it is clear and well defined and was improved over the time with the last available revision dated 2018, which maintain and simplifies the previously defined concepts, making them clearer and therefore more usable.

2.2.1 Risk Assessment in ISO 31000:2018

The **ISO 31000:2018 standard [19]** is a family of standards relating to Risk Management, where the Risk Assessment has a fundamental role. The first step is about the definition of the context of the organisation and the scope of the risk management strategy and the identification and development of the risk criteria. These criteria are designed to establish the way risks are recognized and recorded. Therefore, the next step of the framework is Risk Assessment that is composed of **Risk Identification**, **Risk Analysis** and **Risk Evaluation** respectively devoted to identifying risks, analyse them and evaluate the effectiveness of risk criteria. In ISO 31000, the RA process is foreseen to be systematic, iterative and collaborative. This is also reached through the provisioning of a fully integrated comprehensive and integrated risk management service and strategy,

[5] https://www.academia.edu/40159111/Risk_management_-Guidelines_Management_du_risque_-Lignes_directrices
[6] https://quality.eqms.co.uk/blog/iso-31000-developing-your-risk-treatment-strategy
[7] https://www.process.st/iso-31000/
[8] https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

requiring the involvement of key internal and external stakeholders in RA. The perfect strategy must be derived in fact from broad experience, high-level competences and deep knowledge of the key elements in the field.

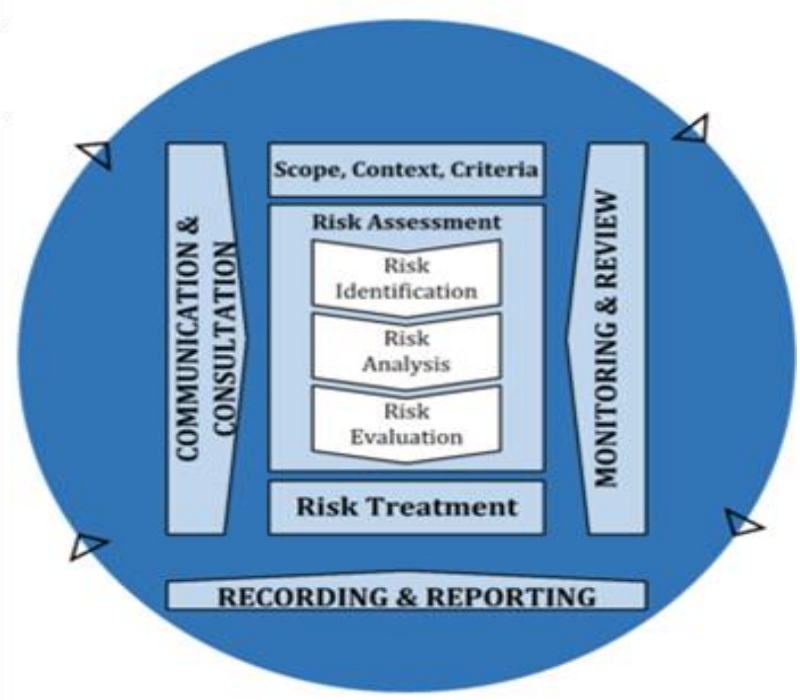

Figure 1: Risk Management process in ISO 31000:2018 [19].

Risk Identification

The Risk Identification is the stage in Risk Assessment where the list of possible risks is produced. Identification may happen depending on several factors, which may affect an organisation. As a reference, Qualsys[9] introduces the following list[10]:

- *Tangible and intangible sources;*
- *Causes / events;*
- *Threats and opportunities (even positive risks need to be assessed);*
- *Existing capabilities for handling risk, and any vulnerabilities;*
- *Contextual changes, such as alteration to an external factor;*
- *Resources available, the nature and value of such;*
- *The likelihood and consequences of a risk;*
- *The severity of a risk should it occur;*
- *Knowledge gaps;*
- *Time resources and allocation of risk management team;*
- *The bias, experiences, and assumptions of stakeholders involved in risk assessment.*

Moreover, when identifying a risk, it's important to note that there may be more than one outcome to a risk occurrence – and that this may impact upon further identified risks.

[9] https://qualsys.co.uk/
[10] source https://quality.eqms.co.uk/blog/iso-31000-risk-assessment

Risk Analysis

Risk Analysis is a fundamental phase to support decision-making process since it provides information on risks from which risk treatment and definition of organisation attitude and needs to risk can be derived. The analysis keeps into consideration a set of values (a *triplet*, as named in the following sections in the aim of E-MAF methodology):

- Risk type,
- Risk level,
- Risk likelihood.

The ISO 31000 methodology opens to the application of several risk analysis methods and techniques, depending on the organisation choices and needs. As an example quite often a combination of qualitative, semi-quantitative, or quantitative approach is used (as it will be depicted for E-MAF case). Usually, a full qualitative analysis or a semi-quantitative one are also valid choices depending on the real case. What is clearly important is to analyse the risk by inspecting internal and external factors, resources, and effects/influences. Also the ranges and the scales defined to measure the risk level are fundamental for an adequate risk analysis process.

Risk Evaluation

A risk is usually evaluated through a set of criteria and measures in order to complement the work performed during Risk Analysis and provide support to risk mitigation/governance in terms of decisions on treatment and priority. Risk Evaluation enables a smart decision-making process, if it is able to define a set of effective criteria through which (together with prioritization and treatment) the Risk Analysis process can be validated successfully. Risk Evaluation provides very important information on the need to analyse risks further, update or keep the security controls in place, estimate the effectiveness of risk strategy (e.g. objectives of organisation change during its lifetime, and if they change the risk strategy must necessary be adapted). Evaluation should be seen as a regular process which positively contributes to a continuous risk management process.

2.3 TOGAF Enterprise Architecture Framework

In TOGAF Standard, Risk Management is defined "*as a technique used to manage risk during an architecture transformation project. It is therefore an integral part of Enterprise Architecture*" **[30]**, where the term Enterprise means whatever be a collection of organisations dealing with common goals and objectives. TOGAF is a standard implementing a framework for Enterprise Architecture, providing solutions (tools, methods, etc.) to support the four phases which are typical for an Enterprise Architecture:

- Acceptance
- Production
- Use
- Maintenance.

The Standard aims to improve and refine the quite fragmented legacy of processes turning it into a highly integrated environment effectively responding to changes and fostering "*implementation of the business strategy*" **[30]**.

Five main activities are involved in Risk Management:

1) Risk Classification, in order to enhance and speed risk mitigation processes up, through a set of risk categories. Examples are the following: scope, environment, technology, complexity, time, etc.
2) Risk Identification, to identify and describe the potential risks for the project/organisation.
3) Initial Risk Assessment, in order to assess the level of risk at the beginning of Risk Management process. Four levels were set for the level of risk and five for the potential frequency of it. The risk can be:
    a. Catastrophic,
    b. Critical,
    c. Marginal, or
    d. Negligible.

    As regards the frequency, the levels are:
    e. Frequent,
    f. Likely,
    g. Occasional,
    h. Seldom,
    i. Unlikely

    The meaning of the levels described above will be explained later in this section.
4) Risk Mitigation, aimed to theoretically zero and quite often practically reduce the risk, through the adoption of mitigation actions. In case the risk remains after identification, planning and conduct of mitigation actions the non-mitigated risk is named “residual risk”.
5) Risk Monitoring, which tracks the whole process of Risk Management; monitoring enables fast identification of new upcoming risks and of the corresponding strategies to manage them.

Security and risk management are getting little attention in TOGAF standard. It limits the scope of risk management to risks associated with the architectural project itself.

The Guide “*Integrating Risk and Security within a TOGAF® Enterprise Architecture*” **[33]** describes how to integrate security and risk into an Enterprise Architecture. This Guide defines risk, in line with ISO 31000:2010**[18]**, that is “the effect of uncertainty has on the achievement of business objectives” and the uncertainty concerns the possibility of future outcomes.

Therefore, every decision is based on assessing the balance between positive and negative outcomes, the likelihood of beneficial outcomes with respect to harmful outcomes, the magnitude of these positive or negative events, and the likelihood associated with each identified outcome.

“Risk assessment” refers to the identification and evaluation of all these factors. “Risk management” concentrates on identifying and controlling events that have the potential of causing unwanted change. The purpose of risk management is, therefore, to mitigate negative risk, rather than maximize positive outcomes.

The TOGAF standard describes one method of administrating the result of a risk assessment, but not include the act of assessing risk and the ways to do. The current approaches to risk assessment use either qualitative or quantitative means to measure, estimate and express risk. A qualitative risk assessment delivers a listing of relevant risk scenarios with a high-level prioritization (high – medium - low), whereas a quantitative approach seeks for numeric determination of the risk. This is usually based on identified threats, their likelihood of occurring, and the impact of an incident. A deliverable of a risk assessment is the Business Risk Model, a Risk Register, which determines the cost (both qualitative and quantitative) of asset loss in failure cases.

The TOGAF Standard includes a content framework to drive greater consistency in the outputs that are created when following the Architecture Development Method (ADM). The TOGAF content framework provides an

integrated approach of Enterprise Risk Management and it has a modular structure. The modular structure supports:

- Greater usability – defined purpose for each part; can be used in isolation as a standalone set of guidelines;
- Incremental adoption of the TOGAF standard.

As stated in **[33]**, "*ADM is composed by the Enterprise Architecture (including Security Architecture), and it is all about aligning business systems and supporting information systems to realize business goals in an effective and efficient manner (systems being the combination of processes, people, and technology)*".

Quality, in TOGAF case, derives also from the information security process. Formerly threaten as an isolated aspect, thanks to the introduction of the concept of Security Architecture information security started to be considered as an integrated part of Enterprise Architecture. A security architecture comprises a structured set of components (physical, logical, conceptual and organizational ones) coherently interacting in order to achieve/maintain a given state of managed risk and information security **[33]**. The TOGAF structure is shown in the following figure, also depicting the relationships between the Enterprise Architecture and the Enterprise Security one.

In the central column, the core security and risk concepts complementing the TOGAF standard in the aim of Information Security Management (ISM) and Enterprise Risk Management (ERM) are underlined.

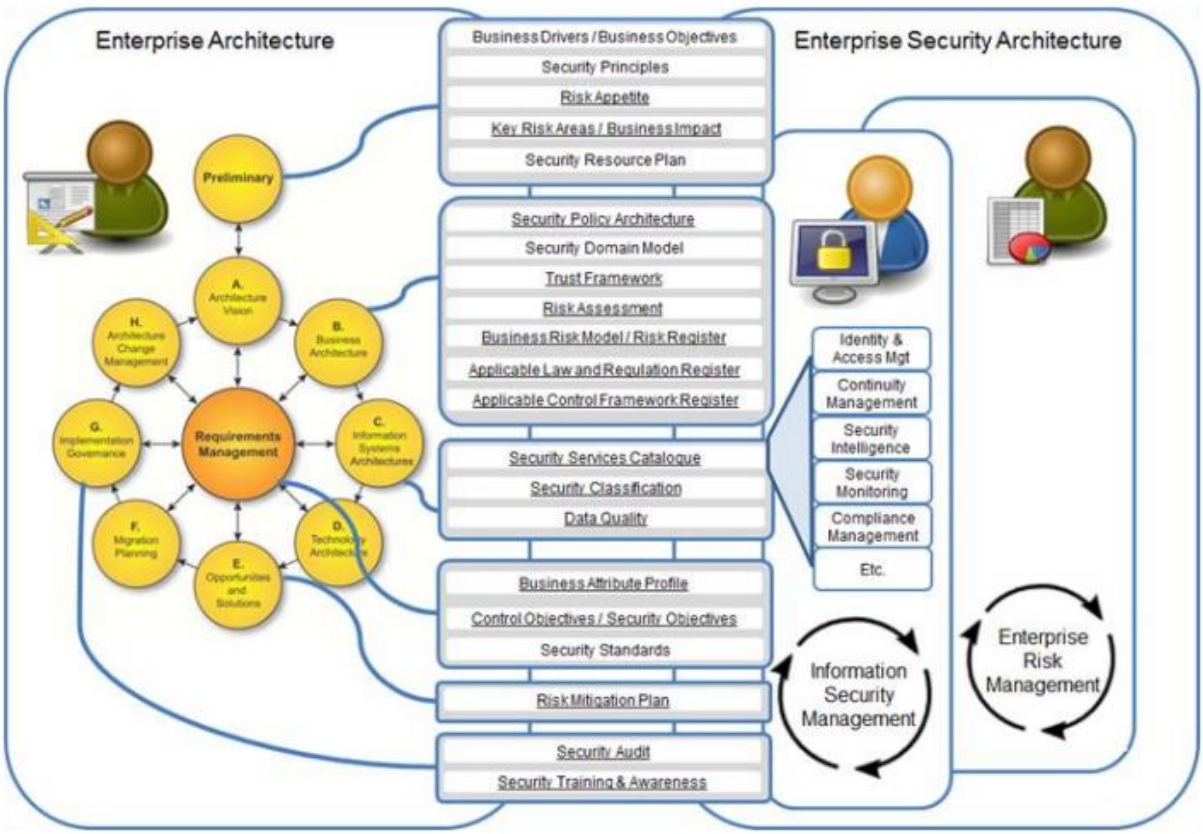

Figure 2: Essential Security and Risk concepts in TOGAF Enterprise Architecture [34].

In TOGAF, RA aims to determine *the risks that are relevant to an asset or objective***[33]** and comprises two phases:

- **Initial Risk Assessment**, classifying risks with respect to the combination of frequency and effects to provide a preliminary assessment, and
- **Residual Assessment** after Risk Mitigation.

As of initial assessment, no hard and fast rules are available to measure effects and frequencies. So, in the following the RM best practices are reported as described in **[33]**.

Effects are assessed through the four criteria listed below:

- ***Catastrophic:*** *infers critical financial loss that could result in the bankruptcy of the organization;*
- ***Critical:*** *infers serious financial loss in more than one line of business leading to a loss in productivity and no return on investment on the IT investment;*
- ***Marginal:*** *infers a minor financial loss in a line of business and a reduced return on investment on the IT investment;*
- ***Negligible:*** *infers a minimal impact on a line of business' ability to deliver services and/or products.*

Frequency are estimated as follows:

- ***Frequent****: likely to occur very often and/or continuously;*
- ***Likely****: occurs several times over the course of a transformation cycle;*
- ***Occasional****: occurs sporadically;*
- ***Seldom****: remotely possible and would probably occur not more than once in the course of a transformation cycle;*
- ***Unlikely****: will probably not occur during the course of a transformation cycle.*

The combination of effect and frequency factors represents the **Impact** to be determined through an heuristic and consistent classification scheme for the risks. A potential classification scheme base on a 4 level range could be based on the following values:

- ***Extremely High Risk (E)****: the transformation effort will most likely fail with severe consequences;*
- ***High Risk (H)****: significant failure of parts of the transformation effort resulting in certain goals not being achieved;*
- ***Moderate Risk (M)****: noticeable failure of parts of the transformation effort threatening the success of certain goals;*
- ***Low Risk (L)****: certain goals will not be wholly successful.*

By using the classification scheme listed above, impacts can be derived using the following Risk Classification Table.

Corporate Risk Impact Assessment					
Effect	Frequency				
	Frequent	Likely	Occasional	Seldom	Unlikely
Catastrophic	E	E	H	H	M
Critical	E	H	H	M	L
Marginal	H	M	M	L	L
Negligible	M	L	L	L	L

Table 6: The Risk Classification Scheme [33].

After the proper/selected mitigation action has been applied for each one of the risks, it is necessary to re-assess all of them. So, effects and frequencies have to be recalculated and the foreseen impacts estimated again. The comparison between the initial and the residual risk values could measure the added value of the mitigation action. The core concept is that mitigation reduces the impact and does not leave the risk at the same level. In order to check this, a table similar to the following one should be calculated after the RA.

Risk ID	Risk	Preliminary Risk			Mitigation	Residual Risk		
		Effect	Frequency	Impact		Effect	Frequency	Impact

Table 7: Risk Identification and Mitigation Assessment Worksheet [33].

2.3.1 TOGAF RA Methodology

The main methodology of Risk Assessment is TOGAF RA which has the objective to enable risk analyst to perform effective information security risk analysis using the Factor Analysis of Information Risk (FAIR) framework. When coupled with the Risk Taxonomy Standard **[31]**, it provides risk analysts with the specific processes necessary to perform effective FAIR-based risk analysis. This Standard has the following functions:

- Educate information security, risk, and audit professionals;
- Establish a common language for the information security and risk management profession;
- Introduce rigor and consistency into the analysis, which sets the stage for more effective risk modelling;
- Explain the basis for risk analysis conclusions;
- Strengthen existing risk assessment and analysis methods;
- Create new risk assessment and analysis methods;
- Evaluate the efficacy of risk assessment and analysis methods;
- Establish metric standards and data sources.

Moreover, this RA Standard defines the FAIR taxonomy for the factors that drive information security risk and it is intended to be applied toward the problem of managing the frequency and magnitude of loss that arises from a threat (whether human, animal, or natural event). The Risk Analysis Process consists of four phases:

- Identify Scenario Components (Scope the Analysis);
- Evaluate Loss Event Frequency (LEF);

- Evaluate Loss Magnitude (LM);
- Derive Cyber Risk.

It is important that the analyst clearly documents their key assumptions to ensure all that those who review the analysis understand the basis for the values that were used. One area where therefore documenting all assumptions is vital is within the identification of the components of the analysis. The first step is identifying the IT asset, the threats and the vulnerabilities, in order to define the scenario analysis and, consequently, the Loss Event Frequency (LEF) and the Loss Magnitude (LM).

During the scoping of the analysis multiple scenarios are generated considering some common characteristics as the motives, the objectives, the access method or the awareness of the resources.

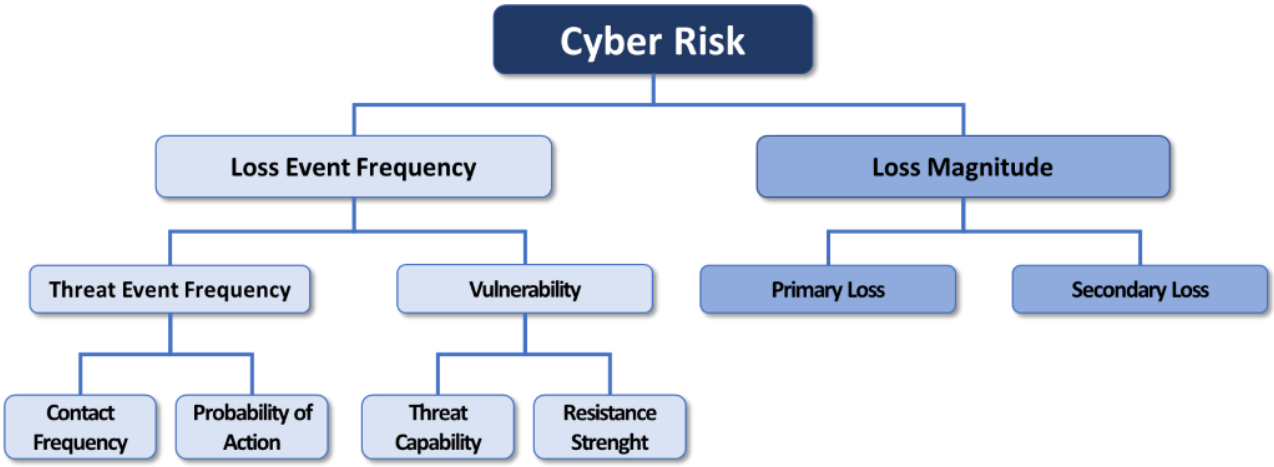

Figure 3: TOGAF RA Hierarchical Structure [31].

It is possible to start deriving LEF at three different layers of abstraction. To leverage the top-down approach it should first be considered whether we are able to make defensible estimations at the high level itself (for example LEF). If the detected loss event has occurred in the recent past, then we may be able to put our estimations directly at the LEF. Instead, if there aren't data on past loss events, or if factors have changed, the analyst should step down one layer and attempt to work at Threat Event Frequency (TEF) and Vulnerability (Vuln). Another additional consideration around which level of abstraction the analyst should work at is based on the purpose of the analysis. For instance, if the evaluation presents several different control options and are looking to identify which option is most effective from a risk reduction perspective, then deriving Vuln by analyzing Resistance Strength (RS) and Threat Capability (TCap) may be most appropriate.

In summary, the appropriate level of abstraction to use in an analysis will usually be determined by:

- ***The purpose of the analysis***. If the analysis will be performed multiple times to assist in determining the effectiveness of a new control, then we should work at a lower level (e.g., RS) where the change can be more objectively and accurately estimated.
- ***The type and quality of data*** at hand and/or the amount of time available to the analyst – deeper levels of analysis take longer. The benefit of working higher in the taxonomy is increased efficiency, and when there is data it often is more objective in nature.

A Loss Event Frequency (LEF) estimate would be based upon how frequently the loss event has or can be estimated to occur within a given timeframe. As mentioned above, estimating the LEF is straightforward if the loss event for the scenario has occurred multiple times in the past. Recognizing that the risk landscape is dynamic and threats, as well as organizational controls, may change and for this, it is important to be mindful

when using historical event data to estimate LEF directly. For example, if the organization has implemented several new controls as a result of an event in the past, these new controls may impact either the Threat Event Frequency (TEF) or Vulnerability (Vuln) of the organization to the threat. If this is the case, as always, it may be more comfortable to make estimates at lower levels of the taxonomy. In fact, due to the prevalent absence of historical data in this domain, it's very difficult to estimate directly the LEF. Therefore, the estimate of the LEF is based on the attribution of a qualitative-quantitative score of the likelihood of the threat event, through the analysis of TEF and Vuln. The TEF is estimated through the Contact Frequency (CF) and the Probability of Action (PoA), analyzing the motivations and the frequencies of various cybercrimes in the domain. Instead, the Vuln analyses the difference between the force that's likely to be applied, and the asset's ability to resist that force and it is derived from the analysis of the Threat Capability (TCap) and the Resistance Strength (RS). Threat Capability (TCap) refers to the threat agent's skill (knowledge and experience) and resources (time and materials) that can be brought to bear against the asset. The estimates of the skill and resources (time) is relative to every scenario. Resistance Strength (RS) has to do with an asset's ability to resist compromise. Also the estimates of this term are relative for every scenario.

Then, at the same time of the estimate of LEF as described above, the loss if an event does occur are analysed. In determining of the Loss Magnitude (LM), FAIR uses an approach of differentiating Primary and Secondary Loss. The estimate of Primary Loss can focus on Misuse (for example identity theft), Disclosure or Deny Access (for example destruction) that are a common concern. In some cases, it may be necessary to evaluate the loss associated with more than one threat action in order to decide which one has the most significant loss potential. This is often possible within the same analysis when performed quantitatively. A useful tip in determining which forms of Primary Loss (e.g., productivity, response, replacement, etc.) may be applicable is by leading discussions with individuals within the organization that typically respond to or manage negative events. This is especially important for loss events that may have not occurred in the past. These discussions around the types of organizational involvement and loss when a given loss event materializes help to ensure that all forms of loss are evaluated, and estimates are accurate. The estimates of the Secondary Loss is to identify which, if any, secondary stakeholders would be relevant to every scenario. In other words, identify who, outside of the organization, might react negatively in a manner that would generate additional loss. For example, for a financial institution, the most common secondary stakeholders of interest are customers, regulators, and shareholders.

At the end of the estimates of LEF and LM of every scenario generated, the related cyber risk is determinate through a heat map of risk.

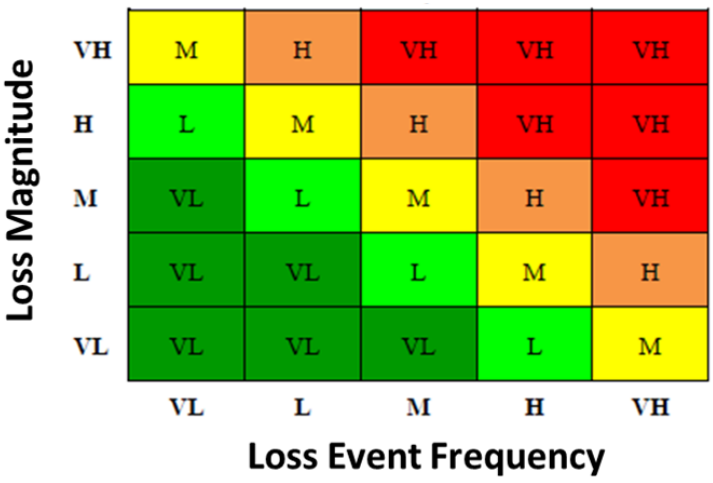

Figure 4: Heat map of risks for TOGAF.

2.4 NIST Risk Management Framework

The National Institute of Standards and Technology is a U.S organisation, part of the U.S Department of Commerce. Its mission is to provide innovation and industrial competitiveness through technical leadership. NIST laboratories develop measurements and standards for government and industry. NIST standards are widely used outside the U.S and thus is relevant to the ECHO project. The NIST Special Publication 800-series provides standards and guidelines for information security for U.S government and industry **[24]**.

Special Publication 800-30**[24]** provides guidance for carrying out each of the steps in the risk assessment process (i.e., preparing for the assessment, conducting the assessment, communicating the results of the assessment, and maintaining the assessment).The SP-800 series supports a unified information security framework that includes the following risk management activities:

- Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View;
- Special Publication 800-37**[25]**, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach;
- Special Publication 800-53**[103]**, Recommended Security Controls for Federal Information Systems and Organizations;
- Special Publication 800-53A**[104]**, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans **[24]**.

Special Publication 800-39 provides guidance for an overall risk management process to manage information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the national government resulting from the operation and use of government information systems. SP 800-39 defines risk management as a comprehensive process that requires organizations to:

(i) frame risk (i.e., establish the context for risk-based decisions);
(ii) assess risk;
(iii) respond to risk once determined; and
(iv) monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations **[24]**.

(i) Establishes the context and provides a common perspective on how organizations manage risk. Risk framing produces a risk management strategy that addresses how organizations intend to assess risk, respond to risk and monitor risk.

(ii) Addresses how organizations assess risk within the context of the organizational risk frame. The objective is to identify: threats to organizations, vulnerabilities internal and external to organizations, the harm and the likelihood that harm will occur.

(iii) Risk response aims to provide a consistent, organization-wide response to risk in accordance with organizational risk frame.

(iv) Risk monitoring is the process of evaluating risk process effectiveness throughout the project and tracking identified risks **[24]**.

2.4.1 Overview of the SP800-30 Risk Assessment Process

SP 800-30**[24]** details the risk assessment component of risk management - providing a detailed step-by-step process for organizations on how to:

1. prepare for risk assessments;
2. conduct risk assessments;
3. communicate risk assessment results to key organizational personnel; and
4. maintain the risk assessments over time.

The NIST Risk Assessment is composed of **four steps**: prepare for the assessment (STEP 1); conduct the assessment (STEP 2); communicate assessment results (STEP 3); and maintain the assessment (STEP 4). The NIST Risk Assessment describes:

- High-level overview of the risk assessment process,
- Activities necessary to prepare for risk assessments
- Activities necessary to conduct effective risk assessments
- Activities necessary to communicate the assessment results and share risk-related information
- Activities necessary to maintain the results of risk assessments on an ongoing basis.

The following Figure illustrates the basic steps in the risk assessment process and highlights the specific tasks for conducting the assessment.

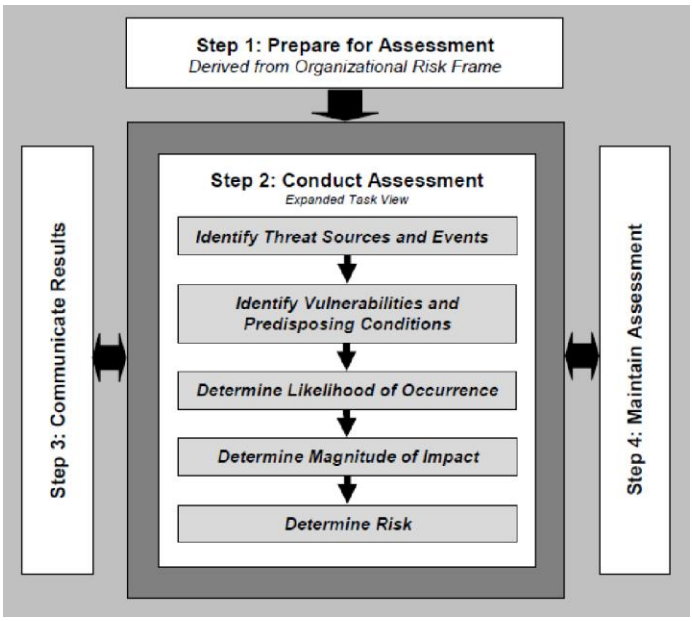

Figure 5: SP 800-30 Risk assessment procedure [24].

The first step is to PREPARE for the assessment and has the purpose to establish a context for the risk assessment. This context is established by the results from the risk framing. Preparing for a risk assessment includes the following tasks:

- Identify the purpose and the scope of the assessment
- Identify the assumptions associated with the assessment
- Identify sources of threat, vulnerability to be used in the risk assessment

- Identify the risk model and analytic approaches to be employed during the assessment.

The second step is to CONDUCT the assessment. The objective is to produce a list of information security risks that can be used to inform risk response decisions. Conducting risk assessment includes the following specific tasks:

- Identify threat sources that are relevant to organizations
- Identify threat events that could be produced by those sources
- Identify vulnerabilities within organizations that could be exploited by threat sources
- Determine the probability that the threat sources would initiate specific threat events
- Determine the adverse impact to organizational operations; determine information security risks **[24]**.

The third step is to COMMUNICATE the assessment results and SHARE risk-related information with the purpose to ensure that decision makers across the organization have an appropriate risk related information needed to inform and guide risk decision.

The fourth step is to MAINTAIN the assessment. Maintaining risk assessment includes the following tasks: monitor risks factor and update the component of risk assessment reflecting the monitoring activities carried out by organizations **[24]**.

NIST declares explicitly that the concepts and principles associated with the risk assessment processes and approaches contained in this publication are intended to be similar to and consistent with the processes and approaches described in International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) standards and report as reference standards:

- ISO/IEC 31000:2009, Risk management – Principles and guidelines;
- ISO/IEC 30101:2009, Risk management – Risk assessment techniques;
- ISO/IEC Guide 73, Risk management – Vocabulary;
- ISO/IEC 27005:2011, Information technology – Security techniques – Information security risk management.

The steps depicted in Figure 4 remind clearly the methodology described in ISO 27005.

The threats and vulnerability taxonomies are weakly defined. Asset categories or asset catalogue are not defined at all.

A *threat* is characterised by a *threat event* and a *threat source*.

An exemplary taxonomy of threat sources by type, description, and risk factors (i.e., characteristics) is given, distinguishing between *adversarial* and *non-adversarial* (accidental, structural, environmental) sources.

Adversarial threats sources are characterised by *capability, intent, targeting*. *Non-adversarial threat* sources are characterised by a *range of effects*. A reference scale for assessing each characteristic for each threat source is given as a customizable example, with a description of the criteria for assigning a certain score/qualitative value. These scales are used to assess the risk factors associated to the threat source. **[24]**

Similarly, an exemplary taxonomy of threat events is provided. They are also distinguished in adversarial and non-adversarial. The adversarial threat event is described based on their TTP (tactics, techniques and procedures) characteristics and is identified following the flow of an APT campaign. A list of non-adversarial threat events is also provided. An exemplary assessment scale for the relevance of those threat events is provided.

Threat characterization	Adversarial	Non-adversarial
Source	capability, intent, targeting	Range of effects
Event	By TTP, following a typical APT flow	List

Table 8: Threat characterization

Vulnerabilities are seen as weaknesses that can affect not only a system but also a governance element (procedures, roles…). In addition to vulnerabilities, the document defines also "predisposing conditions". A predisposing condition is a condition that exists within an organization, a mission or business process, enterprise architecture, information system, or environment of operation, which affects (i.e., increases or decreases) the likelihood that threat events, once initiated, result in adverse impacts. For example, the location of the data centre in an area subject to earthquakes. The guideline does not provide a taxonomy for vulnerabilities but only for predisposing conditions, that are organised in three categories: information-related, technical, operational/environmental. The exemplary assessment scales are provided, based on:

- Severity in case of vulnerability;
- Pervasiveness in case of predisposing conditions.

Assessment scales for the evaluation of likelihood and impact of a threat event are provided, but they are quite generic and the criteria to assess the level of impact or likelihood have to be tailored by the risk analyst based on the organization and the context of the risk assessment.

The document provides general inputs on sources for information related to threat sources, threat events, vulnerabilities and predisposing conditions.

This guideline does not specify algorithms for combining semi-quantitative values. Organization-specific risk models should define algorithms (e.g., formulas, tables, rules) for combining risk factors (assessment scales combination).

To integrate the risk management process throughout the organization, a three-tiered approach is employed that addresses risk at the:

(i) Tier 1: organization level;
(ii) Tier 2: mission/business process level; and
(iii) Tier 3: information system level **[24]**.

Risk assessments can be conducted at all three tiers in the risk management hierarchy—organization level, mission/business process level, and information system level.

The results of the risk assessment conducted at each layer can feed the others, but it is not clear if it is possible to connect risks at information level with the risk at business and organization level, indeed it is extremely important understand how security risks can impact the business and, vice versa, how business and organizational issues can be caused by an impact on information systems CIA **[[24]**.

This guideline highlights also the importance of reproducibility[11] and repeatability[12] of the risk assessment, nevertheless, considering the high degree of freedom of the security analyst, it seems very difficult to achieve such objectives even though the steps are very well detailed.

The guide introduces the concept of "Threat Scenario (or Threat Campaign)" as a "set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time" to describe how the events can contribute to or cause harm. This concept is to be used in place of the mere combination of asset-threat-vulnerability as it tells a story, and hence is useful for risk communication as well as for analysis.

The aim of RA is the production of a list of information security risks which can be prioritized by level of risk. The objective is to support decision-making process in risk response. In order to accomplish this, a threat and vulnerabilities analysis as well as another analysis on impacts and likelihood or events must be performed. Also, the uncertainty associated with the RA must be taken into consideration. For this reason, the gathering of essential information is crucial for the task and it has to be made always in accordance with the assessment context (established in 'prepare' step,RA process).

Conducting RA, in compliance with SP 800-30**[24]**, includes the following specific tasks:

- ***Identify threat sources*** *that are relevant to organizations and the* ***threat events*** *that could be produced by those sources;*
- ***Identify vulnerabilities*** *within organizations that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation;*
- ***Determine the likelihood*** *that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful;*
- ***Determine the adverse impacts*** *to organizational operations and assets, individuals, other organizations, and the Nation resulting from the exploitation of vulnerabilities by threat sources (through specific threat events);*
- ***Determine information security risks*** *as a combination of the likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations***[24, p.29]**.

In summary, the following advantages and drawbacks of the methodology are drafted hereafter:

- Advantages:

  - the methodology is well described and detailed steps are provided in order to carry out a risk assessment;
  - the methodology is part of the Risk management framework (SP 800-37) and Information security risk management (SP 800-39) that allow to address the full risk management lifecycle;
  - the taxonomy is defined in a generic manner, so it is open to specification and tailoring for the different sectors;
  - it is flexible, as it allows to define different algorithms for assessing and combining the risk factors that can be applied to the different use cases and also to different stages of a system/service lifecycle;
  - introduces the concept of risk scenario that should improve the communication towards management, among other things.

[11] Reproducibility refers to the ability of different experts to produce the same results from the same data.
[12] Repeatability refers to the ability to repeat the assessment in the future, in a manner that is consistent with and hence comparable to prior assessments—enabling the organization to identify trends.

- Drawbacks:

  - the definition of the risk factors likelihood and impact (based on Relevance, Likelihood of Attack Initiation, Vulnerabilities and Predisposing Conditions, Severity, Pervasiveness, Likelihood Initiated Attack Succeeds) that depends on "organizational and management inputs" and therefore on the "security analyst" designing and implementing the procedure;
  - The low level of definition of the taxonomies, the asset taxonomy is completely missing;
  - It does not provide criteria for asset-vulnerability-threat combination;
  - It does not really support the reproducibility and repeatability criteria meant to be pursued by the methodology;
  - The concept of residual risk is not considered;
  - The methodology stops at risk assessment, it does not address risk treatment, and it simply refers to security controls provided in SP 800-53 Revision 4**[103]**.

2.4.2 Evaluation of NIST SP 800-30 in the context of ECHO

In the context of ECHO the SP 800-30**[24]**:

- The methodology is sector-agnostic and written to be open and applicable to a generic organization and subject to specification of threats/vulnerability/scale value for each organization, therefore it can be potentially applied to any sector but it does not provide an approach to take into account explicitly of inter-sector opportunities and challenges neither security measures, it is quite generic on assessing ICT risks from a multi-sector perspective;
- It does not address at all the risk treatment, and therefore does not provide directly a vision on transversal countermeasures or potential roadmap. It is worth adding anyway that security controls are detailed in SP 800-53**[103]**. Nevertheless, SP800-53 should be analysed to assess if it is able to provide countermeasures applicable to any of the ECHO sectors;
- The methodology is considered fully compliant and capable to support the NIST Cybersecurity framework**[28]**;
- It doesn't rely on any EU methodology, but it is designed to be compliant to ISO activities;
- It doesn't support any benchmarks: criteria and scales are left to the organization decision;
- The methodology is well defined, but not self-standing, as it must be considered in the context of the NIST Risk assessment framework and open source;
- Taxonomies are not defined, only examples and categories in some cases are defined;
- It does consider the financial factor as criteria, but it doesn't provide any guidelines or criteria to use them in the risk assessment;
- Cybersecurity skills and training are not considered;
- It can be used in a certification scheme, but it doesn't provide any means to correlate risks to assurance levels.

2.5 Other Risk Assessment Methodologies

ENISA[13] collected a set of Risk Management/Assessment methods. Some of these methods are not widely used and some others have not been updated for several years, or are not in English language, as it is summarized in Table 4.

[13] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods

2.5.1 MEHARI Risk Assessment Method

MEHARI is a European (first developed in France) open-source widely known risk assessment methodology, fully compatible with ISO 27001 **[15]** and part of the ENISA suggested risk assessment methodologies.

MEHARI, an Open Source methodology provided under a Creative Commons License, is fully documented, with multiple guidelines and manuals. MEHARI is enriched by a risk assessment tool provided as an excel sheet, able to support the risk analyst though a complete risk assessment iteration.

Overview of MEHARI Risk Assessment process

MEHARI foresees a risk analysis that follows the steps shown in the following Figure:

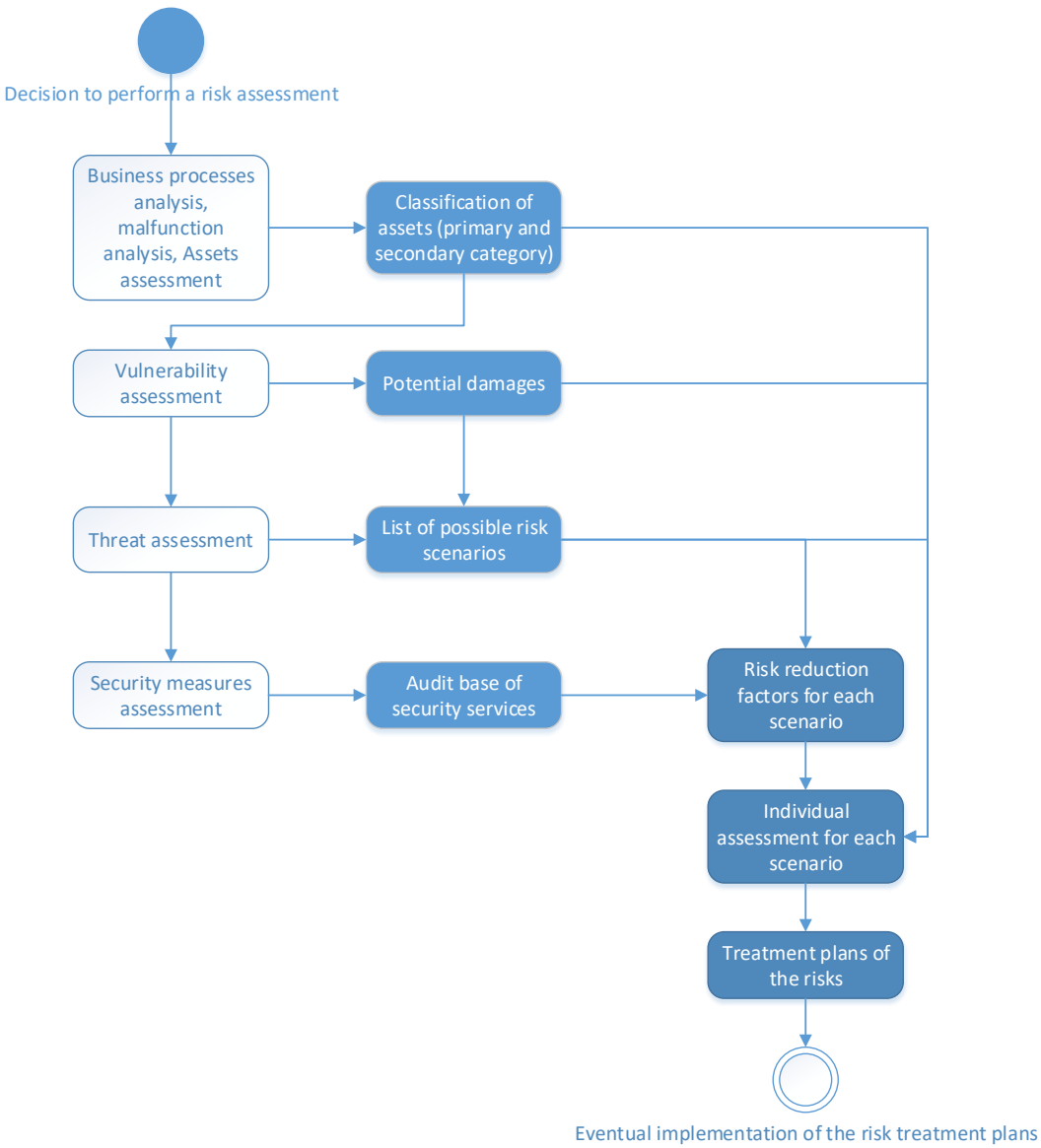

Figure 6: MEHARI Risk Assessment procedure

Business process analysis, malfunction analysis, assets assessment

MEHARI approach consists on analyzing the activities of the enterprise or organization, and therefore its business processes underlying the system under risk assessment. Possible malfunctions related to these business processes are identified and must be evaluated in terms of Seriousness for the organization. Once the malfunctions have been analysed it is easier to start the classification of the Assets (each asset will be assigned to two categories: Primary Category and Secondary Category).

Vulnerability assessment

Risks arise from the fact that a given Asset has one or more vulnerabilities.

MEHARI focuses on intrinsic vulnerabilities, which depend on the Secondary Asset Category, as they are essentially caused by the nature of the Asset (e.g. hardware medium, software medium). It is also important to note that the intrinsic Vulnerability of an Asset may be described as a specific susceptibility to Asset damage. Consequently, describing the Asset damage or the intrinsic Vulnerability are very similar concepts.

The type of consequence on an Asset (Asset damage) can be inferred from the intrinsic Vulnerability. Of course, if the Asset is susceptible to an Availability Impact, any assigned Vulnerability leading to a Confidentiality damage would bring no potential harm to the Asset.

Threat assessment

There can be no risk without a cause that leads to the intrinsic Vulnerability actually being exploited. Security standards and references, including ISO/IEC 27005, use the idea of a "threat" to describe this cause. It remains necessary, however, to include more than just the simple cause, or event, when describing the Threat: anything that can be used to describe how the damage may occur and, most importantly, anything that may influence the likelihood of the risk occurring should also be indicated. Consequently, MEHARI describes, when modelling threats, the following threat elements:

- The Event originating the risk occurring;
- Whether this Event is voluntary or accidental;
- The Actor;
- The circumstances in which this event occurs (declined in Time, Access, Process and Place).

Each of these parameters clearly has an influence on the probability of the risk occurring.

MEHARI asks the risk analyst to select threats from its taxonomy and associate them to a combination of assets and vulnerabilities, in order to create Risk Scenarios that can be used in order to evaluate the current level of risk of the System.

Security measures assessment

Once the Asset, the Vulnerability and the Threat Models have been created (or part of them), it is possible to start the assessment of the existing security measures. Since the basic components of the risk assessment (Impact and Likelihood for a set of Risk Scenarios composed by the different combinations of assets, vulnerabilities and threats) have been analysed, it is possible to already compute the intrinsic Seriousness of the composed Risk Scenarios. However, without an analysis of the existing security measures (an activity

called Safeguard Modelling) it will not be possible to assess the *real* Seriousness of the Scenarios. In MEHARI, the security measures assessment is performed by completed a very detailed security audit, divided in thirteen categories fully covering ISO 27002 security controls. Formulas help the risk analyst on assessing the degree of effectiveness of existing security measures within the defined system/organization scope.

Traditionally, risk is measured based on two parameters:

- The degree of seriousness of the consequences, or "Impact",
- The probability of the occurrence, or "Likelihood".

Global and direct assessment of these two parameters is usually difficult; as such, MEHARI prefers to use a more analytical approach that breaks these parameters down into multiple levels and individually evaluates:

- The *intrinsic* Impact, excluding all security measures,
- The *intrinsic* Likelihood, excluding all security measures,
- The effect of security measures on these two parameters (*calculated* impact and *calculated* likelihood), which is automatically computed leveraging on formulas provided by the methodology. This reduces the degree of human error.

Risk scenarios assessment

As from the previous Section, each Risk Scenario is assessed in multiple stages, each of which contributes to independently evaluating the Likelihood and the Impact of each Risk Scenario, as illustrated in the Figure below:

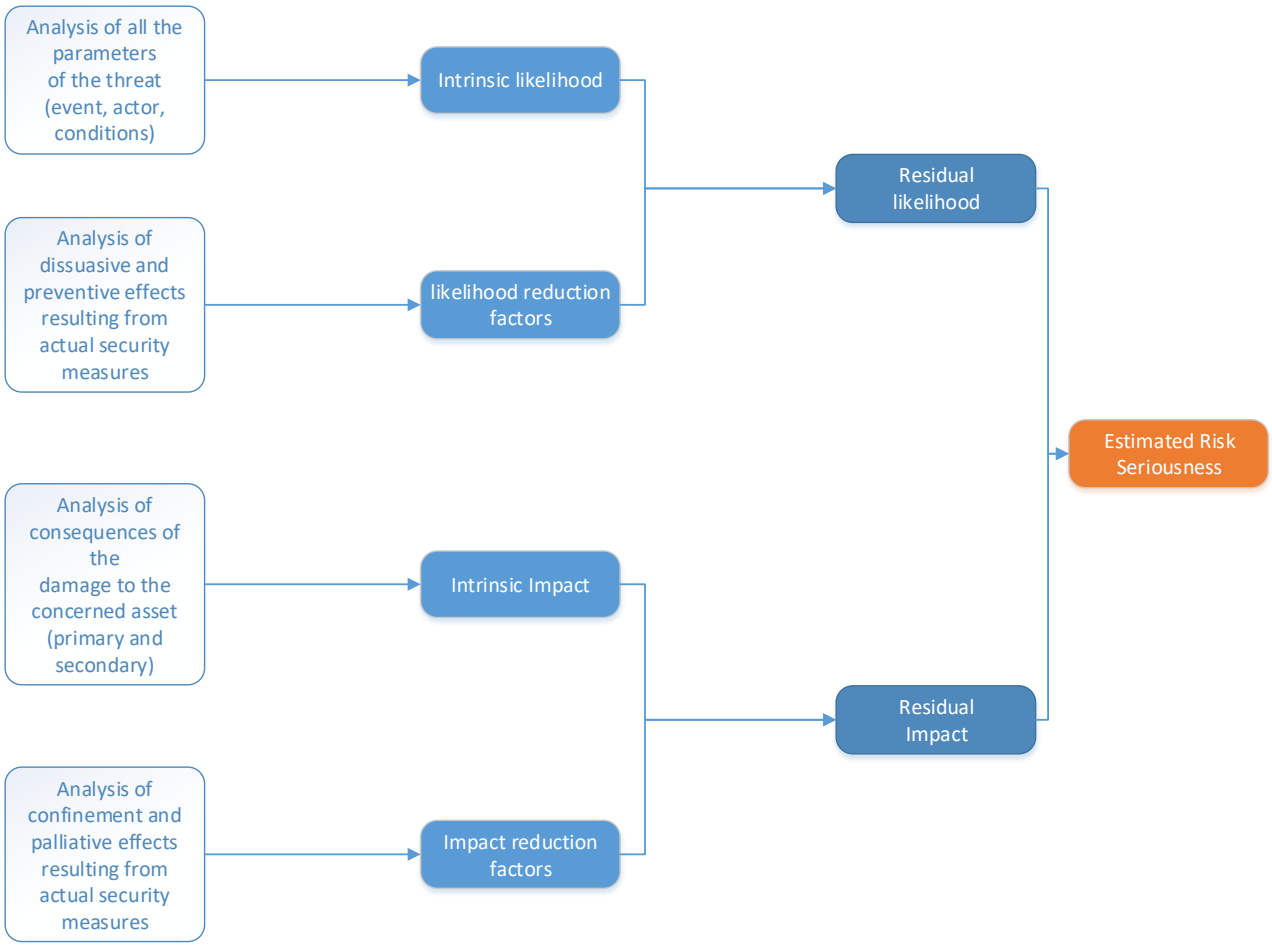

Figure 7: Risk Scenario estimation process

The Seriousness of each Risk Scenario is a function of its calculated Likelihood and Impact.

Risk treatment

Based on the Likelihood and Impact of the risk analyzed, the risk analyst needs to assess if the risk situation is *acceptable* as it is or if it must be *reduced, transferred* or even *avoided* somehow.

The decision to accept a risk or deem it unacceptable should be made using a process that ensures the reliability of the decision.

As an example, three categories of risk can be defined:

- Intolerable risks, which require emergency measures outside of normal budget cycles;
- Inadmissible risks, which must be reduced or eliminated at some point in time. This should be integrated into a planning cycle (security plan);
- Accepted risks.

The first two categories correspond to what had previously been called unacceptable risks.

MEHARI leverages on a standard risk acceptability table:

	Likelihood LOW	Likelihood MEDIUM	Likelihood HIGH	Likelihood VERY_HIGH
Impact CRITICAL	Seriousness MEDIUM	Seriousness HIGH	Seriousness CRITICAL	Seriousness CRITICAL
Impact HIGH	Seriousness MEDIUM	Seriousness HIGH	Seriousness HIGH	Seriousness CRITICAL
Impact MEDIUM	Seriousness LOW	Seriousness MEDIUM	Seriousness MEDIUM	Seriousness HIGH
Impact LOW	Seriousness LOW	Seriousness LOW	Seriousness LOW	Seriousness MEDIUM

Table 9: MEHARI Risk acceptability Table.

Different options are available for treating risks once they have been identified, listed and evaluated. MEHARI considers four main options available for treating risks, which are described in the ISO/IEC 27005 standard. These options are:

- **Accept** the risk as it is;
- **Reduce** the risk, by taking measures to diminish the impact or the likelihood (or both), thereby reducing the residual seriousness of the risk;
- **Avoid** the risk by removing the risk situation using structural or organizational measures;
- **Transfer** the risk, typically through insurance.

If the Risk Scenario has to be *Reduced*, it is possible to initiate one or more Action Plans in order to reduce the level of Seriousness of the Risk Scenario to an acceptable value.

Reducing a risk means reducing one of the two characteristic parameters of that risk, Likelihood or Impact, or both simultaneously using specific actions. Such actions are determined for each risk identified as *unacceptable*.

These actions aim to improve certain risk reduction factors by implementing suitable safeguards.

The first step in the decision-making process used in relation to reducing risks is choosing the security services suitable for both the Risk Scenario in question and the risk reduction factor that is to be improved. To do this, risk analysts have to be able to rely on a knowledge base of safeguards/security requirements (provided by MEHARI) that should include at least:

- A list of the safeguards/security requirements;
- The purpose (or objectives) of each Safeguard/Security Requirement;
- The technical and organizational mechanisms that may be envisaged for implementing the Safeguard/Security Requirement.

Risk reduction is usually a complex activity because it is not easy to link a Risk Scenario to one or more possible safeguard. Even if the link is possible, it is even more complex to assess the seriousness reduction factor depending on the quality of the safeguard. MEHARI helps the risk analysts on performing the task.

The decision-making process for reducing risks involves:

- Selecting suitable security measures;
- Selecting a target level for these measures;

- Deducing new values for the risk reduction factors;
- Verifying that these new values reduce the risk to an acceptable level of seriousness.

After analyzing the risks and making decisions on how to treat these risks, the organization may decide to go ahead with a certain number of actions that, according to the type of treatment chosen, are based on:

- Implementing safeguards/security measures, each with a quality level objective;
- Structural measures designed to reduce the exposure to certain risks;
- Organizational measures designed to avoid certain risks.

That said, it should be obvious that not all of these actions will be carried out simultaneously, nor will they all be implemented immediately, for various reasons such as limited budgets or lack of available human resources. As such, action plans should be developed according to the following steps:

- Choose priority objectives in terms of security services to implement, and optimize this choice;
- Transform the choice(s) of security services into concrete action plans;
- Choose potential structural measures and risk avoidance measures;
- Validate the preceding decisions.

The boundaries of a risk assessment methodology such MEHARI usually is limited at step 1 of the previous list (but of course a risk assessment iteration can be started after the implementation of the action plans extracted by the previous iteration in order to check if the risk has been effectively reduced).

Evaluation of MEHARI in the context of ECHO

MEHARI current knowledge base and taxonomy is focused on ICT risks. No specific sector is targeted: the methodology is widely used to analyse and treat risks on multiple sectors. Available knowledge does not take into account explicitly of inter-sector opportunities and challenges neither security measures, since it relies on a multi-sector horizontal approach, but it is quite generic on assessing ICT risks from a multi-sector perspective. The Knowledge Base, could be expanded/updated in order to identify inter-sector risk scenarios (challenges) which would lead to inter-sector risk treatment (opportunities) where transversal security measures can be applied.

The methodology is extremely clear and well documented. Several manuals and guidelines are available and are defined Threats, Vulnerabilities, Risk Scenarios and Security Controls complete taxonomies, with a focus on horizontal ICT risks. It is defined as a systematic method for analysing, providing standard elements and criteria that can be used to perform benchmarking activities through an excel tool. The tool itself is not of easy use, but it is extremely complete and potentially it could be updated/modified to enrich the list of supported risk scenarios or security controls. Although it is possible to expand all the taxonomies, the activity is not simple, because of the high degree of automation of the methodology: each vulnerability/threat/risk scenario is linked to the other taxonomies via formulas which enable a precise computation of the risk. Adding one or more of these elements requires a precise analysis of how the new element needs to be linked to the other during the risk computation. A new vulnerability space-specific, for example, will need to be linked to one or more specific threats and risk scenarios and the way the vulnerability affects the level of seriousness of the risks will need to be assessed and integrated in the formulas. Aside from what described above, one of the strengths of MEHARI is its capability to be extended.

Although the methodology does not offer a direct and guided support on financial factors, defines the impact component of the risk as dependent on malfunctions related to business processes. Each Malfunction carries a score, defining the impact over the business process in case the Malfunction is actually triggered. The Impact

metrics can be defined as the risk analyst prefers and must be consistent during the whole risk assessment iteration. MEHARI guidelines suggest to define the impact on the business processes as a financial impact, but this decision is completely up to the risk analyst: it is also possible to define more than one metric for the impact definition (could be financial and operational impact, for example). Once the residual risk is computed (in form of treated risk scenarios) it is possible to define how the residual risk will be handled (transferred, ignored, accepted). Moreover, MEHARI could hence be used in order to support insurance-based schemas to cover the residual risk.

MEHARI could be used to analyse the Scenarios and Use Cases of T2.1. It may be needed, however, to expand its knowledge base in order to cover more risk scenarios and potentially, more threats, vulnerabilities and security controls. Additional data would be needed from the Storylines in order to better define the business context. So MEHARI risk treatment can fit to the ECHO proposed concept of Technology Roadmap one in ECHO. The aforementioned excel tool isn't the only tools available to perform the risk analyst. RHEA developed two tools fully supporting MEHARI: an Open Source tool built for the European Space Agency, and a commercial version.

The methodology is listed by ENISA as an EU RA methodology and fully compliant with ISO27001. Moreover is open source under a License adapted from Creative Commons Attribution-ShareAlike 4.0 International Public License. MEHARI can be freely used also in commercial contexts, but it must be referenced. In case of updates to the methodology or its knowledge base/taxonomies, its governing body (CLUSIF) must be notified.

Must be noted that MEHARI does not support the concept of Curricula; the skills a person must have to use the methodology are not made explicit. In itself, the methodology is defined so that anyone can execute it. Neither is defined the concept of Certification Scheme like in ECHO, because MEHARI is a methodology for risk analysis and detection. The possible certification is conditioned to the necessary changes to carry out in the noncompliance of risks detected under the methodology. At the academic level, there is no explicit possibility of MEHARI certification, neither Training programs are not defined.

MEHARI could be viable as the basic methodology for the ECHO Multi-sector Assessment Framework. It is a complete, European, detailed methodology It is expandable and provides results, while not quantitative, certainly much less prone to human errors than most of RA methodology, thanks to the whole set of formulas linking assets types, vulnerabilities, threats and risk scenarios. MEHARI, however, is not a simple methodology and risk assessment iterations using it may require longer effort than with other, higher level, methodologies. As a summary, MEHARI could fit the role as a starting point for the ECHO MAF and the workgroup took lesson for the following design. Any update to the methodology, however, must be notified to its governing body (CLUSIF). This could slow down its usage on ECHO.

2.5.2 MAGERIT

MAGERIT**[20]** is an Open Source methodology for Risk Analysis and management. Developed in 1997 by the Spanish Ministry of Public Administration. MAGERIT was offered as framework and guide to the Public Administration in response to the perception that the government (and, in general, the whole society) increasingly depends on information technologies for achieving its service objectives. The v2 was published in 2005 and is available in Spanish and English. Given its open nature, it is also used outside the Ministry of Public Administration and can be applied to all companies that use ICT systems. It offers compliance with the following standards: ISO/IEC 27001:2005, ISO/IEC 15408 / 2005, ISO/IEC 17799 / 2005, ISO/IEC 13335 / 2004. Although MAGERIT uses no EU Methodologies, ENISA analysed MAGERIT within their inventory of Risk Management/ Risk Assessment methods.

According to ISO 31000**[18][19]** terminology, MAGERIT **[105]***implements the Risk Management Process within a working framework for governing bodies to make decisions taking into account the risks derived from the use of information technologies. It is based also on the following sector specific best practices*:

- "Risk Management: Multiservice Tactics, Techniques, and Procedures for Risk Management", Air Land Sea Application Center, FM 3-100.12, MCRP 5-12.1C, NTTP 5-03.5, AFTTP(I) 3-2.30. February 2001 **[34].** (DEFENSE)
- Air Force Pamphlet 90-902, "Operational Risk Management (ORM) Guidelines and Tools", December 2000 **[35]**. (MARITIME)
- Federal Office for Information Security (BSI). "IT Baseline Protection Manual", October 2003 Germany **[36]**. (MARITIME)
- "The Vulnerability Assessment and Mitigation Methodology", P.S. Antón et al., RAND National Defense Research Institute, MR-1601-DARPA, 2003 **[37]**. (MARITIME)

Following frameworks are referenced for vocabulary and general risk approach **[105]**:

- NIST 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems **[25];**
- "CRAMM, CCTA Risk Analysis and Management Method (CRAMM)", Version 5.0, 2003**[12]**;
- "Managing Information Security Risks: The OCTAVE Approach", C.J. Alberts and A.J. Dorofee, Addison-Wesley Pub Co; 1st edition (July 9, 2002) **[28]**;
- ISO31000:2010**[18]**;
- ISO/IEC 27005 (all threats and vulnerabilities associated with each asset are identified) **[16]**;
- Common Criteria framework (process of evaluation and certification or registry has been formalised in security products) **[38]**;
- ISO27001:2013 (process of evaluation and certification or registry has been formalised in information security management systems) **[15]**.

MAGERIT relies on the EU OCTAVE Methodology and can be the starting point for benchmarking initiatives. It anticipates some problems recurrently coming up when analysing risks.

Overview of MAGERIT Risk Assessment process

MAGERIT support the following RA phases:

- **Risk identification**:
  - Assets: identification, classification, dependencies between assets, and value.
  - Threats: identification relationship with assets and evaluation of vulnerability.
  - Safeguards: identification and evaluation; tool support.
- **Risk analysis**: accumulated impact and risk; deflected impact and risk; tool support.
- **Risk evaluation**: from technical risks into business risks[14].

The MAGERIT method has the following concurrent steps:

- Characterisation of assets: identification, classification, dependencies and valuation.
- Characterisation of threats.

[14] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_magerit.html

- Evaluation of safeguards.

MAGERIT **[16]** is open source, clear and well defined using separate books to deepen topics. Indeed, version 3 of MAGERIT has been structured into two books and a technical guide:

- Book I – The method
- Book II – Catalogue of elements
- Guide of Techniques – Compilation of different kinds of techniques that could be useful to apply the method.

The “Elements catalogue” allows uniformity in the results of the analysis, giving very specific items of the following components in risk assessment:

- Types of assets
- Valuation dimensions
- Valuation criteria
- Catalogue of threats

The Book Catalogue of elements can enable transversal and inter-sector opportunities. Identification is challenged, however, it does not expressively address the improvement of multi-sectoral management processes for mitigation of Cyber Security risk. The Guide of Techniques could be useful to apply the method providing additional information and guides on some techniques often used when carrying out risk analysis and management projects. Techniques specific to risk analysis are presented (analysis using tables, Algorithmic analysis, attack trees, graphical techniques, interviews, meetings and presentations, Delphi evaluation). The catalogue of elements is open to additions and provides guidelines for types of assets, dimensions for evaluating assets, criteria for evaluating assets, typical threats to information systems and safeguards to be considered for protecting information systems.

MAGERIT enables a transversal vision for countermeasures. MAGERIT implements the Risk Management Process within a working framework for governing bodies to make decisions taking into account the risks derived from the use of information technologies. The ultimate aim of using MAGERIT is to make a methodical approach that leaves no room for improvisation and not to depend on the analyst’s whim **[105]**.

MAGERIT Taxonomy **[105]** is well defined providing guidelines on: type of assets, dimensions for evaluating assets, criteria for evaluating assets, threats and safeguards, taking vocabulary from the following standards:

- [CNSS 4009:2010] Committee on National Security Systems. CNSS Instruction No. 4009. National Information Assurance (IA) Glossary;
- [ISO/IEC 7498-2:1989] Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture;
- [ISO/IEC 19790:2012] Information technology -- Security techniques -- Security requirements for cryptographic modules;
- [ISO/IEC 21827:2008] Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®);
- [ISO/IEC 27000:2014] Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary;
- [ISO/IEC 27031:2011] Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity;
- [ISO/IEC Guide 2:2004] Standardization and related activities -- General vocabulary;
- [ISO/IEC Guide 73:2002] Risk management -- Vocabulary".

There are rules on which taxonomy has been built and rules about how to use it and guidelines how to expand it. The catalogue of elements includes, for each session, XML notation to be used for regularly publishing the elements in a standard format that can be processed automatically by analysis and management tools. If the reader uses a risk analysis and management tool, this catalogue will form part of it. If the analysis is carried out manually, this catalogue provides a wide starting base for quick progress without distractions or oversights. The types of assets can be expected to develop over time to adapt to technological developments. For this reason, XML grammar is given below that allows updates for the types described above to be published periodically.

```
types ::=
  <types>
    { type }*
  </types>

type ::=
  <type code>
    #name#
    [ description ]
    { type }*
  </type>

description ::=
  <description>
    #text#
  </description>
```

Figure 8: XML grammar

There are many sources that identify assets within the area of information and communications technologies.

- GMITS ISO/IEC IS 13335-1:2004, “Information technology - Security techniques - Guidelines for the management of IT security - Part 1: Concepts and models for information and communications technology security management”.
- SP 800-60, “Guide for Mapping Types of Information and Information Systems to Security Categories”, NIST, June 2004.[15]
- UNE-ISO/IEC 17799:2002, “Tecnología de la Información. Código de Buenas Prácticas de la Gestión de la Seguridad de la Información”. 2002.
- “Managing Information Security Risks: The OCTAVE Approach”, C.J. Alberts and A.J. Dorofee, Addison-Wesley Pub Co; 1st edition (July 9, 2002)

Categories of assets are transversal but items inside can be specific:

- [S] Services
- [D] Data
- [SW] Software
- [HW] Hardware
- [COM] Communication networks
- [SI] Storing Information Media
- [AUX] Auxiliary equipment
- [L] Installation (places housing information and communications systems)
- [P] Personnel

[15] http://csrc.nist.gov/publications/nistpubs/index.html

An example of declination:

- [COM] Communication networks
- [PSTN] telephone network
- [ISDN] digital network
- [X25] data network
- [ADSL] ADSL
- [pp] point to point
- [radio] wireless network
- [sat] satellite
- [LAN] local network
- [MAN] metropolitan network
- [Internet] Internet
- [vpn] virtual private network

MAGERIT does not define risk financing strategies for the residual risk but the methodology supports it because the "Guide of techniques" gives an analysis model based on qualitative and quantitative valuations, taking into consideration also the concept of residual risk. The "**Guide of techniques**" gives an analysis model based on qualitative and quantitative valuations. Every asset involves a set of security dimensions when it is under cyberattack. It is crucial to properly determine which of them are if interest in an asset and to value it in order to estimate the loss of value in case of an eventual incident. MAGERIT **[16]** suggests to estimate through the following list of factors:

- *Replacement cost: acquisition and installation;*
- *Labour cost invested in recovering (the value of) the asset;*
- *Loss of income;*
- *Loss of capacity to operate: lack of confidence of users and suppliers resulting in a loss of activity, or in worse economic conditions;*
- *Penalties due to non-compliance with the law or with contractual obligations;*
- *Damage to other assets, internal or external;*
- *Injury to persons;*
- *Environmental damage* **[105]**.

The methodology takes into account economic factors such as initial cost, annual costs, improvements to decide if a measure can be considered a good investment. Financial studies can be made comparing what is at risk with what the solution costs by answering the questions:

- *Is it worth investing so much money in this safeguard?*
- *Which group of safeguards optimizes the investment?*
- *Over what period of time is the investment recovered?*
- *What is the reasonable cost of an insurance policy?* **[105]**

MAGERIT supports the provisioning of a selection of roadmaps of ways (e.g. controls) to reduce the risk, based on the principle that not all the assets are of the same type. The threats and safeguards are different according to the type of assets. Chapter 2**[105]** of the "Elements catalogue" gives a list of types of assets. A detailed table is intended as a guide for users uniformly valuing assets whose value is important for different reasons after taking account of:

- *The security of persons;*
- *Personal information;*
- *Obligations arising from the law, from the regulatory framework, from contracts, etc.;*
- *Capacity for following up offences;*

- *Commercial and financial interests;*
- *Financial losses;*
- *Interruption of the service;*
- *Public order;*
- *Corporate policy;*
- *Other intangible values* **[105]**.

Chapter 6 of the "Elements catalogue" gives a list of suitable safeguards for each type of asset. Safeguard types and level of effectiveness are defined with respect to specific threats divided into the following main categories:

- [N] Natural disasters
- [I] Of industrial origin
- [E] Errors and unintentional failures
- [A] Wilful attacks **[105]**

Each threat is shown by asset type in a table as follows:

[code] short description of what may happen	
Types of assets: ▯ that may be affected by this threat	**Dimensions:** 1. [of security] that may be damaged by this threat; sorted by relevance
Description: longer presentation of what may happen	

Figure 9: Example of treat definition [105].

Evaluation of MAGERIT in the context of ECHO

Based on the previous consideration about guidelines provided in the Catalogue of Elements, it is possible to use the methodology for a RA of the use cases from T2.1. There are a lot of specific assets divided in common types of asset; there is a wide description of possible impacts wrt a scale from 0 to 10; there is a comprehensive set of threats; Safeguards are divided in types and level of effectiveness are defined with respect to specific threats.

Mapping specific assets, vulnerabilities and impacts of the Storylines and Use Cases from T2.1, it is possible to proceed with the following steps of RA in MAGERIT **[105]**:

1. *Key assets have been identified: information to be dealt with and services provided;*
2. *Needs or levels of security have been assessed that are required for each key asset in each security dimension;*
3. *Other system assets have been identified;*
4. *It has been established the value (or the required security level) of the other assets depending on their relation with other essential assets (for example, through the identification of the premises);*
5. *Possible threats on the assets have been identified;*
6. *The consequences have been estimated, if those threats actually occurred;*
7. *The likelihood that those threats actually occurred has been estimated;*
8. *Potential impacts and risks - inherent to the system - have been estimated;*
9. *The applicable safeguards have been identified to tackle potential impacts and risks;*

10. *The implementation of the identified safeguards has been assessed;*
11. *The values of residual impact and risks have been estimated, which correspond to the level of impact and risk that the system, after the implementation of the safeguards, continues to support*";

MAGERIT enable/define linkability to tools/ICT product: PILAR[16], the Spanish acronym for "Logical Computer Procedure for Risk Analysis", is an open tool, available in Spanish, Italian, French and English developed to the specifications of the National Security Agency to support risk analysis in information systems using the MAGERIT methodology. The tool calculates security ratings according to the usual *dejure or de facto* standards, including:

- Spanish National Security Framework;
- ISO/IEC 27002 Security management systems;
- Spanish RD 1720:2007 Personal data protection **[105]**.

Another commercial tool supporting MAGERIT is EAR[17]. Due to the XML/CVS input/output functions, MAGERIT provides the possibility to be easily integrated with other tools.

Features required from present or future tools for supporting the risk analysis and management process are described in the Annex of the Methodology**[20]**. All the techniques in the Guide of Techniques can be used without automated aids; however, for repeated or complex use, it is recommended to use tools as widely and frequently as possible. It is important to point out that the notation proposed for applying the technique is in no case compulsory. Each organization may adapt to the available tools or sector specific notations.

MAGERIT gives few and indirect support to the concept of Certification Scheme (as they will be defined in ECHO): indirect objectives of MAGERIT is to prepare the organisation for the processes of evaluating, auditing, certifying or accrediting, as relevant in each case. Paragraph 1.8. Evaluation, certification, auditing and accrediting section provide a conceptual presentation of these activities. The reader will find a specific discussion of the standards relating to management systems and security products in Appendix 4 **[105]**.

The methodology gives weak support to support the concept of Curricula (like defined in ECHO): *the best security plan would be seriously undermined without the active collaboration of the persons involved in the information system, especially if the attitude is negative, and contrary or one of "fighting against the security measures". This requires the creation of a "security culture" which, coming from top management, encourages the awareness of all those involved of its need and relevance. There are three basic pillars according to MAGERIT for creating this culture*:

- *A corporate security policy which is understood (written so as to be understood by those who are not experts in the matter) which is published and kept updated;*
- *Security policies that, in specific areas of activity, clarify the stance of the Organisation; i.e., defining the correct use and what non-compliance means;*
- *Continuous training at all levels, with reminders of routine precautions and specialised activities, depending on the responsibility assigned to each job.*

The methodology does not identify transversal, inter-sector and specific skills for Curricula, nor provides a basis for Training Programmes **[105]**.

[16] http://www.ar-tools.com/pilar/
[17] http://www.ar-tools.com/

2.5.3 OCTAVE

The conceptual framework that formed the basis of the original OCTAVE approach was published by the Software Engineering Institute (SEI) at Carnegie Mellon University in 1999 **[39]**. The SEI cooperated with the Telemedicine and Advanced Technology Research Center (TATRC) and developed the OCTAVE methodology to address the security compliance challenges faced by the U. S. Department of Defense (DoD) in addressing the provisions of the Health Insurance Portability and Accountability Act (HIPAA) for the privacy and security of personal health. After the first release in September 1999, there have been a number of updates and changes to the OCTAVE methodology. The table below provides the list of the subsequent updates and related developments:

Date	Publication Title
September 1999	OCTAVE Framework, Version 1.0
September 2001	OCTAVE Framework, Version 2.0
December 2001	OCTAVE Criteria, Version 2.0
September 2003	OCTAVE-S v0.9
March 2005	OCTAVE-S v1.0
June 2007	Introduction of OCTAVE Allegro v1.0

Table 10: The history of OCTAVE.

Overview of OCTAVE Risk Assessment process

The OCTAVE method is the first OCTAVE-consistent methodology to be introduced. The approach is defined by a method implementation guide (procedures, guidance, worksheets, information catalogues) and training. The method is performed in a series of workshops carried out and eased by an interdisciplinary *analysis team* composed by people coming from the business units of the organization (e.g. senior management, operational area managers, and staff) and members of the IT unit.

The intended audience for the OCTAVE method is large organizations with 300 or more employees. It is designed for organizations that:

- have a multilevel hierarchy;
- maintain their own computing infrastructure;
- have the ability to run vulnerability evaluation tools;
- have the ability to interpret the results of vulnerability evaluations **[41]**.

OCTAVE is not another technology-focused methodology; it provides an assessment framework based on the evaluation of the organizational risks and focused on strategic, real and practical issues that can be adapted to the most part of the organizations.

The application of the OCTAVE methodology starts from the work of a small team of people from the operational (or business) units and the information technology (IT) department, who work together to address the security needs of the organization, balancing the three key aspects: operational risk, security practices, and technology.

Two elements characterize the OCTAVE approach: operational risk and security practices. Technology is taken into consideration only as related to security practices, allowing an organization to refine the view of its

current security practices. Through OCTAVE an organization makes information-protection decisions based on risks to the confidentiality, integrity, and availability of critical information-related assets. All aspects of risk (assets, threats, vulnerabilities and organisational impact) are taken into account in the decision-making process, allowing an organisation to combine a practice-based protection strategy with security risks.

OCTAVE is self-directed, requiring an organization to manage the evaluation process and make information-protection decisions. An interdisciplinary team, called the analysis team, leads the evaluation. The team is composed by people from both the business units and the IT department, because both points of view are important to characterize the global, organizational view of information security risk.

The analysis teams have to:

- identify information-related assets (i.e. information and systems) that are critical to the organization;
- focus risk analysis activities on those assets deemed to be most critical to the organization;
- consider the relationships among critical assets, the threats to those assets, and vulnerabilities (both organizational and technological) that may expose assets to threats;
- evaluate risks in an operational context - how they are used to conduct an organization's business and how those assets are at risk due to security threats;
- create a practice-based protection strategy for organizational improvement as well as risk mitigation plans to reduce the risk to the organization's critical assets.

A three-phased approach integrates the organizational, technological, and analysis aspects of an information security risk evaluation. OCTAVE is based on these three phases, focused on three different aspects, which allow the organization to define a complete overview of its information security needs. The phases are:

Phase 1*: Build Asset-Based Threat Profiles* – This is an organizational evaluation. In this phase the information-related assets of the organization are identified by the *analysis team*, along with what is currently being done to protect them. The analysis then continues with the selection of the critical assets, the most important ones, and with the corresponding security requirements. For each critical asset it is then defined a threat profile, containing its threats.

Phase 2*: Identify Infrastructure Vulnerabilities* – In this phase, the assessment of the organization information infrastructure is carried out. The analysis team analyses the network access paths, identifying classes of information technology components related to each critical asset. The team then determines the extent to which each class of component is resilient to network attacks.

Phase 3*:Develop Security Strategy and Plans* – This phase, based on the information previously collected, is devoted to identify the risks related to the organization critical assets and to decide a protection strategy and the mitigation plans to address them.

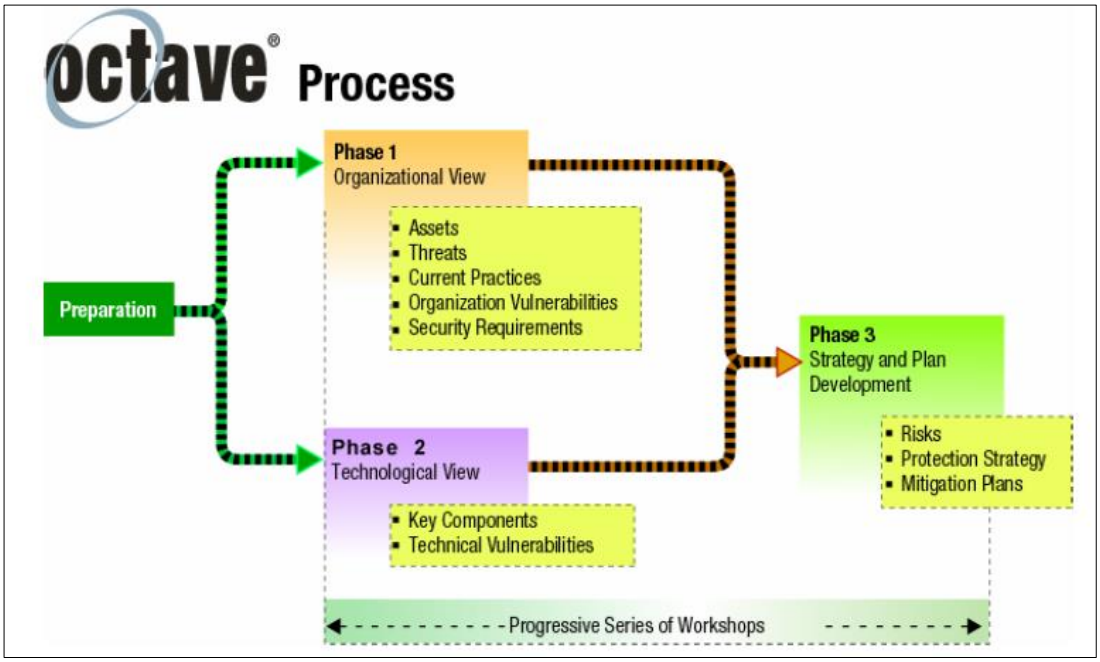

Figure 10: OCTAVE phases [14].

OCTAVE Criteria

The OCTAVE criteria cover the fundamental elements, the requirements, of the methodology. There is only one set of OCTAVE criteria even if there can be many methods consistent with them; the OCTAVE method is documented in the OCTAVE Method Implementation Guide, v2.0. It is designed for large companies; its first evolution, OCTAVE-S (see sub-section below) was developed for small organizations. It is always possible to define methods for specific contexts that are consistent with the criteria.

The OCTAVE criteria are a set of *principles, attributes, and outputs*. **[40]**

Principles are the fundamental concepts leading the type of the evaluation, and defining the philosophy behind the evaluation process. They define the evaluation approach and provide the basis for the evaluation process. For example, one of the principles of OCTAVE is self-direction. This means that people from the organization are the best evaluators and decision makers as for the security organization strategy.

Attributes and *outputs* involve the evaluation requirements. *Attributes* refer to the qualities, or distinctive features, of the evaluation. From a process and organizational point of view, attributes are the requirements in charge to specify the core elements of the OCTAVE methodology and the needs to achieve a successful evaluation. Attributes come from the OCTAVE principles; as an example, an OCTAVE attribute states that the analysis team driving the evaluation has to be composed by personnel from the organization. Self-direction is the principle behind this specific requirement.

Moreover, the required results of each phase of the evaluation are the *outputs*, which are in charge of specifying the results to be achieved by the analysis team. OCTAVE outputs can be generated by more than a single set of activities, and then a unique set of activities is not specified. Outputs are arranged according to the three phases; the tables below **[40]** list the principles, activities, and outputs of the OCTAVE approach.

Principle	Attribute
Self Direction	RA.1 Analysis Team RA.2 Augmenting Analysis Team Skills
Adaptable Measures	RA.3 Catalog of Practices RA.4 Generic Threat Profile RA.5 Catalog of Vulnerabilities
Defined Process	RA.6 Defined Evaluation Activities RA.7 Documented Evaluation Results RA.8 Evaluation Scope
Foundation for a Continuous Process	RA.9 Next Steps RA.3 Catalog of Practices
Forward-Looking View	RA.10 Focus on Risk
Focus on the Critical Few	RA.8 Evaluation Scope RA.11 Focused Activities
Integrated Management	RA.12 Organizational and Technological Issues RA.13 Business and Information Technology Participation RA.14 Senior Management Participation
Open Communication	RA.15 Collaborative Approach
Global Perspective	RA.12 Organizational and Technological Issues RA.13 Business and Information Technology Participation
Team Work	RA.1 Analysis Team RA.2 Augment Analysis Team Skills RA.13 Business and Information Technology Participation RA.15 Collaborative Approach

Table 11: OCTAVE Principles and Attributes [40].

Phase	Output
Phase 1	RO1.1 Critical Assets RO1.2 Security Requirements for Critical Assets RO1.3 Threats to Critical Assets RO1.4 Current Security Practices RO1.5 Current Organizational Vulnerabilities
Phase 2	RO2.1 Key Components

Phase	Output
	RO2.2 Current Technology Vulnerabilities
Phase 3	RO3.1 Risks to Critical Assets RO3.2 Risk Measures RO3.3 Protection Strategy RO3.4 Risk Mitigation Plans

Table 12: OCTAVE Outputs [40].

An information security risk evaluation is part of an organization's activities for managing information security risks. OCTAVE is an evaluation activity, not a continuous process. Thus, it has a fixed beginning and end. This means that the risk management activities define a plan-do-check-act cycle.

As a consequence, an organization that uses the OCTAVE methodology can need to carry out a new OCTAVE analysis; this can be determined either by the occurrence of particular, major events (i.e. an internal reorganization, or a renewal software infrastructure), or by the definition of a specific time plan (i.e. yearly). Between evaluations, an organization can periodically identify new risks, analyze these risks in relation to existing risks, and develop mitigation plans for them.

OCTAVE developments

There are now **[41]** three distinctive OCTAVE methodologies available for public use: the OCTAVE method, OCTAVE-S, and OCTAVE Allegro. Allegro is the next generation OCTAVE that offers a streamlined process with focus on information assets. However, each OCTAVE method can be broadly applied and users can identify the approach that best fits their particular information security risk assessment needs. The following sub-sections describe the two methodologies named OCTAVE–S and OCTAVE Allegro.

OCTAVE-S [41]

The Technology Insertion, Demonstration, and Evaluation (TIDE) program at the SEI supported the realization of the OCTAVE – S methodology. The aim was to develop an OCTAVE framework and approach to small manufacturing companies; the most up-to-date version of OCTAVE-S, version 1.0, is specifically intended for organizations of no more than 100 people. The OCTAVE-S approach is obviously OCTAVE–consistent; it is based on three similar phases.

One difference is that the analysis team (3-5 persons) is supposed to have concrete and actionable knowledge of the important information assets, security requirements, threats and security practices of the organization; this means that the approach is not based on formal knowledge education workshops to gather the required information.

Another distinguishing feature is that OCTAVE–S is more articulated than the traditional approach. OCTAVE-S worksheets and guidelines include security concepts, making it possible for operators less experienced in risk and safety to deal with a wide range of risks with which they may be unfamiliar.

Finally, another significant difference can be highlighted in the examination of the information infrastructure of the organization , Considering that small companies, to which OCTAVE – S is focused, may not have the resources to pay and execute vulnerability tools, the method is delivered include a restricted review of infrastructure risks, in order to facilitate the methodology adoption.

OCTAVE-Allegro

After the introduction of the OCTAVE and OCTAVE-S methodologies, the information security risks to be addressed, and consequently the ability to manage them by the organizations, has substantially changed.

Moreover, the evolution of the method also came from the experience of using the OCTAVE approach in real cases.

The result of the improvements is OCTAVE Allegro, an updated version whose approach is based on a more information-centric focus respect to the previous OCTAVE vision. Data, information assets are now studied in their living context, taking into account the way they are collected, stored, transported, elaborated, and their interaction with threats, thus identifying vulnerabilities and consequences in order to carry out a risk assessment.

OCTAVE Allegro provides methods to rationalize and optimize the process of information security risk assessment. Investments in time, resources and personnel from an organization to achieve acceptable results are limited. Allegro enables the organization to consider people, technology and facilities in the context of their relationship to the information and business processes and services they underpin. Moreover, the overall usability of the risk assessment process has been improved. Guidance, worksheets, and questionnaires are the supports on which, like the previous ones, this updated OCTAVE version can be operated. On the other hand, it is more applicable to the needs of organizations, individuals, who want to reduce the required levels of knowledge and training necessary for performing effective risk assessment.

Methodology

The OCTAVE Allegro approach consists of eight steps that are organized into four phases, as illustrated in the following Figure.

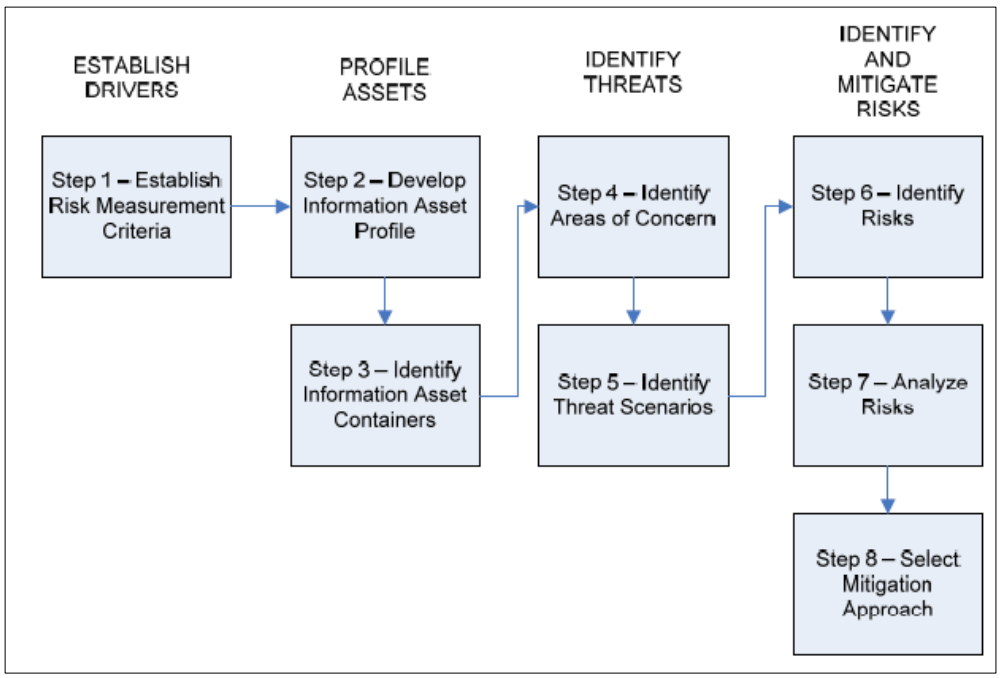

Figure 11: OCTAVE ALLEGRO Phases and steps [41].

Phase 1 - Establish drivers**,** where the organization develops risk measurement criteria that are consistent with organizational drivers. These risk measurement criteria are a set of qualitative measures against which the effects of a realized risk can be evaluated and form the foundation of an information asset risk assessment. In addition to evaluating the dimension of an impact on a specific area, an organization must identify the impact areas which are the most significant to its mission and business objective (i.e. the relationship with its customer base, the technology innovation).

Phase 2 - Profile assets*,* where the information assets that are the focus of the risk assessment are identified and profiled and the assets' *containers* are identified. A container can be a person (people can store information as knowledge, process information by thinking and acting), an object (for example a piece of paper), or a technology (for example a database). This process defines clear borders of the asset, capture its security requirements and identifies all of the locations where the asset is stored, transported, or processed.

Phase 3 - Identify threats, where threats to the assets - in the context of the locations where the assets are stored, transported, or processed - are identified and documented through a structured process that begins with the analysis of the possible situations that can threaten an organization's information asset. The analysis defines the so called "areas of concern": a specific team of the organization is in charge to quickly identify real–world scenarios, then situations, conditions that propose threats and their corresponding unwanted results. The areas of concern are then developed into threat scenarios, providing details of the identified threats. The set of threats is then enriched and completed by additional threats coming from threat scenarios. A set of threat scenarios can be represented visually in a tree structure, the so called ***threat tree***; threat trees come from the OCTAVE method and are described as follows:

Threat Tree	Definition
Human actors using technical means	The threats in this category represent threats to the information asset via the organization's technical infrastructure or by direct access to a container (technical asset) that hosts an information asset. They require direct

Threat Tree	Definition
	action by a person and can be deliberate or accidental in nature.
Human actors using physical access	The threats in this category represent threats to the information asset that result from physical access to the asset or a container that hosts an information asset. They require direct action by a person and can be deliberate or accidental in nature.
Technical problems	The threats in this category are problems with an organization's information technology and systems. Examples include hardware defects, software defects, malicious code (e.g., viruses), and other system-related problems.
Other problems	The threats in this category are problems or situations that are outside the control of an organization. This category of threats includes natural disasters (e.g., floods, earthquakes) and interdependency risks. Interdependency risks include the unavailability of critical infrastructures (e.g., power supply).

Table 13: Description of threat trees [41].

Phase 4 - Identify and mitigate risks, where risks to information assets are identified and analyzed based on threat information, and mitigation strategies are developed to face the risks. First of all, threats are identified (step 5), then the consequences to an organization if a threat occurs are identified (step 6), providing a complete risk representation. A threat can have various potential impacts on an organization. Moreover, a quantitative measure of the extent to which the organisation is affected by a threat is estimated (step 7). Finally, the organization's analysts identify and select, among the others, the major risks that need mitigation to produce a ranking list based on a risk score and define the strategy to address them. The outputs from each step in the Allegro process are reported on a series of worksheets which are then used as inputs to the next step in the process. The use of the worksheets supports the process and facilitate the application of the Allegro methodology.

Evaluation of OCTAVE in the context of ECHO

The analysis of the OCTAVE methodology revealed the following issues:

OCTAVE enables a very low level of traceability to tools or ICT products. ENISA refers to the so-called "OCTAVE automated Tool"[18]. Actually, the link refers[19] to the Advanced Technology Institute (ATI), the organization that developed the tool, does not provide information on it. Any other reference to specific ICT technologies which can enable an even partial automation of the risk assessment workflow process has not been found.

- The methodology does not support the concept, as defined in ECHO, of curricula or skills. Although conditions are set at the level of use (i.e. the profiles of the organization personnel composing the analysis team), there is no envisaged definition of a set of these instruments;

[18]https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_octave.html
[19]http://oattool.aticorp.org/Tool_Info.html

- OCTAVE does not specifically support the implementation of training programs to raise the level of widespread Cyber Security Level;
- It does not define a set of requirements; it does not offer/rely on a certified EU methodology;
- It does not allow organizations to quantitatively model risk.

In conclusion, the OCTAVE methodology, in its most recent version, Allegro, is a methodology for streamlining and optimizing the information security risk assessment process, showing a set of weaknesses where the scarce capability to set up the risk factor is probably its most significant limitation.

2.6 Concluding Remarks

The bottom-up analysis, described in the previous sections, was necessary to understand the Risk Assessment landscape and the most used frameworks and methodologies.Table **14** shows a high-level comparison between the assessed items.

		ISO31000	TOGAF	SP800-30	MEHARI	MAGERIT	OCTAVE
1	**Specific Requirements.** Does the Methodology…						
1.1.1	... enable improvement of multi-sectoral management processes for mitigation of Cyber Security risks?	medium	low	low	high	no	medium
1.1.2	... assess transversal and inter-sector opportunities and challenges?	medium	low	low	medium	low	no
1.1.3	... enable a transversal vision for security countermeasures?	no	no	no	medium	high	no
1.1.4	… has been developed in the EU	medium	no	medium	high	high	No
1.1.5	… enable benchmarking initiatives?	medium	high	no	low	medium	low
1.2	Is the Methodology clear and well defined?	medium	medium	medium	high	high	medium
1.3	Is the Methodology open source?	no	high	yes	high	yes	medium
1.4	Are the related Taxonomies well defined?	no	high	low	high	medium	no
1.5	Are the related Taxonomies expandable?	no	no	low	high	high	no
3	**Economic factors**						
3.1	Does the Methodology include a risk analysis method based on financial factors?	low	medium	no	medium	high	no
3.2	Does the Methodology support risk financing	no	no	no	medium	medium	no

		ISO31000	TOGAF	SP800-30	MEHARI	MAGERIT	OCTAVE
	strategies for the residual risk?						
4	**Innovation**						
4.1	Towards assessment of the support to concept of Technology Roadmap one in ECHO, does the methodology …	…	…	…	…	…	
4.1.1	... enable analysis of a StoryLine or a UseCase from D2.1?	medium	no	medium	medium	high	medium
4.1.2	… support the provisioning of a selection of roadmaps of ways (e.g. Controls) to reduce the risk?	no	low	no	high	high	medium
4.1.3	… enable/define linkability to tools/ICT products?	no	no	no	medium	medium	(very) low
4.2	Does it support the concept of Curricula (like defined in ECHO)?	no	no	no	no	low	no
4.3	Does it support the concept of Certification Scheme (like defined in ECHO)?	no	low	no	no	low	no
4.4	Does the methodology identify transversal, inter-sector and specific skills for Curricula?	no	no	no	no	no	no
4.5	Does the methodology provide a basis for Training Programmes?	medium	no	no	no	low	no

Table 14: ECHO Requirements coverage matrix.

As stated in the introduction, it is necessary to understand which risk assessment methodology could be used (and how deeply it could) or eventually be extended/adapted within the E-MAF trying also to classify its strength and weak points. The analysis highlighted that no widely used and well documented methodology explicitly takes into account inter-sector parameters: all methodologies can be applied within the ICT landscape of multi-sector environment, without a specific focus on single sectors and without a clear methodology to develop single sectors focused extensions. Inter-sector dependencies (for example, threats and vulnerabilities taxonomies) are not clearly listed and considered in the risk analysis.

Transversal factors (for example policies and regulations) are taken into account within these methodologies, although not always explicitly or at an enough detailed level. MEHARI, for example, defines generic transversal security controls related to compliance with existing laws and regulations without entering in any specific detail.

Looking more in detail to the criteria that have been defined to assess the suitability of each method to ECHO, we also can state the following.

From the analysis of Table **14** it emerges that the best coverage of the requirements is provided by MEHARI and MAGERIT. For some aspects, they seem to be also complementary. For example, regarding the taxonomies, MEHARI provides a knowledge base based on asset category, while MAGERIT provides rules and guidelines to build and expand the taxonomy.

With respect to the reproducibility and repeatability concepts, MEHARI methodology is very well detailed at each steps, scales are clearly defined (but also open to expert modification): the procedure can be run by different analysts with comparable results. Moreover MEHARI establishes a clear link between business risk and security risk, even though it is traced only in one direction at the moment (e.g. it is possible to address identified security risks from the business risks – the malfunction – but it is not possible to say which security risks causes which malfunction). This is of utmost importance in order to achieve management commitment and resources.

Both of them provides tools to run the assessment and among the ECHO partners, RHEA has also developed two web-based software able to run a full risk assessment based on MEHARI.

MEHARI taxonomy needs to be specialized with respect to the different sectors, and maybe the MAGERIT taxonomy could be applied to carry out this specialization.

In terms of benchmarking and scales definition, it is important to establish clear criteria to define the scales: this is extremely critical in the certification context, where assurance levels are defined against the level and type of risks that need to addressed by a certain product or service. MEHARI provides good support for this but it needs to be tested in a certification context.

Unfortunately, none of the analyzed methodologies provide useful inputs with respect to curricula and training, so these aspects need to be further investigated elsewhere.

As a final conclusion, since a RA methodology is needed to build the E-MAF, the suggestions from the analysis is to consider interesting aspects of the two methodologies MEHARI **[22]** and MAGERIT **[20]** as starting points. Another element to inspire to is the FAIR Risk Analysis in TOGAF **[33]**. As it is depicted in Section 5, the E-MAF is taking his road, based on an architectural design which is different from any of the analysed methodologies and frameworks, but clearly inspired (even for isolated features) to them.

With this respect, it would be extremely useful to evaluate the availability and interest of the respective authors to be part (somehow) of the initiative and support the evolution or even to the merge of the selected methodologies with E-MAF improvements in order to achieve the identified requirements.

3. Analysis of existing Cyber Security Framework adoption in the sectors of interest

3.1 Analysis methodology and criteria

After the definition of the state of the art in Risk Assessment frameworks in the previous chapter (top-down analysis), the next step is to analyse how these frameworks have been applied in the ECHO-sectors and sub-sectors (**healthcare**, **energy**, **maritime**, defense and space), inter-sector and transversally (bottom up analysis). As already stated the final product of T2.2 will be the E-MAF Multi-sector Cybersecurity Framework, which obviously is a cybersecurity framework (see Section**5.2**), and the iterative approach will move from design and implementation of Risk Assessment methodology and framework to the final E-MAF by passing through the ECHO Risk Management Framework. This is the reason why we need to look at current adoption and deployment of existing Cybersecurity Framework to clearly depict the state-of-the-art in ECHO-sectors. Before engaging in the analysis, this introductory paragraph will explain with deeper details some methodological considerations.

The main goal of a Risk Assessment Framework is to serve as an approach for prioritizing the risks posed to an organization, thus enabling a sound decision making in terms of allocation of resources. When applied to the ECHO-network and competence hub that the ECHO project is creating, this statement means that the ECHO Risk Assessment Framework should support the evaluation of the cyber incident risk in the sectors the ECHO project covers. The identification of inter-sector, multi-sector, and transversal aspects will build the basis for the further abstraction/extension of RA methodology which could be easily applied to a wider set of sectors and actors. Aspect identification will be done in a comprehensive way, tackling the vertical and horizontal dimension of the domains:

- Vertical analysis: by zooming in on each specific sector;
- Horizontal analysis: by looking at the transversal/inter-sectoral aspects, i.e. covering more than one sector.

The horizontal analysis is a key added value in today's interconnected and interdependent world. It is also a core part of the vision of the ECHO project: delivering an EU trans-sectoral and inter-sectoral cybersecurity concept.

For each domain (vertical) a specific analysis is performed to investigate how the ECHO-sectors apply the risk frameworks to their key business processes. This analysis will be done in a uniform way in four sub-headings:

- A general description of which are the main used risk frameworks in the specific domain;
- A general description of the sectors' key business processes, the critical IT-assets related to these business processes and the main security challenges affecting these processes (typology of cybercrimes);
- An analysis of the sector storylines of D2.1 **[1]** (which define cybersecurity incidents/crimes) in terms of how they relate to the main security challenges identified in the sectors and the critical IT-assets. Potential gaps can be identified here;
- A concluding paragraph listing the initial, domain related general requirements for the ECHO assessment framework based on the outcomes of the previous sub-headings.

These methodological steps will lead to a clear assessment of what the needs are for the ECHO risk assessment framework for specific domains. The gaps between target security and current security levels will represent a clear qualitative metric to understand what is missing in the current solutions.

The horizontal analysis will follow a different path, as it will first define what is intended by transversal and inter-sectoral risk assessment. After that, it will research whether the existing risk assessment frameworks do cover by design transversal and inter-sectoral risk assessment. Furthermore, it will look at the sector analysis and identify what frameworks are in use in two sectors or more.

It will also identify whether there are key trans-sectoral and inter-sectoral business processes and security challenges and how the storylines of D2.1 **[1]** cover these. Finally, it will define in a concluding section the transversal and inter-sectoral general requirements for the ECHO assessment framework.

The two dimensional analysis will track the route for the innovation of the RA activities and the following identification and isolation of transversal, inter-sectoral, multi-sectoral elements being the added value of ECHO Multi-sector Assessment Framework.

3.2 Health Care sector

As the health care sector continues to offer life-critical services while improving treatment and care by involving new technologies, cyber threats can have critical impact on people's life. In the last 5 years, more than 125 million people were affected by cyberattacks in the Health Care sector. As widely reported in the ECHO deliverable D2.1 **[1]**, if cyberattacks are an increasing threat across all critical infrastructure sectors, as for the health sector they are especially worrying, because they can directly threaten not just the security of medical systems and information, but also the health and safety of the patients. Innovation in *health information technology* is surely one of the main achievements in addressing clinical problems considered unresolved until recently, but the technology itself is an added value only if it is secure.

Another element highlighted by reports dealing with security in the healthcare sector is that the healthcare industry is behind other industries in protecting its infrastructure and digital health information. Despite the huge yearly general investments by both public and private Health Service actors, cyber security is not yet seen as important as it should be. A cyberattack can void important investments, reducing the availability of key services.

Health organizations are then now addressing the need to provide reassurance to patients and, in general, to healthcare players that their internal processes, infrastructures, medical devices are under an efficient supervision and protected by adequate security measures.

From this growing awareness, surely more evident in the USA than in Europe, comes a correspondingly increasing demand to comply with health organizations security with recognized security frameworks and standards.

It should be emphasized that:

- In the healthcare domain, errors in addressing cyber issues have an impact not only at organization and financial level, but produce a loss of credibility and patient trust;
- The size of the health organization (small, medium, big hospitals) is not relevant, as cyber-attacks are indiscriminate, affect healthcare systems of every dimension;
- An effective approach to cybersecurity is based on the fact that all actions are a shared responsibility, involving people from the health organization, but also processes and technological infrastructures and devices;
- Awareness-raising of personnel working in healthcare settings on security and data privacy is important to reduce cybersecurity vulnerabilities;

- The European health organizations seem less ready to address Cyber Security issues through a formalized approach, which implies to earn cyber security certifications. Many structures are lagging behind, even if there are virtuous examples scattered throughout Europe.

Just as an example of this situation, we report the experience of the Italian hospital "Casa Sollievo della Sofferenza"[20], whose personnel, according to what reported by the Director of the hospital Information Services, is working on a cyber security assessment program which includes:

- Evaluation of the cybersecurity risk through the NIST framework;
- Evaluation of the compliance with respect to GDPR through the “Privacy Assessment Tool” for ICT in Health designed by the Italian Association of Healthcare IT Systems. The level of maturity of Data Inventory, Organizational measures, Application measures, Technical Measures and Risk Management is assessed every two years;
- Assessment (every two years) of the hospital cybersecurity adopted measures, following the model proposed by the Research Centre of Cyber Intelligence and Information Security of the “La Sapienza” University of Roma;
- Assessment of the hospital cybersecurity risk profile made (on yearly basis) by the hospital Insurance Company through a questionnaire for the hospital administration;
- Vulnerabilities assessment carried out by the company (Telecom Italia) hosting the public online services of the hospital;
- Analysis (on daily basis) of the threats and mitigation actions carried out by the adopted antivirus solution;
- Check and monitoring (on daily basis) of the IT network infrastructure at firewall level;

- Specialized Courses to raise privacy and cybersecurity awareness, involving at least 600 participants per year.

Coming back to the security frameworks and standards, the following part of the section highlights a set of the most widely tried, tested and used CS frameworks in the healthcare domain. Taking into account what reported above, the identified frameworks come from to an in-depth analysis carried out in 2018 by the Healthcare Information and Management Systems Society – North America (HIMSS) **[42]**, whose aim was to find out what medical cybersecurity frameworks are the most popular in the American health sector. The analysis results are reported in the table below.

Framework	Percent
NIST CSF	57.9 %
HITRUST	26.4 %
Critical Security Controls	24.7 %
ISO	18.5%
COBIT	7.3 %
Other	5.1 %
No framework	16.9 %

[20] https://www.operapadrepio.it/it/

Table 15: Most used Security frameworks in USA [42].

A brief description of the most applied CS frameworks and standards is then reported.

3.2.1 NIST Cyber Security Framework

The (American) National Institute of Standards and Technology (NIST) has developed its Cyber Security Framework (CSF) that can be adopted by various sectors or organizations to improve the management of cybersecurity risk. It is, according to the American Healthcare Information and Management Systems Society (HIMSS **[42]**) the most adopted CS framework in the Healthcare sector (57.9%).

The NIST CSF **[27]** framework is built on the foundations of threat modelling, threat intelligence, and collaboration. It is aimed to support organizations to perform adequate risk analysis, proactively address active and emerging threats and cooperate to effectively address cyber threats. Please refer to Section **2.4** for an initial assessment of the NIST Risk Management and Risk Assessment Frameworks adopted in the CSF.

The Framework was created in 2014 to reinforce the resilience of critical infrastructures and is widely used by all private and federal organizations in the United States. It is then new and has yet to be accepted in Europe and generally speaking outside USA.

3.2.2 HITRUST Common Security Framework

According to the *2018 HIMSS Cybersecurity Survey***[42]**, 26.4% of the interviewed healthcare information security professionals showed their preference for the Health Information Trust Alliance (HITRUST) security framework. Some of the most important healthcare organizations (e.g. Anthem, Humana, UnitedHealth, and Walgreens) are part of this private association[21], which maintains and offer a certifiable and recommended framework trusted by many health networks and hospitals to manage risk, the so called Common Security Framework (CSF). CSF is a clear example of the HITRUST commitment to provide a framework fitting for any healthcare organization: it is a global and flexible framework, compliant with standards such as HIPAA, ISO, COBIT (see below), and NIST.

The CSF is certifiable and uses the ISO/IEC 27001:2005 Information Security Management System**[15]** as its foundation, primarily with the objective of supporting non-US organizations, even if it is not a standard for the HC domain. Though it has been adopted internationally, it is yet to be localized outside the USA. HITRUST CSF v9.3 **[43]** is the latest version of the framework, published on Oct 15, 2019.

[21] https://hitrustalliance.net

3.2.3 CIS Critical Security Controls

According to **[42],** the(24.7%) of the interviewed professionals give their preference in terms of healthcare security frameworks to the Critical Security Controls, provided by the *Centre for Internet Security* (CIS[22]). CIS is a community-driven non-profit organization, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. The 20 CIS Controls are security practices organized and accessible through a list[23], which starts from "Inventory and Control of Hardware Assets" and includes the vulnerability management, malware and boundary defenses, data protection and so on. Anyway, the CIS controls are not expected to provide a complete healthcare cybersecurity framework: they are often used re often used in conjunction with other frameworks, such as NIST. Version 7 of the CIS 20 Controls **[44]** was released in March 2018.

3.2.4 ISO 27000

Again according to the *2018 HIMSS Cybersecurity Survey***[42]** report, 18.5% of respondents work with the ISO standards. ISO stands for *International Organization for Standardization*, the international standard-setting body composed of representatives from various national standards organizations. It is headquartered in Geneva, Switzerland, and works in 164 countries.

The ISO/IEC 27000 – or simply "the ISO" – are a series of standards for realizing and maintaining an information security management system, work done in cooperation with the International Electrotechnical Commission (IEC).

Among the other related standards like ISO/IEC 27001, 27002, 27003 and so on, the information security requirements are featured on ISO/IEC 2700**[15]**. Standards like 27002 and 27003 are "codes of practice" or definitions aimed to support the requirements in 27001.

Others listed under 27000 are "codes of practice" or definitions to be used to in support of the requirements in 27001.

The latest version is ISO/IEC 27001 Information Security Management Systems Requirements**[15]**, published in 2013. In this document, Section **2** analyses ISO 31000**[10][19]** devoted to Risk Assessment.

3.2.5 COBIT

About 7.3% of respondents follow COBIT (Control Objectives for Information and Related Technologies) **[45]**, an IT governance framework created by the non-profit organization ISACA (Information Systems Audit and Control Association) aimed to provide organizations with instruments to bridge the gap between control requirements, business risks, and technical issues. It offers an implementable set of controls over Information Technology and organizes them around a logical framework of IT-related processes and enablers. The group describes its COBIT 5 framework as the "overarching business and management framework for governance and management of enterprise IT".

[22] https://www.cisecurity.org
[23]https://www.cisecurity.org/controls/cis-controls-list/

Today, hospitals and insurance companies are joining financial institutions, governments and private corporations in adopting COBIT that has become an integrator for IT best practices by harmonizing other standards. The framework further allows covered entities to optimize resources while mitigating risks. Seemingly, COBIT is focused on efficiency and effectiveness of IT environment, rather than information security linked to business issues. However, the framework is used to implement practices provided by other information security standards such as the NIST Cyber Security Framework and ISO27001/2.

The latest version of the COBIT framework, COBIT 5, was released in April 2012.

3.2.6 ECHO healthcare scenarios: weaknesses and potential mitigation actions

Digital assets and data generally require protection. This is much true in Health Service. When mostly unlimited access to networked medical devices, equipment, personal computers, client and servers is obtained, the likelihood of either a Critical or Catastrophic event increases (to Likely or even Frequent) generating an extremely high risk or an high-risk impact for the organization. Assets are quite always equipped with password protection only which is not enough for cybersecurity aims.

Taking into account also the human factor, the systems usually involved in cyberattacks are:

- Monitoring and Information systems;
- Hospital equipment and devices;
- IT and communication infrastructure;
- Enterprise and Clinical Service;
- Hospital Staff.

The assets primarily affected by cyberattacks are:

  - Networked medical devices;
  - Networking equipment;
  - Identification components;
  - Client devices;
  - Clinical networked information systems;
  - Enterprise information systems;
  - Data Centre;
  - Information;
  - Staff;
  - Buildings;
  - Mobile and wearable devices;
  - PCs and laptops;
  - Backup and storage devices.

The criticality is often high due to the wide range of attacks the HC sector is subjected to. The likelihood is generally high also because of the lacks in security awareness. A general statement about the recovery time and efforts after a generic attack cannot be provided. Depending on the type of attacks and how successful attacker activities are, time to detect and recovery may vary. The obvious statement is that a prompt reaction is very important. For a more detailed description of HC StoryLines and UseCases please refer to D2.1 **[1]**.

Loss of sensitive data, e.g., may lead to a clear case of patient identity theft, and, with thousands of records potentially stolen, the medical practitioner reputation could be at stake if all the patient records make it to the dark web for sale. Terabyte of privacy-protected data can be stolen every day. They can be organized and used for several scopes, depending on the goals of cybercriminals activity.

Also, databases are well-known vulnerability points for the HC actors and it could be very risky if a database contains modified medical data. In lack of any data integrity protection technique, hospital staff do not know which digital data have been modified.

Loss of access credential is obviously another critical issue. Remediation is obtained, in some cases, by the adoption of a PAM system to be configured, at least for critical accounts, to work under third-party authorization. In this case even the supplier has to be authorized to the maintenance of equipment and devices. Also a periodical password change for users can be seen as a simple but effective countermeasure.

It is quite generally understood that several attacks cannot be successful in lack of the contribution of at least one staff member. For this reason, as stated in the following, an appropriate training process for the human factor in the hospital should be considered unavoidable.

Moreover, diagnostic, treatment, and surgical services can be easily made unavailable. Hospital operation capabilities are reduced and patient's trust zeroed.

Identified key countermeasures include:

- Trainings and awareness raising, the most important measure for the staff; having an information security strategy available for all smart assets in the hospital is focusal; a common understanding of systems and components as well as their interactions is very important;
- Identifying appropriated roles and responsibilities: clear assignment of roles and responsibilities for all people in addition to regular training and awareness raising activities are key elements of a proactive approach to information security;
- Improve organizational processes, like scheduling up periodic backups, making them protected and available on demand, antivirus and anti-spam, software patching and updating; also medical system and devices configuration errors compromising either (or both) operation or (and) cybersecurity posture should be avoided as well as system and device failures which are serious threats in HC, particularly due to the increasing complexity and dynamics of the systems;
- Policies and procedures, for IT or service request verifications, use of social media, reporting of suspicious people within the hospital perimeter, etc.; moreover: create a BYOD and mobile device policy for all users; identify assets and their interconnection to the Internet and refuse built-in network capabilities;
- Audits, with e.g. penetration tests, in order to improve appropriate control in several circumstances (e.g. access control to resources) as well as incident identification and assessment of corrective/improvement actions; proactive and reactive means such as asset classification, risk analysis and audits are key resources;
- Network segmentation to isolate critical parts of the network and use of Smart Firewalls; separating critical parts of the network from non-critical ones is crucial: e.g., in HC it is recommended to separate medical devices to the other more office-related components (typically susceptible to a wide range of attacks); devices with known vulnerabilities not to be easily removed should lay on a separate (and isolated) network (or not connected to the network at all;
- Setting up an authentication and authorization infrastructure to clearly and strongly authenticate users as well as evaluate their permissions to access to a given resource, when they request to.

The analysis of the Healthcare scenarios reported in the ECHO D2.1 **[1]** deliverable provides a picture suitable to identify specific needs in terms of security risk governance.

The following table, starting from the D2.1 **[1]** four storylines and corresponding use cases, summarizes weaknesses and potential mitigation actions of the cyber-attack types there described. The comparison of the

weaknesses and mitigation actions is aimed to highlight the gap between the current and the target cyber security levels.

Cyber attack type	Weakness	Potential mitigation action
Social engineering attacks on hospital staff		
Lack of Security in hospital staff credentials/logins release process	Vulnerability in the authentication and authorization service	Adoption of a Privileged Access Management (PAM) system Assignment of a Registration Authority to safely manage identities
Phishing campaign redirecting to a fake copy of hospital website	Lack of efficiency in IT services Insufficient cyber-awareness by the hospital personnel	Certification of the IT equipment, with special attention to the network services Training for the hospital staff
Intentional modification of digital medical images	Lack of efficiency in IT services Insufficient cyber-awareness by the hospital personnel	1. Certification of the IT equipment, with special attention to the network services 2. Training for the hospital staff
Tampering with medical devices		
Theft of electronic health records through hacking a connected medical device	Vulnerability of medical devices connected to remote access (e.g. patches not implemented promptly) Use of old and unpatched commercial, off-the-shelf software and operating systems Lack of vendor effective security management Lack of cooperation (contracts) with device manufactures	Adoption of specific information security practices, such as: security risk assessment of new devices and validation of vendor practices on networks or facilities contract and cooperation with device manufacturers Development and implementation of network security applications and practices for device networks
Hospital havoc through hacking a connected medical device (terrorist attack)	Vulnerability of medical devices connected to remote access (e.g. patches not implemented promptly) Use of old and unpatched commercial, off-the-shelf software and operating systems Lack of vendor effective security management Lack of cooperation (contracts) with device manufactures	Adoption of specific information security practices, such as: security risk assessment of new devices and validation of vendor practices on networks or facilities contract and cooperation with device manufacturers Development and implementation of network security applications and practices for device networks
Cyber assassination through an implanted medical device (terrorist	Vulnerability of medical devices connected to remote access (e.g. patches not implemented promptly)	Adoption of specific information security practices, such as:

Cyber attack type	Weakness	Potential mitigation action
attack led by Intelligence Services)		security risk assessment of new devices and validation of vendor practices on networks or facilities Development and implementation of network security applications and practices for device networks
Theft or loss of hospital equipment or data		
Stealing or losing equipment and devices	Lack of asset inventory and control Lack of physical security practices (open offices and poor physical access management) Lack of simple security measures on hospital equipment (e.g. computer cable locks to protect devices within the work environment) Lack of awareness about the spread of the theft practice in hospitals Lack of effective vendor security management, including controls to protect equipment	Implementation of a security policy to face hospital equipment theft User awareness training on securing the devices
Insider Accidental Data Loss	Poor skill, little attention from hospital staff Lack of effective vendor security management, including controls to sensitive data	Improvement of organizational processes, like scheduling up periodic backups Acquisition and use of data loss prevention tools Increase of (cybersecurity) awareness and training among the hospital personnel
Theft of Medical Data	Lack of efficiency in IT services and security services Lack of adequate internal processes to manage patients' information and data Insufficient cyber-awareness by the hospital personnel	Implementation and use of privileged access management and data loss prevention tools Improvement of organizational processes (e.g. scheduling up periodic backups, making them protected and available on demand, antivirus and anti-spam, software patching and updating) Conduct regular (cyber) security training to improve employees' education and awareness
Malware Attacks on hospital information systems		
Attack against IT infrastructure (by e-mail phishing)	Lack of awareness training.	Staff training to increase awareness

Cyber attack type	Weakness	Potential mitigation action
	Lack of IT instruments to scan, manage, test and validate e-mails, their potentially malicious content /bad links, senders	Improve organizational processes (e.g. scheduling up periodic backups) Use of Antivirus and anti-spam, software patching and updating Network segmentation, to isolate critical parts of the network Setting up an authentication and authorization infrastructure
Ransomware attack (by e-mail phishing)	Lack of awareness training. Lack of (IT point of view) : system backup antiphishing instruments anti –malaware detection tools network security controls (e.g. segmentation, authentication and authorization controls)	Staff training to increase awareness Patching and keeping software always updated. Running antimalware and anti-spam (on IT equipment/devices and Cloud-based data/applications, clinical networked information systems, medical devices, SCADA, mobile devices to connect to health information system, etc. Performing full or incremental backups on regular intervals

Table 16: Cyber-attacks in the Healthcare sector[1].

3.2.7 Conclusions

From the described analysis, some important concepts arise in relation to the HC sector:

- An increase in vulnerability and threats is expected, not only as a consequence of the increasing adoption of IoT devices. The Health Care sector could exploit the availability of a common reference in Europe for Risk Assessment, such as ECHO E-MAF, in order to increase the level of protection with a shared and mature solution and to learn from more mature sectors through inter-sector and transversal features as well as experiences made by other European entities even if operating in different sectors;
- The complexity of Health Care systems must be reduced. Innovation and ICT should help in introducing solutions to allow a better understanding, management, and control of the several parts of an HC system which could be first identified and then isolated. Opening the Health Care to the concept of Technology Roadmap, as defined in ECHO, could introduce a new approach in facing cyber risks;
- The need for the definition of specific cyber security Skills and Curricula is now clear for all levels of staff members. This could fix the lack of awareness who is limiting the responsivity of the HC Systems to attacks. Curricula and Skills as defined in ECHO would help the HC sector in making a huge step ahead towards a completely new cyber security level;
- The budget in hospitals and HC organizations balances should be increased and cyber security risk assessment and management should be seen as main activities toward the improvement of services;

Policies on cyber security skills/features should be requested when provisioning of Equipment and Devices. They should be defined at international level so that all HC actors in Europe could have a common reference for their requests to suppliers.

3.3 Energy Sector

Electrical Power and Energy System (EPES) has special needs in terms of cybersecurity mainly due to real-time requirements in involved Supply Chain. For this reason, special consideration must be paid to cascading effects triggered, e.g., by blackouts. Also, cross-section implications must be considered as well as possible consequences of mixing old and new technologies, not always providing the same level of compliance with cybersecurity requirements. The challenges identified from D2.1 **[1]** StoryLines can be grouped in the following categories[24]:

- *digital aspects* since recent digital technologies play a fundamental role in the energy system, imposing higher risks, increasing threats and vulnerabilities;
- *older technologiesin legacy systems issues* due to that fact that those systems were designed when the technical specifications did not include cybersecurity;
- *control systems issues* since EPES might not be disconnected from the network when attacked;
- *micro grid operations issues* to improve tolerance to attacks and cascading effects;
- *new security approaches* in detection and prevention.

FireEye[25] detects threats compromising organizations in the energy sector **[59]** and classifies them by the malware family used. The most used are:

- SOGU (Kaba, PlugX): backdoor for file upload and download with access to filesystem and registry, process execution, remote shell access, providing the command and control server with graphical access to the desktop, etc.;
- ADDTEMP (Desert Falcon, Arid Viper): taking screenshots, keystrokes and passwords logging, file upload and download, querying information on files, etc.;
- WITCHCOVEN: logging operating systems, browsers, and applications information; it also captures streams (screen, audio, webcam), opens command shells and manipulates files;
- SpyNet: enabling hackers to interact with a compromised system (keylogging, remote shell and registry), to upload and download files (even password saved), to launch and kill processes and services, to capture streams (screen, desktop, audio, webcam), to capture images of the desktop, record from webcam and audio inputs, extract saved passwords, to turn a compromised system into a proxy server.

As regards commonly detected crimeware software in the energy sector **[59]** it is possible to enlist:

- Jenxcus (njw0rm, njworm, evolution of njRAT/Backdoor.LV): sent through emails and downloads it spreads among removable drives and steal credentials;
- HOUDINI (H-Worm, VBS-based Remote Administration Tool) using HTTP to steal and transfer data, providing command line execution, downloading and executing software programs;
- JpiProx: a Trojan in the form of a browser add-on stealing data, also able to install further malware and programs (e.g. web proxy);

[24] also inspired and merged with classification proposed by Cybersecurity & Digital Privacy in the Energy sector (https://ec.europa.eu/inea/sites/inea/files/3.03_cybersecurity_m.dionisio.pdf)
[25] source https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/ib-energy.pdf

- ZeroAccess (Sirefef): a Trojan offering rootkit capabilities.
- Upatre: a Trojan downloader arriving via a spam email.

The systems primarily affected by cyberattacks on energy domain are:

- PLCs (Program Logic Controllers);
- ICS (Industry Control Systems);
- Monitoring and information systems;
- Smart Meters;
- Routers;
- Servers;
- Storage and backup devices;
- Data Centre;
- Databases;
- Shared printers and others.

A smart meter (electricity meter) is an electronic device recording consumption of electric energy and sets up a two-way communication channel to deliver information to and from the supplier for monitoring, messaging, and billing. Communications from the meter to the network may be wireless (e.g. via ZigBree, power long range wireless, etc.) or via fixed wired connections such as power line carrier. Smart meters can vehiculate cyber attacks or be used to interfere on the consumption measurement.

The energy sector, such as many similar industrial sectors, has developed supervision and data acquisition control systems, also called SCADA systems in the latest 30 years. Today SCADA is intended as the software system for supervision, control and remote control of industrial infrastructures.

SCADA systems have evolved to a large extent as a complement to the automation solutions provided by the world's leading companies in the sector (Siemens, Allen-Bradley, Rockwell etc.) and that the terminology can vary depending on the geographical context (Europe, America, Asia) and sectorial (heavy industry, pharmaceutical industry, production and transport of electricity, transport of people, etc.) as the reference regulations and the cultural context they are inspired by are different.

Those who create and use SCADA systems are often technicians with background in industrial process control rather than IT, but today these systems are increasingly interconnected with office networks and use IT solutions that are not purely industrial to optimize increasingly geographical remote-control functions. SCADA systems that link decentralized structures as energy, increasingly use TCP-IP-based communication protocols and legacy systems.

In the energy domain since 2014, a group of BlackEnergy hackers began deploying SCADA-related plugins to target ICS (Industrial Control Systems) and energy systems around the world. BlackEnergy is a trojan that is used for DDoS attacks, cyber espionage and information destruction attacks. BlackEnergy APT Group worked in the following sectors: ICS, energy, government and media in Ukraine, ICS / SCADA companies around the world, energy companies around the world.

Since mid-2015, the BlackEnergy APT group has been actively using phishing emails containing malicious Microsoft Power Point file with 0-day exploit, MS Excel and Microsoft Word macros to infect computers on the target network. After opening the document, the user is presented with a dialog box in which it is recommended to enable macros to view the contents. Enabling macros launches a BlackEnergy malware infection.

Various Trojans were used by BlackEnergy:

- Backdoor.Win32.Blakken;
- Backdoor.Win64.Blakken;
- Backdoor.Win32.Fonten;
- Heur: Trojan.Win32.Generic[26]

Trojan activity has been detected in 27% of manufacturing companies, APT attacks (15%) and ransomware attacks (25%), cyber-espionage and theft of confidential data.

In accordance with the StoryLines in T2.1 and well-known cyberattacks in the domain, common actors and factors can be identified.

The first factor, as we have said, those who design and use these systems are often technicians with experience in controlling industrial processes rather than IT and IT security. As result of the use of legacy interconnection technologies and systems that often have no form of authentication, password or encryption, these "closed systems" are today exposed to cybercrime. Low users' awareness of cyber threats is one of the main factors, the human factor that an attacker can use to plan a strategy.

The second factor is the limited or absent governance of computer security, until now limited by the "concept" of isolation of these systems compared to the rest of the world, or of being “closed systems”. Therefore, the attackers can use often simple tools and technique to build the cyber-attack that maximize damage to the objective.

To counteract the two factors mentioned above, it is essential to determine the risk of cyber incidents of the structure with appropriate analysis methods that are able to:

- Identify the cyber risk in terms of human, systems and organizational factors such as critical assets to protect
- Protect these critical assets with both security policy and technologies fully implemented
- Detect anomalies following best practices and procedures to analyse event related to, and if an attack is ongoing, takes respond actions.
- Respond to an attack following best practices and procedures to mitigate effect and saving the critical assets, but if it is not possible move to fast recovery of the normal operational status through well done Recovery plans.

Today, the main topics listed above are at base of the Risk Analysis In for the energy sector and, more in general for all critical infrastructure.

The European Parliament and Council Directive (EU) 2016/1148 of 6 July 2016 (also known as NIS Directive **[58]**) requires all member states to analyse cyber risk by evaluating the governance of IT security of critical infrastructures, especially the energy sector. Each nation of EU has acted in this regard by supplying the owners of critical infrastructures of the energy sector with reference analysis models. Most of these models and methodologies for RA are based on existing security frameworks and standards. Highlighted in the following part of the section a set of cybersecurity frameworks which resulted to be the most used in the energy domain at the end of our investigation:

- MEHARI;
- MAGERIT;

[26] https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/

- IEC/ISO 31000;
- OCTAVE;
- NIST;
- ISO 27001;
- COBIT.

3.3.1 MEHARI

MEHARI (MEthod for Harmonized Analysis of RIsk)**[22]** is a risk assessment and management (RA/RM, see Section **2.5.1**) asset-based method involving users in the assessment. This perfectly fits with the special knowledge and needs of Critical Infrastructure (CI) management organisations even the qualitative approach adopted by MEHARI for the analytical techniques, which relies on expert opinion, introduces a certain degree of subjectivity on the results. Please refer to Section **2.5.1** for more details. The Energy sector deploys MEHARI since it provides a full RM model compliant to ISO27005. MEHARI contains a complete classification of assets, a well-defined likelihood taxonomy for the threats, and a methodology to measure attitude and exposure to vulnerabilities. It is able to estimate the level of risk (through automatic formulas) by operating on generic risky situations and to propose countermeasure and corrective actions.

The CI **RA** in MEHARI runs through the following phases:

- **Context establishment** for organization or its part(s);
- **Stakes analysis and assets classification**: identifying classes for data and services, estimating compliance to regulations;
- **Risk identification**: identifying and evaluating stakes, threats likelihood and countermeasures;
- **Risk analysis**: enlisting stakes, threats and vulnerabilities for the RA;
- **Risk assessment**: based on a scale with 4 seriousness levels for the organization.

The following ones are instead used during **RM**:

- **Risk assessment**, depicted above;
- **Risk treatment**, selecting the proper action among 4 possible:
    - reduce,
    - accept,
    - transfer/share,
    - avoid.

  When a decision of reduction is taken, MEHARI allows selecting the security (counter)measure to reduce the likelihood or the impact of the risk.

- **Risk acceptance**, allowing to individually accept the threat scenarios;
- **Risk communication**, enabling communication with stakeholders to be involved in the analysis.

A clear definition of Risk Identification, Analysis, and Evaluation phase is available in Section **2.2**. Context and Stakes analysis are discussed in Section **5.1**, MEHARI RM and RA details in Section **2.5.1**.

3.3.2 MAGERIT

MAGERIT**[20]** is directly related to the generalization of the use of information technology, it is a risk analysis and management methodology developed by the Spanish Ministry for Public Administrations (see Section **2.5.2**). In addition to the classical qualitative approach, this methods enables a quantitative approach in Risk Assessment providing a mathematical evidence to be used in support of decision-making under uncertainty, at the price of high-quality input data and well-developed project models which are both quite normal in Critical Infrastructure management organisations. It is an asset-based method and requires the involvement of users in the assessment process, like experts of Critical Infrastructures are. The application of the methodology can be supported by the PILAR (Spanish state administration)/EAR (commercial) software. Complex Critical Infrastructures Risk Management and Assessment usually exploit MAGERIT basic concepts like:

- *Assets* (anything that is useful or valuable for a company) and *Dependencies* between them in order to estimate the value of the damage caused to the organization by a malfunction in any of the security dimensions; this is clearly the case on the Energy domain where the damage is not strictly related to the value of critical infrastructure but, much more to the consequences of service disruption. For this reason, essential assets are on top level of the MAGERIT dependency graph, services are immediately under them, and at the last level, other assets;
- *Threats* to be identified with respect to each asset and dimension. They must be evaluated according to frequency, likelihood, and degradation provoked on the asset if they materialize.

Predefined and Custom Safeguards (countermeasures) tightly bound to threats. Together with the list of predefined safeguards associated with assets and threats, the Complex Critical Infrastructures need to define custom countermeasures.

3.3.3 ISO 31000

Implementing ISO 31000 **[18][19]**helps energy-related organizations see both the positive opportunities and negative consequences associated with risk, and allows for more informed, and thus more effective, decision making, namely in the allocation of resources. It can be an active component in improving an organization's governance and, ultimately, its performance. In addition to this, ISO 31000 Risk Management fosters the process to realise the benefits of new technology in a safe and reliable manner. As stated in Section **2.2**,provides a common approach to managing any type of risk and is not industry or sector specific and this is very valuable for complex Critical Infrastructures. It can be used throughout the life of the organization and can be applied to any activity, including decision-making at all levels.

Unlike other modern RM/RA methodologies and tools which are "asset-based", ISO 31000 (and ISO 27001:2013 **[15]**as well), represents an international standard that clearly states the ability to utilize process-based Risk Assessment. ISO 31000 **[18][19]** guidelines provide energy domain organisations with the chance to focus on services rather than assets, for the whole lifecycle, whatever the risk is, with both positive (opportunity) and negative (risk) consequences. This is much more important for energy domain since 2016, when the 2016/1148 Directive of the European Parliament and the Council **[58]** stated that the existence of a service-driven risk management is needed with the primary objective to protect essential ones for the citizen services, be they provided by a single or multiple infrastructures.

In the energy domain, ISO 31000 is applied for different purposes: in the day-to-day Risk Management and for stage gate reviews as well as permit applications. The emphasis is on the continuous improvement of risk management through setting goals for the organization, measuring, reviewing and subsequently modifying processes, systems, resources, capabilities and skills. In this aim, the ISO 31010 provides energy domain

organisations with guidance on the selection and application of risk assessment methods in a wide range of situations. Methods are used to assist in decision making when uncertainty exists, to provide information on specific risks and as part of the risk management process.

3.3.4 OCTAVE

Unlike the other methods mentioned above, OCTAVE extensive standardized documentation throughout risk assessment ensures traceability of results. OCTAVE is a risk-based strategic assessment and planning technique for security following the qualitative approach, which relies on expert opinion, at the price of a certain level of subjectivity for the results.

For several years, OCTAVE approach had been the most complete methodology for Risk Assessment for IT systems. For this reason, some organisations in the energy domain adopted it even it was not conceived for industrial systems. Because of this, its results may be less accurate than ones produced by other methods when analysing impact, vulnerabilities, and consequences in those case. For detailed information on OCTAVE RA please read Section **2.5.3**.

3.3.5 NIST

The NIST CSF has been adopted in energy sector thanks to its native capability to share cybersecurity attitude and expectation among business partners, customers and suppliers in a cross-sectoral manner. In particular, energy sector actors are learning day-by-day how to map the CSF to their current needs and approaches, as well as matching up with standards, guideline and best practices. One of the main consequences for the organisation is reducing the lack of compliance with legislation and regulations which internal policies suffers from. Another is the chance to use NIST CSF (and other frameworks) as a planning tool for strategic risk and practice assessment. More information on NIST Framework can be found in Section **2.4**.

3.3.6 ISO 27001

The attitude of ISO/IEC 27001**[15]** to deal with and protect financial data, IPR-related information, sensitive data is very important for CI sector. It is helpful to the organisation in order to improve risk identification and the proper countermeasures selection processes with tight connection with business goals leading to an effective risk management policy. The deeper understanding of threats and vulnerabilities and the cybersecurity awareness also lead to manage risks efficiently. Because of this, the personnel under organisation control must be aware of policies adopted in it (e.g. information security policy), the expected contributions they have to provide, and the negative consequences in case of non-conformity.

In this aim, organisation ensures the relevant communications (both internal and external) to Information Security Management System and, in general, to make information security process properly operate are traced and propagated. It is clearly necessary to define what, when, and how to deliver. This standard is relevant to managers and staff concerned with information for security risk management in industrial energy sector. It provides the following types of analysis:

- Situation Analysis;
- Requirement Analysis;

- Documentation requirements.

In accordance with ISO/IEC 27001:2013, information security must always be considered from a holistic perspective – this means that there are further sources of risk to an organization's information/data, and they can develop because of the following factors:

- the exchange of data within and outside of the organization;
- changes to internal organization and cooperation (particularly at large companies); (existing) systems and applications that cannot be updated or replaced;
- cooperation with external partners/service providers;
- remote access to the company network (by partner companies or manufacturers, for example);
- natural phenomena/natural disasters;
- sabotage and white-collar crime;
- humans as a risk factor (e.g., social engineering);
- using new systems and technologies (cloud and mobile devices, etc.);
- entering new markets (geographic or product-based).

All sources of risk and risk factors should be considered, but each energy-related organization has to define its own areas of focus in RM based on its field of business and the internal and external requirements that arise in that field; risks can only be managed efficiently if the risk exposure and environment of the business field in question are first analysed. A good starting point for this process would be a process map or a situation analysis.

ISO/IEC 27005:2011 can be consulted when formulating and designing the RA process. In addition to the detailed main section, the appendices contain useful tips for the implementation.

3.3.7 COBIT

The following features of COBIT were identified:

- it includes subsection "Monitor and scan the technology environment", which can be used for analysis of the technology equipment used in the facilities of an energy-related organization;
- perform systematic monitoring and scanning of the enterprise's external environment to identify emerging technologies that have the potential to create value (by realizing the enterprise strategy, optimizing costs, avoiding obsolescence, better enabling enterprise and IT processes);

It allows monitoring the marketplace, competitive landscape industry sectors and legal and regulatory trends to be able to analyse emerging technologies or innovation ideas in the enterprise context.

3.3.8 ECHO energy scenarios: weaknesses and potential mitigation actions

The domain of energy-specific anomaly detection and intrusion detection systems is fairly active. The analysis of existing frameworks for use in the energy domain to ensure risk accounting and analysis, and cybersecurity has shown that the NIST**[27]** and OCTAVE**[39][40][41]** frameworks can detect various types of vulnerabilities, record the time of the attack, and NIST**[27]** is designed specifically for critical infrastructures. Qualitative and complete risk analysis, risk management allows implementing the ISO 31000**[18][19]** standard at the enterprises of the energy domain. IEC ISO 27001**[15]** can be used to describe various cybersecurity incidents.

MEHARI **[22]** can be used to assess business risks; it does not fit the goals of the energy domain, unless updated accordingly. The MAGERIT**[20]** framework can be used for risk assessment as an additional tool.

Based on the analysis of Energy storyline from D2.1 **[1]**, we can conclude that 2 companies did not take into account the risks associated with cyberattacks, integrating a network, making sharing of cameras and printers. Proper access control, setting appropriate access policies, would avoid the serious consequences of the attack. It is advisable to conduct a risk analysis in accordance with the ISO 31000**[18][19]** standard, which sets out the steps to be taken in case of cyberattacks.

Cyber attack type	Weakness	Potential mitigation action
Cyber-attacks on [ENERGYCO] and [WATERCO] operational technology and information technology infrastructures		
Compromising of spare units	Lack of efficiency in IT services Improper management of the spare parts lockers and warehouses	Implement a proper warehouse management system Training for the warehouse staff
Social engineering attack	Lack of efficiency in IT services Insufficient cyber-awareness by the technician personnel Improper incident analysis and response	Certification of the IT equipment, with special attention to the network services Training for the staff
Physical breaking of the network printer	Insufficient access and visitor policies and surveillance. Lack of network traffic monitoring Lack of efficiency in IT services Insufficient cyber-awareness by the personnel Disclosure of reserved information	Improve access and surveillance policies Certification of the IT equipment, with special attention to the network services Conduct regular (cyber) security training to improve employees' education and awareness
Malware for a network printer firmware and attack on a printer	Insufficient access and visitor policies and surveillance.	Improve access and surveillance policies
Keylogger on a network printer	Lack of network traffic monitoring	Monitor network traffic
Remote access via a network printer	Lack of network traffic monitoring Default password use	Monitor network traffic Lack of password policies
Inter-sector attack	Lack of network traffic monitoring Improper file sharing policies Anti-malware detection tools	Monitor network traffic Lack of Network security policy Running antimalware.
Unauthorized access and control of a SCADA system	Lack of network traffic monitoring Obsolete/Vulnerable Public key infrastructure	Monitor network traffic Security risk assessment
Anomaly detection	Lack of network traffic monitoring	Monitor network traffic Lack of response plan

Table 17: Cyber attacks in the Energy sector[1].

3.3.9 Conclusions

As happened in the last decades, the demand of electricity provisioning is expected to increase by 80% between the years 2012 and 2040. So, the CIs in the energy sector are obviously requested to improve their resiliency, fault tolerance and robustness through a considerable investments ($7.6 trillion over the next 25 years[27]), while their plants simultaneously move towards a more modern, innovative, scalable, distributed structure. In this landscape, a more effective approach must take place when considering issues related to Information Management Systems, training programmes, involvement of staff and professionals, organisational attitude and appetite for Risk Management also in terms of tools, methods and methodologies. For these reasons, an effective RM approach should require that the organisation periodically:

- periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context; this requires definition and continuous review of a set of indicators;
- report on risk, progress with the risk management plan and how well the risk management policy is being followed; and
- review the effectiveness of the RM framework, also monitoring risk management plan progress and deviation with respect to the original objectives.

The organisation is obviously demanded to develop/ensure the capabilities (experts involved) to identify the source of the risks and the risks themselves (independently whether they can be controlled or not by the organisation) as well as to evaluate impact areas and levels, to identify events, their modifications when situation changes, related sources/causes and consequences/effects. Depending on the organisation and its risk attitude and appetite, its internal competencies/capabilities, its objectives the proper Risk Identification techniques and tool should be applied and also identify the relevant information to keep always up-do-date to continuously support Risk Identification process.

It is also necessary to train personnel what actions should be performed when the attack begins. Network devices, PLCs must be protected from attacks by configuring the built-in firewalls and the hardware firewall. Authorization, authentication, and accounting must be performed. Databases must be encrypted and backed up. It is also desirable to provide demilitarized network zones.

3.4 Maritime Sector

The maritime transport industry is increasingly using information and operational technology systems that depend on digitization, integration, automation, and network-based systems. This reliance has created an increasing need for cyber risk management in the shipping industry.

The impact emerging from the cyber risk threats are underestimated because they are not widely spread and rarely occur. Increasing awareness obviously is the first necessary step to assess and mitigate the cyber risk, as well as to think about it as a concrete treat because of the high level of impact a single violation of security can cause. This can be intended not only as loss of money, but also as causing environmental issues, loss of human lifes, etc.

[27]https://www.microsemi.com/applications/industrial-m2m-wireless/smart-metering

3.4.1 IMO guidance

Recently, the International Maritime Organization (IMO) has published "G*uidelines on high-level recommendations on maritime cyber risk management*" **[46]**. By January 1, 2021, vessel owners and operators must have incorporated measures to manage cyber risk into their existing risk management processes, which have traditionally focused on the physical risks to safe shipping operations.

For cybersecurity risk management, IMO proposes a framework based in five functional elements, which are not sequential, but all should be concurrent and continuous in practice and should be incorporated in a risk management: *identify*, *protect*, *detect*, *respond*, *recover*. The approach to cyber risk management described herein provides the basis for understanding and managing cyber risks, thus enabling a risk management approach to address cyber threats and vulnerabilities. The IMO refers to the requirements of the member states, as well as relevant international and industry standards and best practices:

- The Guidelines on Cyber Security Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI **[101]**, named the "BIMCO guide" in the following;
- SO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements;
- NIST Cybersecurity Framework (NIST CSF).

3.4.2 Guidelines on Cyber Security on board Ships

The aim of the BIMCO guide **[101]** is "*to offer guidance to ship owners and operators on procedures and actions to maintain the security of cyber systems in the company and onboard the ships*". In compliance with this statement, in **[101]** a RM methodology/framework aims at provisioning a well-defined list of outcomes. It enlists the following four objectives:

- *identify the roles and responsibilities of users, key personnel, and management both ashore and on board;*
- *identify the assets, data, which if disrupted, could pose risks to the ship's operations and safety;*
- *implement technical and procedural measures to protect against cyber incident;*
- *finally implement activities to prepare for and respond to cyber incidents.*

The guide **[101]** also introduces the set of Critical Security Controls (CSCs) including both technical and procedural aspects as well as prioritization. The CSCs must ensure effective and affordable defense mechanism at organisational level.

Technical protection measures indicate the controls that are relevant for cybersecurity on board ships:

- limitation and control of network ports, protocols and services;
- configuring of network devices such as firewalls, routers and switches;
- secure configuration for hardware and software;
- physical security; wireless access control.

Procedural controls are focused on how personnel use the onboard systems. Some examples are: training and awareness; software maintenance and upgrades; anti-virus updates and use of administrator privileges.

In this guide, a key concept regards Information Technology (IT) and Operating Technology (OT) systems onboard ships and their differences. OT is hardware and software that directly controls physical devices and

processes. IT covers the spectrum of technologies for information processing, including software, hardware and communication technologies.

3.4.3 Cyber security resilience management for ships and mobile offshore units in operation

Like the IMO, the NIST Cyber Security Framework has also been accounted for in the development of these guidelines. "*Cyber security resilience management for ships and mobile offshore units in operation*" **[47]** is a recommended practice (RP) that guides owners, managers and operators of ships and mobile offshore units towards enhanced cyber security of their assets.

This RP recommends three different assessment levels, each serving a different need and using tailored methodologies.

- High-level assessment: it focuses on technical aspects, awareness, policies and enforcement mechanism.
- Focused assessment: this RP proposes a systematic and focused approach to assess the effectiveness of barriers (or countermeasures) against threats.
- Comprehensive, in depth assessment: this RP is based on a detailed inventory of the IT and an automated control related processes. It is also recommended to determine the consequences of successful attacks for each of these concerning CIA triad plus authenticity (CIAA). The comprehensive, in depth assessment is built on the requirements of the ISO/IEC 27001 standard as well as on other standards that are accepted such as the "BSI Grundschutz" (BSI is the German Federal Office for Information Security) or the "IEC-62443-3-3" (Standard on Industrial communication networks) requirements.

The assessments just described above will help to identify areas for improvement. The improvement actions to be realized typically fall within the areas of competence and awareness, technical improvements (e.g., access control, software configuration management and barrier management) and the implementation of an Information Security Management System (ISMS). Once the cyber security of an organization has been assessed and improvement actions initiated, the achieved improvements should be verified and validated. This RP proposes two different approaches: monitoring and testing of technical and procedural controls, and verification of ISMS. As already mentioned, the guidelines refer to best practice from NIST CSF, BIMCO and ISO/IEC 27001 as sources of additional guidance and standards.

Referring to NIST Framework for Improving Critical Infrastructure Cybersecurity is foreseen in Maritime sector This Framework presents an approach for managing cyber security in critical infrastructure protection and therefore applicable to the shipping sector. In fact, the five functional elements presented by the IMO for risk management (Identify, protect, detect, respond recover) are those indicated in the NIST Cyber security framework guide.

Considering a cyber-attack scenario in industrial ship sector (MT01) that hit a member of the crew and the consequent actions that allow the impairment of the ship navigation system, the standard NIST provides the capability to address an objective value of risk for the specific technology and threat events.

Also, in the scenario of an insider member of the crew in a cruise ship (MT02) with the aim of sabotage the ship, the NIST CSF approach could have highlighted the risk related to the threat events "exploit vulnerabilities of internal organizational information systems".

We can consider the NIST cyber security risk assessment methodology a good way to manage the cyber risk. But there are some aspects that can introduce some issues in the “Step 2: conduct assessment”, more in detail the phases related to the identification of the threat sources and the identification of the vulnerabilities can be very difficult due to the scope of assessment: a ship can be considered as a “system or systems”, composed by hundreds of systems.

3.4.4 ISO27001

ISO/IEC 27001**[15]** is the most applicable standards for network and information systems security in the maritime domain and is divided into ten clauses, which support the implementation and maintenance of an ISMS, and an annex A, that defines in detail controls to be used for the main clauses of the standard.

A risk assessment process in the maritime domain is necessary for what concerns the cyber security of the technological system in an industrial ship.

The top-down approach proposed by ISO 27000 series framework outlines the requirements for Information Security Management Systems and gives organizations guidance on how to establish, implement, maintain and continually improve an ISMS. In this case we can focus upon the main critical systems and implement the specific controls in order to mitigate the cyber risk related to the critical aspects of the ship (e.g. navigation, safety system, etc.). For this approach, we can identify as an issue the different actors operating on the ship during the ship construction and lifecycle phases that could introduce a complexity during the definition of the ISMS. The ISO also has an approach less technical related to the NIST and could be far from the real case scenario of a ship.

3.4.5 TOGAF

The TOGAF standard **[30] [33]**, being an enterprise architecture methodology that considers a high-level approach to manage an enterprise architecture, does not provide an adequate way for managing cyber risk in a maritime domain as the shipping industry meets very strict regulations. Please refer to Section **2.3** for a detailed analysis of TOGAF and TOGAF RA.

3.4.6 ECHO maritime scenarios: weaknesses and potential mitigation actions

In accordance with the StoryLines in T2.1 and well-known cyberattacks in the domain, a common list of actors can be identified. They act as triggers in one or more cyberattacks and are enlisted among round brackets in the following list:

1. insiders (moved by personal reasons like dissatisfaction, revenge, etc.);
2. external actors moved by;
    a. industrial espionage (business);
    b. war actions or terrorism (political);
    c. hacktivism (environmental/social aspects);
    d. curiosity of passengers/clients to test the infrastructure among vulnerability (curiosity).

Regardless of the origin of the attack, the emerging and mostly leveraged vulnerabilities can be enumerated in the following list:

1. human factor intended as:
    a. source of sabotage, unintentional error and lack of awareness;
    b. destination of social engineering, phishing and fraud;
2. IT hardware and software rarely updated and assessed after the ship launch:
    a. system not patched promptly against 0-days;
    b. lack of regular assessment plan;
    c. lack of continues control over vulnerability;
3. default password use;
4. not properly air gapped IT networks:
    a. devices used for multiple functions, bridging although sealed networks causing the spread of the infection:
        i. active devices, such as PC, improperly connected to network air gapped by design
        ii. use of unauthorized devices in a restricted zone
            1. personal PC, Notebook, mobile device
            2. unauthorized Memory Devices (USB) (case study: Stuxnet[28])
    b. network misconfiguration or improper management
        i. improper direct access over Internet
        ii. misconfiguration of firewall, ICS and antivirus

The domain players usually face assessment not only of the raw ships as a “system of systems”, but also of fleet as swarms of ships, as well as of dedicated operation control stations and related assets (ports, offices, etc.). Usually, within a ship it is possible to identify some or all the following (groups of) systems:

- Navigation, dealing with the position and the route of the ship like navigation system (INS) and voyage data recorder (VDR);
- External communications, providing a communication channel from the ship to the onshore environment (SATCOM, radio station);
- Internal communications, providing communication solutions inside the ship like, e.g., Wi-Fi system, alarm and call systems, telephone system;
- Safety systems, guaranteeing the safety of the on-board crew, including fire detection system (FDS), public address and general alarm system (PA/GA), and emergency shutdown (ESD);
- Platform systems, providing to the ship the ability to ship, including automation system (IAS), propulsion system, and the thrusters;
- Cargo services, aimed at loading, unloading and monitor e.g. the crude oil cargo transported;
- Crew services, supporting the crew, like time control services, email services and corporate IT devices (PCs, tablets and mobile phones);
- Passenger’s services, supporting cruise passengers like local entertainment system, shop alarm systems, hospital systems and payment systems.

The most common threats are intentional with a purpose or unintentional virus or malware. A ship can be attached to the bridge's command and control systems, cartographic and radar control systems (ECDIS), to energy control systems or to ship and engine automation. The bridge personnel can be deceived about the position of the ship, the speed and other control parameters. The effects can be devastating. An attack on the bridge systems can isolate the verbal communication systems: in the event of loss of contact the engines and

[28] https://en.wikipedia.org/wiki/Stuxnet

the route remain the ones set and without communication the Engine Control Room staff can cause an accident. The Blackout is one of the most dangerous situations for a large vessel in navigation, there are at least two distributed redundancy systems (emergency line powered by Emergency Diesel) and ship UPS. No emergency system logic has proven to be infallible in countless circumstances, so a power supply attack has catastrophic domino effects.

Every one of the above systems is a valuable asset to be (both individually and jointly) protected against from internal and external cyberattacks originating from the above mentioned actors. Even a single point of failure can potentially impact the remaining systems allowing e.g. to vector an attack via a bridge originating from a weaker system not properly assessed, to access network and system designed to be air gapped. To conclude the ship automation has full control of the engines and interacts with countless IT equipment, including the Voyage Data Recorder. This VDR, or black box, has also recently been linked to electronic mapping systems that also operate remotely to allow the ship owner to control the ship: access via satellite connection to these systems means bypassing all the security designed to be null or non-existent as it is dedicated to isolated networks. Do not underestimate the local passage of software / data or cartographies with infected USB flash drives: a ransomware attack on the bridge could have various consequences.

The presence of subsystems affected directly by vulnerabilities belonging to other domains (e.g. the ship energy generation and management system, falling in the energy domain; the hospital system, falling in the healthcare domain) highlight the need of multi-sector assessment framework otherwise that would require an assessment by his own, as exposed in the Section **2** of this document.

Identified key countermeasures include:

- Trainings and awareness raising, the most important measure for the staff; a common understanding of systems and components as well as their interactions is very important;
- Hardener the infrastructure to neutralize the effect of malicious behaviour conducted by insiders;
- Identifying appropriated roles and responsibilities: clear assignment of roles and responsibilities for all people in addition to regular training and awareness raising activities are key elements of a proactive approach to information security;
- Improve organizational processes, like scheduling up periodic backups, making them protected and available on demand, antivirus and anti-spam, software patching and updating;
- Policies and procedures, for IT or service request verifications, use of social media, reporting of suspicious people, etc.; moreover: create a BYOD and mobile device policy for all users; identify assets and their interconnection to the Internet and refuse built-in network capabilities.
- Audits, with e.g. penetration tests, in order to improve appropriate control in several circumstances (e.g. access control to resources) as well as incident identification and assessment of corrective/improvement actions; proactive and reactive means such as asset classification, risk analysis and audits are key resources;
- Network segmentation to isolate critical parts of the network from non-critical ones is crucial e.g. ; use of smart firewall and IDS and Air gap on critical parts of OT, IT, guest network and office-related components (typically susceptible to a wide range of attacks); devices with known vulnerabilities not to be easily removed should lay on a separate (and isolated) network (or not connected to the network at all;
- Setting up an authentication and authorization infrastructure to clearly and strongly authenticate users as well as evaluate their permissions to access to a given resource, when they request to.

The analysis of the Maritime scenarios reported in the ECHO D2.1 **[1]** deliverable provides a picture suitable to identify specific needs in terms of security risk governance.

The following table, starting from the D2.1 **[1]** two storylines and corresponding use cases, summarizes weaknesses and potential mitigation actions of the cyber-attack types there described. The comparison of the weaknesses and mitigation actions is aimed to highlight the gap between the current and the target cyber security levels.

Cyber attack type	Weakness	Potential mitigation action
Cyber-attacks on an Industrial ship		
Phishing campaign targeting internal employees and crew	Lack of efficiency in IT services Insufficient cyber-awareness by the crewmembers	Certification of the IT equipment, with special attention to the network services Training for the crewmembers
Spread of malware using unauthorized devices in restricted zones	Lack of efficiency in IT services Insufficient cyber-awareness by the crewmembers	Certification of the IT equipment, with special attention to the network services Training for the crewmembers
Cyber-attacks on cruise ship systems		
Cruise Navigation System Cyber Attack (Hacktivists)	Use of old and unpatched devices with off-the-shelf software and operating systems Vulnerability of network devices Lack of efficiency in IT services Insufficient cyber-awareness Default password use	Training for the crewmembers Adoption of specific information security practices, such as: security risk assessment of new devices and validation of vendor practices on networks or facilities contract and cooperation with device manufacturers Development and implementation of network security applications and practices for device networks
Cruise HVAC System Cyber Attack (Cyber criminals and industrial espionage)	Human factor: sabotage from insiders Vulnerability of devices connected to remote access (e.g. patches not implemented promptly) Use of old and unpatched commercial, off-the-shelf software and operating systems Lack of vendor effective security management Lack of cooperation (contracts) with device manufactures	Adoption of specific information security practices, such as: security risk assessment of new devices and validation of vendor practices on networks or facilities contract and cooperation with device manufacturers Development and implementation of network security applications and practices for device networks
Takeover of a cruise ship (terrorism)	Insufficient cyber-awareness by the crewmembers Vulnerability of devices connected to remote access (e.g. patches not implemented promptly)	Training for the crewmembers Adoption of specific information security practices, such as: security risk assessment of new devices and

Cyber attack type	Weakness	Potential mitigation action
	Use of old and unpatched commercial, off-the-shelf software and operating systems Lack of vendor effective security management Lack of cooperation (contracts) with device manufactures	validation of vendor practices on networks or facilities Development and implementation of network security applications and practices for device networks
Cargo Management system intrusion (Insider)	Human factor: sabotage from insiders Insufficient cyber-awareness by the crewmembers Lack of asset inventory and control Lack of physical security practices (open offices and poor physical access management) Lack of simple security measures on hospital equipment (e.g. computer cable locks to protect devices within the work environment) Lack of awareness about the spread of the theft practice in hospitals Lack of effective vendor security management, including controls to protect equipment	Training for the crewmembers Adoption of specific information security practices, such as: security risk assessment of new devices and validation of vendor practices on networks or facilities contract and cooperation with device manufacturers Development and implementation of network security applications and practices for device networks

Table 18: Cyber-attacks in the Maritime sector[1].

3.4.7 Conclusions

Given the extremely interconnected nature of the devices on board a large vessel it is difficult to draw up a taxonomy of the most exposed parts to be defended. The useful life of a ship is over 20 years and some systems are updated and made compatible with those that remain active. The ship and engine automation system is born and dies with the ship while, for example in a cruise ship, everything related to navigation and on-board comfort of passengers (hotel management and security control) passes under various stages of update called retro-fit. From the described analysis, some important concepts arise in relation to Maritime sector:

- As in the other domains an increase of vulnerability and threats is expected in the upcoming future, because of the unavoidable increase of use of systems relying on digitisation, digitalisation, integration, and automation, which call for cyber risk management on board. As technology continues to develop, IT and OT are networked together and often connected to the Internet, making the risk malicious attacks greater. The Maritime sector could exploit the availability of a common reference in Europe for Risk Assessment, such as ECHO E-MAF, in order to increase the level of protection with

a shared and mature solution and to learn from more mature sectors through inter-sector and transversal features as well as experiences made by other European entities even if operating in different sectors. The Risk Assessment on new devices but also on ones already in place seems to be a common factor in almost all the UseCases discussed in D2.1 **[1]**.

- The introduction of a systematic and periodic risk assessment based on the innovative approach proposed by ECHO should also reduce the likability of treats through the set-up of more effective software maintenance and patching activities as well as the provisioning of certified hardware. The systematic improvement of the definition and the scheduling of security practices would be an additional factor to finally deploy proper risk governance on board.
- The human factor often the most leveraged to exploit access to critical IT and OT. The crewmember awareness should be increased through the definition of cyber skills and training programmes as well as the proper roles among the crew.

Given the non-holistic approach to a ship's system of systems and the different strategy of updating the equipment, there is very little that can be done to trace a line of protection for the past and the future. Avoiding to connect every vital apparatus on the satellite network or to make it provide active USB ports on the bridge or in the other control rooms is not the proper countermeasure. For the future, the maritime domain should start from the already established industrial standards like IEC 62443 (ISO 62443-3-3 System security requirements) **[48]** and NIST SP 800-82 r2 **[26]** but the path has just begun and will clash with the conservative mentality of the naval world.

3.5 Defence and Space Sectors

At the time of this writing, the available information of Defense and Space sectors are the one already highlighted in D2.1 **[1]**.

At the current stage of the research in T2.2, a preliminary analysis has been performed according to available information not covered by (un)disclosure policies, especially when dealing with departments of defense in European countries. Thus, the collected information require future improvement in order to have information useful for E-MAF implementation. Also, the information presented in this deliverable are limited due to the same reasons.

Based on gained experiences, the methodologies used in the defense sector are some of those already described in Section **2**. Generally speaking, it is possible to state that some of the most important players in the international scenario adopt one or more Frameworks or Methodologies between TOGAF, NIST SP-800 series, ISO 27000 series, etc. They are melted or combined with National CSF and regulation to obtain an acceptable value for residual risk, when dealing with organizations which are particularly sensible to cyber risks.

Naturally, due to (un)disclosure policy it is not possible to discuss with deeper details on actors and modalities of methods, methodologies and framework deployments. However, it is possible to provide a general picture, accordingly to available public information released by all national military commands and by supra-national provisions/organizations. This picture enables some important conclusions.

In fact, the analysis conducted on the RA/RM reference scenarios shows that in the field of defense numerous initiatives are promoted at international scale to verify the ability to interact and collaborate in the event of cyberattacks.

In this aim, it is first of all necessary to mention the existence of the *Cyber Coalition*. It reached its 12th edition in Dec 2019 (Tartu, Estonia) and, with the participation of 900 cyber-defenders from 28 NATO Alliance nations and several partner nations/organizations that put in practices consolidated international technical collaboration procedures, under the coordination of NATO's Allied Command Transformation, to protect and defend the "Alliance Cyberspace" as well as to conduct military operations within and through. The partners

worked together to manage cyber threats continuously evolving in through training in realistic scenarios. The main goal was to sstrengthen the capabilities to protect Alliance cyber space and validate organisational and national practices and procedures on information sharing, cyber risk awareness and decision making.

In the experimentation track, the Cyber Coalition Exercise ran three experiments supporting a fruitful understanding of innovation and technology in the cyber space through key elements such as:

- research and development,
- experimentation,
- capability development,
- training.
- etc.

The third of them targeted the multi-level situational awareness, a better understanding of cyber environment, and facilitating decision-making which are goal that also ECHO plans to reach.

Furthermore, of particular relevance is the *NATO Cooperative Cyber Defense Center of Excellence* (CCDCOE) in Tallinn, Estonia, a real international priority think tank which organizes two exercises every year: the *Crossed Swords*, an event reserved for Red Teams, and the *Locked Shields*. Locked Shields, in particular, is the flagship exercise of the Center and is the most complex *live-fire* exercise (attack-defense in real time) in the world. In the 2019 edition, about 30 participating nations (more than 1500 people) were involved in 23 Blue Teams in the defense of complex systems (such as power plants, 4G networks, drone piloting systems, communication systems) from over 2500 attacks of different types.

Finally, there are several initiatives by individual nations that provide NATO, or partner nations, with exercise events organized by military bodies aimed at testing the interoperability of the C4 systems (Command, Control, Communications, and Computer) of the Defense in the several nations to be used during joint military operations; among them stand out:

- The Bold Quest, "trial" exercise (Multinational, Joint, Collaborative Enterprise), organized annually by the US Department of Defense and characterized by the effort to integrate, in a synergistic way, different capabilities of the military sector (Integrated Air Missile Defense, Joint Fire Support, Friendly Force tracking, Coalition Intelligence Surveillance and Rec0nnaissance, etc.), as well as providing adequate cyber defense to deployed networks
- CETATEA, exercise of interoperability of C4ISR/CIS systems (Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance/Computer and Information Systems) conducted every year by the Romanian army, focuses, instead, on development, testing and validation of CIS structures to be used in future multinational/NATO operations, including logistic support systems, protected by a specific cyber security center.

It is clear that, the current international effort in the defense sector is not focused on the development of new protocols and analysis methodologies for risk analysis and management but rather on the cooperation between different countries that use consolidated technological solutions (either frameworks or technologies) in accordance with what is defined by European directives and international standards.

The illustrated international exercises highlight both in the defense sector and in other sectors it is necessary to strengthen the operators' skills and competences. This aspect is fundamental in the ECHO project which focuses competence and staff as assets and for this reason it is of equal importance in the methodological framework.

This section will be finalized by exploiting information to be inserted in the next version of D2.1 **[1]**, also. Modelling of UseCases and possible mitigation actions will be presented. Additionally, CAIRIS will be used to identify gaps and needs for other tasks (T2.3 to T2.7).

Cyber attack type	Weakness	Potential mitigation action
Naval operation to assist Forisma		
Hacking of the satellite control centre to eavesdrop satellite traffic	Maintenance operation error, VPN default credentials, PSExec, Powershell	Secure maintenance procedures Security-by-default-procedures Vulnerability and patch management To be further analysed
DVB-S hijacking	Spoofing a web service request	Link encryption Authenticity and auhentication measures To be further analysed
ECDIS disruption through VSAT vulnerability exploitation	Weak remote access configuration; the lack of segregation of critical systems	Network segregation and access control Secure remote access practices Policy for portable devices To be further analysed
Access to an internal IP based CCTV circuit from satellite communications directed to on board personnel	Buffer overflow, MPEG TS software parser, clear text transmission	To be further analysed
Cyber Attacks on EUSIB+SDR Systems		
Black Hole Attack	In MANETs, every node act as a router and a host. This means that all nodes have information about the network topology	To be further analysed
Man in the Middle Attack	In MANETs, every node act as a router and a host. This means that all nodes have information about the network topology	To be further analysed
Cyber Attacks on the EUSIB HQ General Computer Network		
Wi-Fi router firmware attack	Wi-Fi firmware vulnerabilities Possible Man-in-the-middle (MITM) Personnel Missing data encryption OS command injection Unrestricted download of dangerous file types Reliance on untrusted inputs in a security decision Cross-site scripting and forgery URL redirection to untrusted sites	Vulnerability and patch management Integrity algorithms Awareness training Link encryption Application security (OWASP Top10) Input data screening and sanitization Password policy Antivirus To be further analysed

Cyber attack type	Weakness	Potential mitigation action
	Path traversal Weak passwords Software that is already infected with a virus	
Man-in-the-middle attack	Wi-Fi firmware vulnerabilities Possible Man-in-the-middle (MITM) Personnel Missing data encryption OS command injection Unrestricted download of dangerous file types Reliance on untrusted inputs in a security decision Cross-site scripting and forgery URL redirection to untrusted sites Path traversal Weak passwords Software that is already infected with a virus	Vulnerability and patch management Integrity algorithms Link encryption Application security (OWASP Top10) Input data screening and sanitization Password policy Antvirus To be further analysed
USB flash stick malware attack	Wi-Fi firmware vulnerabilities Possible Man-in-the-middle (MITM) Personnel Missing data encryption OS command injection Unrestricted download of dangerous file types Reliance on untrusted inputs in a security decision Cross-site scripting and forgery URL redirection to untrusted sites Path traversal Weak passwords Software that is already infected with a virus	Vulnerability and patch management Integrity algorithms Link encryption Application security (OWASP Top10) Input data screening and sanitization Password policy Antivirus Portable device security policy To be further analysed
Supply Chain intrusion attack		
Malware attack via email attachment	Lack of, or inadequate management commitment Lack of, or inadequate personnel screening Insecure teleworking mechanisms	Security awareness training Risk management process Password policy To be further analysed

Cyber attack type	Weakness	Potential mitigation action
	Insufficient security training and awareness Loose access control lists Lack of, or inadequate security controls in suppliers' services No security monitoring Poor compliance Weak developer passwords	
Server intrusion	Lack of, or inadequate security controls in suppliers' services Insecure software and systems acquisition, development and maintenance procedures Insufficient protection of information systems Poor compliance	To be further analysed
Denial of a service attack	Vulnerable server	To be further analysed
Data theft	Vulnerable server	To be further analysed
UAV under cyber-attacks		
Attack to UAV mission planning tool by using international military information sharing network	UAV's GPS system, International information sharing system	To be further analysed
UAV GPS spoofing	UAV's GPS system, International information sharing system	To be further analysed
Attack to UAV sensor system	UAV's GPS system, International information sharing system	To be further analysed

Table 19: Cyber-attacks in the Defence and Space Sectors[1].

3.6 Inter-sector and transversal aspects

3.6.1 State of the art and transversal/inter-sector factors

The current EU panorama is still missing a common understanding of the inter-sector, sector specific and transversal opportunities as well as the relationship of security disciplines to the development of technology roadmaps and demonstration cases.

The challenge taken by ECHO will also be the development of a strong foundation for a comprehensive multi-sectoral Risk Assessment Framework, complemented by specific operational guidelines and metrics for each of the sectors examined. A risk-based framework provides a structured process and guidance to help organizations identify and assess those risks and take steps to reduce them to an acceptable level. The multi-sectoral framework will refer to standardized methodologies for risk scoring, so to enable the framework be certifiable and affordable. That way, it will also provide the necessary support to formal certification/assurance processes against the upcoming E-MAF controls for adopting organizations.

Transversal cybersecurity factors are industrial sector agnostic/independent (e.g., personal data privacy protection) while ***inter-sector factors*** are sector related, but span over several ones. E–MAF is aimed at developing a method for assessing the transversal and inter-sectoral technology challenges and opportunities.

The **ECHO Multi-Sector Assessment Framework** is built on the following WP2 analysis:

- Multi-dimensional analysis of **security disciplines** (e.g., cryptography, network security, application security, IoT/cloud security, etc.);
- **sector specific use cases** (e.g., analysis of sector specific needs and challenges);
- **transversal cybersecurity needs analysis** (e.g., common cyber-security needs such as policies, regulations, and skills frameworks);
- **Inter-sector technology and dependency analysis** (e.g., identification of common technology roadmaps solving inter-sector technology challenges).

3.6.2 Transversal challenges and opportunities

Task 2.3 is about transversal cybersecurity challenges and opportunities: it takes as input the results of sectors' scenario and use case analysis performed in Task 2.1 and conducts detailed analysis of transversal cybersecurity challenges that appear prevalent independently from the industrial sector.

These include the following main challenges common to all sectors concerned with cybersecurity focusing on potential social, cultural, human factors, ethical and legal barriers. Specific impacts and root causes of these threats are explained in D2.3 **[2]**. Opportunities are the mitigations envisaged for each transversal risk/issue identified and could be used in E–MAF for security controls identification and organizational countermeasures selection.

Human factor

- Cognitive
    - Cognitive bias
    - Risk perception
- Behavioural
    - Locus of control
    - Internet addiction
    - Gambling
    - Cyber loafing
    - Shopping addiction
    - Password storage
    - Password weakness
    - Privilege abuse
    - Human error
- Psychological

    - Social engineering
    - Job satisfaction
    - Stress, depression and anxiety
    - Fear
    - Fatigue and burnout
- Individual differences
    - Impulsivity
    - Personality Traits
- Organizational factor
    - Miscommunication
    - Insider threat
    - Political motives
    - Cyber vigilantism
    - Inadequate or non-updated trainings
    - BYOD
- Technology designed and organized for end user
    - Privileged accounts
    - Network design
    - Device tampering
    - Critical infrastructures lacks

Economical and financial aspects

- Financial squeezing
- Corporate espionage
- Crypto jacking

Legal, ethics and regulatory aspects

- Applicability of International law in cyber space
- Shifting ethical values
- Non-compliance towards data protection regulations and directives
- Application security

Strategic/societal

- Geo political
- Defence policy
- Cyber terrorism
- International relations
- Fake news
- Hacktivism

Detailed description of common challenges and related opportunities have been identified and Detailed description of common challenges and related opportunities have been identified and documented in D2.3 **[2]** Transversal cybersecurity challenges and opportunities. Dependencies on common factors are depicted in the following picture, extracted from D2.3 **[2]**:

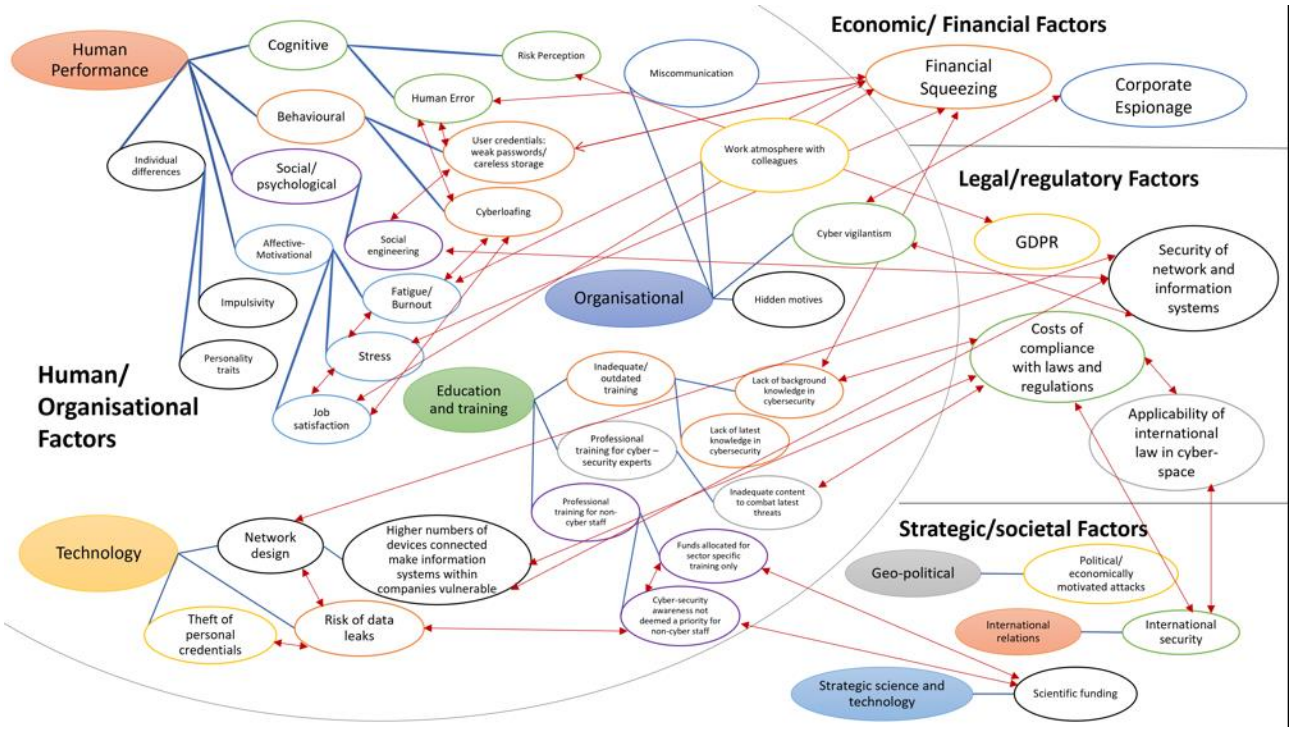

Figure 12: Dependencies on common factors in transversal cybersecurity challenges and opportunities.

It does worth to recognize that risks do not occur in isolation, but often interact, by instigating a cascading or concurrent effect which in turn can leave cyber-systems vulnerable.

Looking at the bullet point areas aforementioned, we can identify **key transversal and general security needs** like, e.g.:

- Awareness of cyber threats
- IT expertise and skills
- Effective internal communication
- Employees life cycle management: recruiting, hiring, management, resignation
- Account management: identity access management and authorisations.
- Internal security policies and procedures
- Supplier selection/performance, contractual compliance, termination of service and transfer
- Prevention, detection and monitoring of cyber threats
- Privacy and Security Risk assessment
- Financial and budgetary requirements
- IT investments decision making and ROSI (Return On Security Investment)
- Data classification, management and monitoring
- Resilience of Infrastructure
- Regulatory compliance

Based on those needs, some **key transversal business processes** can be identified, like:

- Support Processes
    - HR Management
    - Compensation and benefit Management
    - Staff Training
    - Data Management

- Quality Management
- Internal Audit
- Supply chain Management
- Physical security and safety Management
- Infrastructure Management
- Legal Management
- Financial Management
- Governance Risk and Compliance
- IT Support

- Core processes:
  - core processes are business specific, so they are not transversal

In order to identify the **key transversal security processes,** we consider the following implications:

Risk category -> Security Need -> IT Countermeasure -> Associated Security process

In the following table, it is reported the logical steps to find out possible key security processes that each sector should put in place. The risk category is identified from the use cases in D2.1 **[1]**.

Risk Category (Storylines)	Security Need	Internal Policy	IT Countermeasure	Security Process
Malware	Protection of ICT infrastructure, network, end points	Business continuity and disaster recovery policy; Data Breach policy; Policy regarding malware, email and Internet usage;	Monitor the infrastructure for security related events; Recover from security related events; Implement and maintain Security patches and virus control;	Network Management; Incident Management Problem Management; Security Incident Management; Data Breach Management; Threat and Vulnerability Management; Awareness Program Management;
Insider Threat	DLP; Awareness training; Prevention with Recognition/ disciplinary actions;	Log Management Policy; Disciplinary Policy; Recognition policy; Policy regarding malware, email and Internet usage;	Social engineering campaign; DLP solutions; Monitor the infrastructure for security related events; Recover from security related events; Accounting of privileged users actions;	Awareness Program Management; Threat and Vulnerability Management; Log Management; Performance and recognition management; Users account management
Critical Infrastructure / services disruption	Protection of critical assets	Backup Policy; Log Management; Policy; Roles and responsibilities policy; Communication Plan; Business continuity and	Backup and Restore; Access controls (firewall, IPS, authentication, authorization….); SIEM; SOC; CERT; Redundancy Disaster recovery site	Network Management; Threat and Vulnerability Management; Log Management; Business continuity and disaster recovery management Security incident management

Risk Category (Storylines)	Security Need	Internal Policy	IT Countermeasure	Security Process
		disaster recovery plan		
IoT hijacking	Prevent IoT abuse and misuse	Secure configuration policy	Security by default	Configuration and change management Threat and Vulnerability Management;
VoIP Attacks	Countermeasures for: Virus, worm, Trojan horses; DoS; Sniffing; Phreaking; Eavesdropping; Spoofing; Man-In-The-Middle (MITM); Exploiting of OS; Call Hijacking; SPIT (SPAM for VoIP); Media Access Control Flooding; SIP Bomb; SIP TDS (Tearing Down Session); SIP Bindings;	Secure configuration policy	Security by default	Network Management; Asset Management; Configuration and change management Threat and Vulnerability Management;
Attacks to Complex Specific Systems	Security by Design and by Default; Monitor, Evaluate and Assess the System of Internal Control; Monitor, Evaluate and Assess Performance and Conformance;	Access control policy; Users life cycle management; Specific system procedures; SLA and KPI management policy;	IAM solutions; Profiling and authorisations; Log tracking and system alerts; IT expertise and skills; Monitoring solutions;	Identity Access Management; Awareness Program Management; Roles and responsibilities management;
Weak/non updated Operating systems and software applications	Protection against new and evolving threats and attacks	Change Management policy; Application security policy;	Periodical updates; Legacy systems maintenance/integration;	Change Management; Application Management; Threat and Vulnerability Management;
Missing funding for security	Financial and budgetary requirements for security standards and regulation implementation	IT investments decision making and ROSI (Return On Security Investment) policy; Roles and responsibilities policy;	Optimal cost and effective Purchasing of software for Cyber Security purpose;	Business ownership of IT;

Risk Category (Storylines)	Security Need	Internal Policy	IT Countermeasure	Security Process
Theft of devices	Data protection;	Data classification policy; Data management guidelines; Cryptographic policy; Physical Security policy; Secure use of devices policy; Data Breach policy; Disciplinary policy; Access control policy; Backup Policy;	Asset inventory; Data Encryption; Secure asset disposal; Strong password enforcement; Backup and backup test;	Asset management; Backup Management; Security management
Hacking of Mobile devices	Protect mobile devices and local information	Cryptographic policy; Secure use of devices policy;	Asset inventory; Data Encryption; Patch management	Asset management; Backup Management; Security management
Theft / Interception / corruption / deletion of Data	DPIA (Data Protection Impact Assessment) for personal data; Regulatory compliance; DLP; C.I.A.;	Data classification policy; Data management guidelines; Cryptographic policy; Roles and responsibilities policy; Data Breach policy; Disciplinary policy; Password policy; Backup Policy; Data retention policy;	DLP (Data Loss Prevention) solutions; Cryptography; IAM solutions; Log Tracking; Monitor, evaluate and assess compliance With external requirements; Secure erasure; Secure disposal; Backup and backup tests;	Asset management; Backup Management; Log Management; Privacy Management;
Unauthorized access	Awareness for social engineering; Access control;	Remote access control policy; BYOD policy; Physical security policy;	IAM solutions; Access control technologies; Physical security controls;	IAM; Awareness Program Management; Physical security Management;
DoS	Data availability;	Business continuity and disaster recovery policy;	Anti - DoS solutions; SOC; CERT; IDS, IPS, Firewall;	Network Management;

Risk Category (Storylines)	Security Need	Internal Policy	IT Countermeasure	Security Process
Third Part Supplier	Defines technical limitations on sharing and using information; Providing a set approach to selecting suppliers including the acceptance criteria for terms of business;	Supplier management policy; Privacy contractual clauses;	Monitor supplier performance and compliance; Manage supplier relationships and contracts;	Suppliers management Suppliers (selection, performance, contractual compliance, termination of service and transfer); Network management; Log Management;
Environmental threats	Safety; Business Continuity;	Physical security Policy; Business Continuity Plan and Disaster Recovery Plan;	Environment Monitoring; Facilities Management; Physical access to IT assets;	Physical security Management; Resilience Management;

Table 20: Risk category identified from the use cases in D2.1[1].

The following policies are due independently of the specific risk category:

- Roles and responsibilities policy;
- Information Security Policy;
- Data Protection Policy.

3.6.3 Industrial analysis of inter-sector dependencies

HEALTHCARE

Taking into consideration both **[49]** and the HC sector analysis described in Section **3.2**, the main requirements within the e-Health sector can be summarized by the following list:

- Service resiliency against cyber-attacks: procedures to automatically recover from a cyber-attack in the shortest time possible;
- Prevention against data leakage and loss of patients' data and identity theft;
- Real-time security and dependability monitoring of wearable and mobile devices;
- High awareness level in cyber security aspects for all levels of HC personnel, e.g., nurses, technicians, administrative personnel and doctors;
- System availability and business continuity for providing seamless electronic HC services;
- Secure access to critical health information by authorized professionals;
- Secure access control by end-users;
- System availability for eHealth service delivery;
- Data security and integrity, in particular related to data storage and network elements (e.g. an access router to a site hosting the e-Health application) for exchanging health data and Identity and Access Management Systems (IAM);

- Big Data secure management: medical research can largely benefit from access to a large set of data, but it needs to be ensured that data privacy as well as data integrity is preserved, and data subjects can control the usage of their data. Transparency of data usage is a prerequisite;
- Harmonization of laws among Europe;
- Security and privacy by design to be included in the next generation of HC services;
- Implementation of new devices or systems: cyber security aspects need to be planned and implemented already from the beginning, meaning the procurement, outsourcing and maintenance phases of new systems needs to be defined beforehand;
- Delocalized network of care services: securing Assisted Living systems based on mobile services and mobile wellness solutions.

From StoryLines proposed in D2.1 **[1]**, main services needed in HC sector are linked with availability of Big Data, Telecommunication and Physical security as depicted in Chapter 5 of D2.1 **[1]**.

Service	Big Data	Telecommunication	Navigation	Physical
Telephone, ISDN, SMS, and VoIP		X		X
Broadband Internet		X		
Email and file transfer		X		
Multi-voice		X		
Video conferencing		X		
Pager		X		
Digital Medical Image	X	X		
Access Credentials to Data	X	X		X
Internal Navigation			X	
Access Control	X	X		
Connected medical devices		X	X	X
Implantable medical device	X	X	X	X
Megaphone systems		X		X
Queue Management	X	X		
Care Demand Management		X		
Assess Tracking		X		X
Telemedicine		X		
Remote Patients Management	X	X		X
People Location	X	X	X	X
Informed Consent	X	X		
Multiservice network (IT assests&comms)	X	X		X
Control Center	X	X		X
Security Operation Center	X	X		X
Energy Efficiency	X	X		X
Printing outsourcing service		X		X
Business Continuity & Disaster Recovery	X	X		X

Table 21: Dependency of the Healthcare sector on Telecommunications services.

For the previous table, an evident inter-sector connection arises between HC and Energy sectors. HC devices are, in fact, clearly dependent on power supply from energy providers. The energy efficiency service implies the design, installation and maintenance of the devices necessary for telemetry and tele-management of the energy consumption of buildings and equipment as HC-related services do. Both types of energy efficiency

management solution require a deep and specific knowledge (like, e.g., energy costs, consumption prediction, etc.) in order to have an automated and efficient management of energy consumption, as well as simplifying internal audits. In those cases, the use of sensors and telecommunication solutions enable a smarter and innovative way to manage energy consumption-related issues. This brings to a clear identification of the inter-sectoral relationships between HC and ICT as well as Energy and ICT.

That way, we can easily conclude that cyber threats on Energy or Telecommunication sectors would affect primary core activities in hospitals but also secondary ones with respect to efficiency and costs.

ENERGY

The potential cyber security threats in the **energy** domain are listed below:

(i) smart meters may be used by hackers as entry points into the broader power system;
(ii) unauthorized interference on the measurement of electricity consumption (end-users);
(iii) trip a power-generating unit or modify its schedule;
(iv) cause a blackout in a big area of the grid;
(v) attack on the electricity market;
(vi) disrupt the proper functioning of the system;
(vii) attacks through the power system on civil infrastructure.

From StoryLines proposed in D2.1 **[1]**, main services needed in ENERGY sector are linked to availability of Big Data, Telecommunication and Physical security.

Service	Big Data	Telecommunication	Physical
Telephone, ISDN, SMS, and VoIP		X	X
Broadband Internet		X	
Email and file transfer		X	
Multi-voice		X	
Video conferencing		X	
Pager		X	
Access Credentials to Data	X	X	X
Access Control	X	X	
Digital metering	X	X	
Security Operation Center	X	X	X
IoT/Sensors	X	X	
Multiservice network (IT assests&comms)	X	X	X
Energy Efficiency	X	X	X
Control Center	X	X	X
Printing outsourcing service	X		X
Business Continuity & Disaster Recovery	X	X	X

Table 22: Dependency of the Energy sector on Telecommunications services.

Energy can be seen as a double source of threats in the inter-sectoral analysis. First, Energy consumption monitoring can be used to reveal the beginning of specific actions or activities in progress. Specific patterns or cyclic peaks of electrical absorption allow to identify operations.

On the other side the sudden interruption of power supply can cause malfunctioning in devices even when subjected to uninterruptible power supply services. There is a list of very common disturbances that can come in on the power lines and which can have unexpected consequences on devices and equipment. When those disturbances are used in a malicious way to compromise the cyber security processes they can be seen as clear threats for the target system. This IEEE defined power quality disturbances shown in this paper have been organized into seven categories based on wave shape:

- Transients
- Interruptions
- Sag/Undervoltage
- Swell/Overvoltage
- Waveform distortion
- Voltage fluctuations
- Frequency variations

Some surge protectors can reduce or eliminate damage from some of these perturbations but there is no guarantee that all subsystems in an hospital or on a cruise boat are tolerant to all of these disturbances. Like a short-time switching from power supplying to UPS can represent a huge chance to break security services, also the bootstrap phase in network or cyber security devices can be used to raise an attack. In the defense sector, e.g., an even short interruption of energy supply services through a disturbance can easily compromise asset maneuvers on satellites by interrupting command chains, monitoring of military operations by interruption communications or operational support in critical phases, etc. Also manipulating rated grid frequency can cause unexpected behaviors, like computers and hardware glitches, compromising up and down converters to satellites operations, introducing anomalies in phases, burning wires and electronics, inducting fires, etc. Being all other sectors strongly dependent on power supply services we can easily state that most of risks related to energy provisioning would reflect to one or more cybersecurity risk for HC, Defense, Space, Maritime, etc. domains.

DEFENSE/MARITIME

Cyberspace is not just an infrastructure, which enables weapon systems and military ICT systems. It is a domain where the strategic goals may be achieved without use of forces.

In de described use cases, defense sector is strongly linked with maritime, which in turn depends on space. In fact, they are united by several aspects like, e.g., the management of connected mobile means of transportation (cruise boats, vessels, cargos, etc. have similar issues to aircraft carriers, submarines, and other warships). All of them need power supply, knowledge of ship position in the sea (GPS, Galileo, BeiDou, Glonas, etc), engines control, etc. and are connected through data networks as well as monitored, controlled, and managed through IT and OT technologies. The same could be said for airplanes, tanks, and some of the means of road transport used by military armies. Apart of the differences between defense objectives related to National Security in addition to people's and goods safety, the assets must be managed in a similar way

The main categories of security incidents in maritime sector are listed below:

(i) Cyber espionage
(ii) Attacks on shore stations
(iii) Hacktivist initiatives

(iv) Insider threat
(v) Malware
(vi) Web application attack
(vii) Social engineering

From StoryLines proposed in D2.1 **[1]**, main services needed in DEFENSE sector are linked with availability of Telecommunication and Space services (Earth Observation, Telecommunication and Navigation).

A set of satellite services are used in order to support naval operations. Main services provided by satellite to military ships are:

(i) Telephone, ISDN, SMS, and VoIP
(ii) Broadband Internet
(iii) Email and file transfer
(iv) Multi-voice
(v) Video conferencing
(vi) Safety 505 and red button
(vii) Notice to mariners
(viii) Maritime/port regulations
(ix) ECDIS
(x) Vessel routing
(xi) Cargo management
(xii) Planned/Predictive maintenance
(xiii) Radio over IP (RoIP) via walkie-talkie
(xiv) VHF/UHF radio integration
(xv) Crew welfare
(xvi) Telemedicine
(xvii) Tele-training/certification
(xviii) Weather forecasts

From StoryLines proposed in D2.1 **[1]**, main services in DEFENCE/MARITIME depending on Satellite services are reported in the table below.

Service/Satellite	Earth Observation	Telecommunication	Navigation
Telephone, ISDN, SMS, and VoIP		X	
Broadband Internet		X	
Email and file transfer		X	
Multi-voice		X	
Video conferencing		X	
Safety 505 and red button		X	
Notice to mariners		X	
Maritime/port regulations		X	
ECDIS (Electronic Chart Display and Information System)	X	X	
Vessel tracking (AIS)		X	
Vessel routing		X	X
Cargo management		X	

Service/Satellite	Earth Observation	Telecommunication	Navigation
Planned/Predictive maintenance		X	
Radio over IP (RoIP) via walkie talkie			
VHF/UHF radio integration			
Crew welfare		X	
Telemedicine		X	
Tele-training/certification		X	
Weather forecasts	X	X	

Table 23: Dependency of the Maritime sector on satellite services.

SUMMARY OF INTER SECTOR DEPENDENCIES

In the following table are summarized sector specific services that, under cyberattack, can lead to inter sector impacts. The table should be read as: sector in row N has an impact on sector in column M because of services provided in cell (N, M) from sector N to sector M.

Inter-sector	Health Care	Energy	Space	Defense/Maritime
Health Care		no impact*	Telemedicine	Telemedicine
Energy	• IoT and Sensors based services; • Diagnostic process and equipment (CT scanners, MRI machines, PET scanners, etc.); • Therapeutic process and equipment (infusion pumps, surgical machines, medical lasers); • Life support processes and equipment (heart-lung machines, medical ventilators, dialysis machines);		• Power availability;	Energy
Space	Telemedicine	no impact*		Space
Defense/Maritime	no impact*	no impact*	IT and OT on board of ships;	Defense/Maritime
Telecommunication	• Multiservice network; • Managed Security services;	• Efficient energy management; • Central Monitoring System;	• Telephone, ISDN, SMS, and VoIP; • Broadband Internet;	Telecommunication

Inter-sector	Health Care	Energy	Space	Defense/Maritime
	• Next Generation Network Technology; • Efficient energy management; • Workplace Management; • Printing outsourcing services; • Access control technologies; • Disaster Recovery services; • Central Monitoring System; • VoIP services; • Remote Management Devices; • Megaphone Solutions; • Wearable devices; • Central monitoring systems; • Remote Patient Management;	• Workplace Management; • Printing outsourcing services; • Disaster Recovery services; • Access control technologies;	• Email and file transfer; • Multi-voice; • Video conferencing; • Safety 505 and red button; • Notice to mariners; • Maritime/port regulations; • ECDIS; • Vessel routing; • Cargo management; • Planned/Predictive maintenance; • Crew welfare; • Telemedicine; • Tele-training/certification; • Weather forecasts;	

Table 24: Summary of inter sector dependencies.

* No impacts from one sector to another is the conclusion derived from the storylines in the first version of D2.1 **[1]**: further versions of D2.1 **[1]** and new storylines could lead to the identification of inter sector dependencies/impacts not identified at this point. Nevertheless, sometimes there is a strong dependency from one sector to another and not vice versa.

3.6.4 Transversal and inter-sectoral needs addressed in E – MAF and in ECHO

E–MAF should be aimed to grant transversal and inter-sectoral benefits, such as:

- Improving transversal management processes;
- Identifying transversal and inter-sectoral skills;
- Being a basis for training programs;
- Assessing transversal and inter sector opportunities and challenges;
- Providing a risk assessment method based on financial factors;
- Improving inter-sectoral challenges governance through technology roadmaps;

- Supporting risk financing strategies for the residual risk: the framework will provide end-users a guideline to support companies in identifying the most suitable mix of risk prevention and risk protection.

The E-MAF should then provide a basis for further sector-specific analysis, transversal and inter-sector cybersecurity risk assessment that will contribute to the derivation of technology roadmaps and demonstration cases (WP4) as well as requirements analysis for the ECHO Early Warning System (E-EWS) and the ECHO Federated Cyber Range (E-FCR).

E–MAF and other WP2 outcomes will be the input of WP4, Inter-sector technology roadmaps. Indeed, the table summarizing inter sector impacts should be the starting point for further analysis in next tasks of WP2 and other WPs: this is the direction and the scope provided by the E-MAF in order to derive assets and technologies used under the services which are leading to inter sector impacts. After identifying assets/technologies under such services it is possible to plan technologic roadmaps implementing opportunities for enhanced security.

Transversal key business processes and key security processes should be the starting point to build the transversal Layer of the Multi Assessment framework, taking into consideration technological and organizational countermeasures specified in D2.3 **[2]**.

The needs identified in this section will be the basis to derive requirement for E-MAF, which should include:

- Business requirements

  what E-MAF should do; to be derived by leveraging CONOPS methodology.

- Technical requirements:

  - Functional requirements
    - functionalities E–MAF has to implement (wrt specific/transversal/inter-sector needs);
  - Non Functional requirements
    - features the E–MAF should have, included user-interaction with E-MAF. To be derived with CONOPS methodology.

In particular, among technical requirements, E–MAF will identify security controls to derive:

- from the framework adopted (between those analysed);
- from sector specific standards;
- from current WP2 analysis (security controls sector specific);
- from further WP2 analysis.

E-MAF will be able to address both

- Transversal challenges and associated risks, and
- Inter-sectoral challenges and related risks.

So, it is implicit that E-MAF should contain taxonomies addressing:

- assets, threats and vulnerabilities associated with transversal challenges and provide the chance to identify effective security controls (via technology roadmaps where not existing);

inter-sectoral technologies threats and vulnerabilities and possible security controls to govern such risks (via technology roadmaps, if necessary).

4. Analysis of methodologies from other EU Projects

4.1 Analysis methodology and criteria

The design activities of the ECHO Multi-sector Assessment Framework cannot avoid taking into consideration the meaningful work performed by several projects which faced and innovated the Risk Assessment. Some of them also provided new methodologies for RA and for RM as well, paving the way for application in every sector where Supply Chains are applied and laying the foundation for a cross- and multi-sector approach. So, the analysis of risk assessment frameworks and methodologies, will continue in this Section to provide a comparative analysis of innovative methodologies and approaches and then assess their suitability as a reference for the E-MAF. Also, other projects, not directly addressing RA issues, will be assessed with the aim to provide inspiration for complementary architectural aspects to be kept into consideration while building such a complex framework.

Since RA and RM models and methodologies were assessed in Section 2, this section will focus on outcomes of relevant projects funded by EU. They will be assessed in a twofold manner: (i) by analysing publicly available literature (e.g. produced by the projects), and (ii) inspecting official websites (both project and CORDIS) looking for official reports (e.g. deliverables).

As previously done for methods/frameworks in Section 2, the projects in this section have been analysed by taking into account the set of parameters listed in Table 4.

The selected projects/methodologies providing Risk Management/Assessment are enlisted below:

- SPARTA
- CONCORDIA
- CyberSec4Europe
- CYSM
- MEDUSA
- MITIGATE

Other EU funded projects providing innovation in complementary aspects will be:

- AEGIS
- CANVAS
- certMILS
- COMPACT
- CS-AWARE
- DISCOVERY
- DEFeND
- PROTECTIVE

4.2 Other Pilot Projects to prepare the European Cybersecurity Competence Network

4.2.1 SPARTA

The SPARTA project aims to develop a new approach for cybersecurity research in Europe through:

- the creation of a unique set of actors at the intersection of scientific excellence, technological innovation, and societal sciences in cybersecurity;
- the development of common lines of research by cooperation.

In fact, very often scattered and small teams fall short of critical mass capabilities, despite demonstrating world-class talent and results. Moreover, European scientists hold pioneering positions in relevant fields of cyber-security but this excellence does not translate into larger-scale, system-level advantages.

Thus, the project guided by concrete and risky challenges has as major goal that to setup unique collaboration means, leading the way in building transformative capabilities and forming world-leading expertise centres to be achieved through the adoption of innovative governance, ambitious demonstration cases, and active community engagement.

For this reasons, various approaches will be developed to enhance collaboration at many levels because as highlighted by several projects in cybersecurity supported by European Framework program over the past thirty years it is necessary to break the mould, to step up investments and intensify coordination.

Inside SPARTA, the main goal of WP4, Program #1: T-SHARK - Full-spectrum cybersecurity awareness, is to both develop and validate methodological, organizational and technological solutions extending cybersecurity towards comprehensive organization of security functions. It will pay attention to threat prediction and full-spectrum cybersecurity awareness. This will lead to providing high situational awareness, informing decision and policy makers on broad or long-term issues also simultaneously providing timely warnings on threats. As presented in SPARTA proposal “The problem definition is complex as the topic by itself”. For this reason the WP4 activities focus on several aspects such as:

- **Phenomena**. Cyber-attacks have evolved in time and now exploit different kinds of vulnerabilities and formed new categories of cyber-threats. As an example, they are complex by initial design, well planned, organized over the time (e.g. by stages), having often strong social engineering component, political or ideological motives, industrial/geopolitical gains. So, tackling them requires quite completely new approaches and methods.
- **Approach**. For the abovementioned complex, multi-stage cybersecurity incidents traditional cybersecurity function organization became neither sufficient nor effective. With the currently available approaches, we can only fight consequences and this is why new capabilities to fight phenomena on early phases of multi-stage operations (e.g. facing threats and not incidents, being predictive instead of reactive) are needed.
- **Governing cybersecurity**. In order to address the cyber-attacks depicted above, the new cybersecurity governance has to be organized in a cross-institution and cross-border mode in order to increase enough context information to identify correlations, make predictions and take decisions on measures on early stages.
- **Data sharing**. Challenging wider data access as well as data sharing are necessary and have to deal with GDPR, privacy, security and confidentiality issues.
- **Concept**. Even the former cybersecurity was a pretty technical issue limited to IT perimeter security, today it is turned to be focused on important and differently targeted attacks. It then requires a comprehensive approach to tackling threats by considering both their societal and technological aspects. In fact, social engineering plays a more and more significant role nowadays making former marginal aspects, like fake news and lack of information, getting a much more important role in decision making process.

- **Analysis model**. Analytics techniques can nowadays exploit the power of advanced visualization to show in a single model a set of key cybersecurity information and indicators related to threats; which one is the most efficient for cybersecurity threats is still an open question.
- **Regulatory**. Lots of regulatory questions and needs arise regarding e.g. how to define the threat, how to measure it, which privacy/ethical/other standards should be applied to balance enforcement and individual rights, etc.
- **Legal**. Also identifying a proper legal framework to apply when tackling cyber-threats, since the globality of phenomena observed from a totally new PoV and that fact that most of the threats are originated from outside the EU. It is clear the need forthe cybersecurity threat intelligence.

Currently inside the EU, several industrial players as well RTO's and academic institutions are working on separate components enabling one or another feature of the desired solution. In the international landscape, similar solutions can be found in national-level implementation in the USA, as well some of USA originated solutions, like Recorded Future, provides platform covering most of the enlisted aspects.

In the aim of WP5, Program #2 CAPE - Continuous assessment in polymorphous environments, the CAPE Program focuses on providing practical tools to product and service developers, in the following key areas:

- addressing the definition of assessment targets, including in the scope differential assessment.
- assessing the creation and validation of proper audit trails for intrusion detection, impact assessment and forensics, also including the capability to go beyond assessments of components and products, by assessing also complex services towards a more comprehensive component-based approach.
- linking with the training program to ensure that certified components and services are properly developed and operated.

That way, the CAPE Program addresses five challenges:

- developing more agile assessment and certification frameworks, similar to agile development
- automation, supporting developers in writing requirements and executing tests;
- assessing systems of systems, beyond individual components, and modularizing assessment to enable assessment of complex systems and services;
- lifetime dynamicity of environments who may have long lifespans, but where individual components might be replaced or upgraded;
- integrating execution elasticity, particularly for services.

The CAPE program is providing its input to the roadmap along with two separate challenges due to the two aspects of the program having very different expectations. The first one focuses on complexity and dynamicity of IT systems of systems, where the main issue is to adapt assessment processes to dynamicity and complexity. The second one focuses on the resilience of the physical world, embedding both security and safety features into physical components controlled through IT processes. The two challenges are felt sufficiently different at this stage to provide separate roadmap descriptions, even though both may be found in a single use case.

Below the list of the selected tools as well as a short description of the most interesting ones:

1. Frama-C;
2. Approver;
3. Foreshadow-VMM Assessment Tool;
2. NeSSoS Risk Assessment Tool;
3. IDS and SIEM Assessment Tool;
4. Risk Assessment for Cyberphysical Interconnected Infrastructures;

5. Steady;
6. Package Scanner;
7. OpenCert;
8. Sabotage;
9. Visual Investigation of Security Information for Larger Software Development Organizations;
10. Logic Bomb Detection in Android Apps;
11. Vulnerability Detection Tool For DevOps Communities;
12. AutoFOCUS3 (FTS);
13. Buildwatch (UBO);
14. VaCSInE (CETIC).

NeSSoS Risk Assessment Tool

Owner: CNR

The tool supports Risk Assessment of an organisation's IT system. The tool is questionnaire-based and aims at providing quantitative results.

It is an online tool that helps organisations to estimate their expected losses due to possible cyberattacks of various kinds. The tool asks for the core assets and potential impact, once the assets are compromised. Next, the tool requests for the information about the security countermeasures installed and practices applied in the organisation. Then, it computes the expected losses for the organisation. The tool is available in three modes: *short* (with very small set of questions) for a quick estimation, *medium* for a more in depth analysis, and *complete* for in-depth assessment.

The tool provides high level assessment, so it is important for Risk Management process at global level. The analysis targets IT networks (with possible use of cloud, mobile and teleworking[29]. Example on usage:

A person responsible for the security of a system initiates the risk assessment process in order to (i) ensure that all relevant threats are covered, (ii) estimate possible risks due to cyber threats, (iii) plan further actions for the treatment of residual risks. The process can be executed by the security team of the owner, as well as by external auditors (as well as for certification purposes, e.g., to identify the main risks, identify required protection, and analyse the effectiveness of existing countermeasures and practices).

IDS and SIEM Assessment Tool

Owner: LMT

It mainly provides network traffic stress testing. The tool generates different kinds of traffic to fulfill different testing purposes:

- synthetic legitimate traffic to provide a realistic testing environment without incurring privacy issues
- synthetic legitimate/malicious traffic bootstrapping from existing traces with the ability to apply various transformations to the resulting traffic in order to generate a wealth of different traffics and increase the size of the dataset;

[29] see https://www.cybersecurityosservatorio.it/en/ Services/survey.jsp.

- synthetic adversarial traffic which has the ability to evade a detector Adversarial learning can also feed back to the security tool to improve its detection (IDS) and/or correlation ability (SIEM).

Technologies required are adversarial learning, generative learning, neural networks. Some example usages are:

- Automatic noise generation for penetration testing;
- Results analysis to characterize IDS/SIEM robustness;
- Network traffic trace generation/amplification;
- Attack traffic mutation.

Risk Assessment for Cyber-physical Interconnected Infrastructures (MRA)

Owner: NCSRD

The main function of the MRA is the identification and modelling of the cyber-physical interconnections of infrastructure assets. Firstly, a user inserts a threat scenario, which is the initiating point for an impact assessment accounting for cascading effects within and between interconnected infrastructures. MRA follows the ISO 27005 approach, and its novelty lies on the decomposition of both the likelihood and consequences elements of risk. The tool is customizable with respect to the impacts and their importance to the network operation. Example on usage follows:

The security/IT department of a facility should engage the MRA process covering as many risks as possible to the infrastructure (or specific assets therein), and identify based on selected risk levels the most appropriate mitigation plan. The MRA tool has been applied in the risk assessment of a simple infrastructure comprising of interconnected assets (smart lights of the NCSRD facility). The smart lighting infrastructure has been subject to different types of attacks and possible impacts (both in the cyber and physical domains).

The framework behind the tool has already been used within the ISF funded project for CI Protection of national critical infrastructures, serving as a common basis for comparing different types of threats under a common approach.

The MRA tool is built on the following components:

- A user interface that allows user to input information about the infrastructure, its assets and interconnections, their properties and potential vulnerabilities and other needed ancillary input;
- A modelling component that performs a cascade analysis of the assets and estimates risk;
- A display element that transfer outputs to users;
- A database storing all required / processed / produced information. In brief, the tool work as described in the following lines. Users input enters the required inputs (infrastructure assets, properties, interconnections, safeguards, potential impacts), which are stored in the database.

The software passes the data to the modelling component and identifies:

a) Potential threats,
b) Attractive assets,
c) Interconnections and potential cascade effects,
d) Impacts (in the cyber and physical domains),
e) Risks.

This information is fed back to the user through the display element. If the tool can be extended for continuous risk assessment, the interfaces need to be customized to allow inputs from a machine readable format.

Concerning Risk Assessment and Management the project will not develop any new methodology, thus the annex related to the assessment is not included.

4.2.2 CONCORDIA

CONCORDIA project aims to address the current fragmentation of security competence. That will be done by networking diverse capabilities and competences into a leadership role via a synergistic agglomeration of a pan-European Cybersecurity Centre and to build a community with a strong cooperation between all stakeholders, understanding that all of them have their KPIs, bridging among them, and fostering the development of IT products and solutions along the whole Supply Chain.

The technological challenge is that to promote an evolvable data-driven and cognitive End-to-End Security approach for the ever-complex ever-interconnected compositions of emergent data-driven cloud infrastructure, IoT and edge-assisted ICT ecosystems.

Some of the ambitious objectives of Concordia Project are summarized below:

- the development of a Cybersecurity Competence Network to build the European Secure, Resilient and Trusted Ecosystem, including the CODE research center as coordinator and hub, and ENISA as secretary.
- the elaboration of a Cybersecurity roadmap in which are defined research paradigms;
- the adoption of an holistic end-to-end data-driven approach for the develop next-generation cybersecurity solutions;
- the setup of the CONCORDIA's virtual lab and services for the scale up of existing research and innovation;
- the creation of an Advisory Board to give strategic advice and also to improve the connection with clients and users, other research initiatives and important standardization and certification institutions;
- the establishment of an European Education Ecosystem for Cybersecurity;
- supporting European policy makers and industry by providing expertise.

Concerning Risk Assessment and Management the project will not develop any new methodology, thus the annex related to the assessment is not included.

There are interesting aspects related to specific project results to be achieved along the WP1 that will be monitored in order to improve the ECHO results.

The most important objective of WP1 is to stimulate the publication of scientific results into key journals, conferences and workshops in the broad field of cybersecurity. The SMART objective is to publish at least 100 of such papers during the project's lifetime.

The WP1 is articulated in 5 task:

➢ **Task 1.1** is concerned with device-centric security, with a special focus on IoT devices with limited resources. The task aims at:

• developing techniques for detecting misbehaving IoT devices,
• analyzing automated software update mechanisms of IoT devices,

• investigating hardware components for post-quantum cryptography, and,

• researching code analysis techniques to detect advanced persistent threats.

➢ The focus of **task 1.2** is network-centric security. T1.2 puts particular emphasis on three topics within this context: protection against (Distributed) Denial-of-Service ([D]DoS), analysis of encrypted network traffic, usage of Software-Defined Networking (SDN) to provide resilient network services. More specifically, the intention of T1.2 is to:

• investigate proactive, coordinated and distributed strategies to defend against DDoS attacks;
• collect, share and analyze data on attacks to the end of attack mitigation and attribution;
• develop techniques to monitor encrypted traffic for security purposes; and

• investigate SDN as a means to form a trusted and resilient Internet for Europe.

➢ **Task 1.3** is concerned with software/systemcentric security. Specifically, the main research topics addressed are:

• malware analysis,
• security by design: adaptive software and OSs,
• detecting service dependencies, and

• system security validation and zero-days.

➢ **Task 1.4** is concerned with data and application-centric security.

➢ **Task 1.5** is focused on user–centric security. Specifically, the main research pillars of T1.5 are:
  - *Privacy:* this task aims on developing techniques for Personal Identifiable Information (PII) leakage detection to the advertising ecosystem and the general Web;
  - *Identity Management:* the objective of this task is the development of Blockchain based methods for creating digital identities. This will allow users of Online Social Networks (OSN) to verify their real-world identities without a centralized authority for storing and managing their personal information.
  - *Social Networks and Fake News:* this task focuses on investigating techniques for identifying fake news in Online Social Networks as well as developing Blockchain based methods for suppression of fake News.

Concerning the connection between the ECHO Project and Concordia Project it is necessary to underline that:

➢ Outcomes of T1.4 and foreseen collaboration on Threat Intelligence could help improving the ECHO Threat Taxonomy in E-MAF and in other ECHO tasks (e.g. T2.7).
➢ Outcomes of T1.5 will be monitored for Risk Assessment (and consequently eventual interest ofE-MAF and E-EWS), Fake News and Social Network due to implications on online information sources for new Threats discovery. It would be worthwhile to monitor Identity Management for possible enhancement of Personal Data Information in HC sector and worthwhile of consideration while dealing with Independent and Transversal aspects as they will be defined in the aim of E-MAF (see Section **5.2**, Transversal Foundation Tier).

4.2.3 CyberSec4Europe

CyberSec4Europe is a project with a wide consortium (44 participants) that covers 21 EU Member States and Associated Countries. The project aims to address the EU and Member States' next generation cybersecurity challenges through strengthening research and innovation competence and cybersecurity capacities. Thus, the project cybersecurity research and innovation will be conducted through technology advancements supporting:

- the autonomy of the Digital Single Market;
- the security of the European citizen, European industry, the European economy and society as a whole.

In the context of the project will be tested and demonstrated potential governance structures for the network of competence centres using the best practices examples from the expertise and experience of the participants, including concepts like CERN.

Among the major objective of CyberSec4Europe there are:

- to support the implementation of the EU Cybersecurity Act, to
- to address cybersecurity challenges within the vertical sectors of digital infrastructure, finance, government and smart cities, health and medicine and transportation through demonstration cases. Moreover, a roadmap and recommendations for the implementation of the Network of Competence Centres using the practical experience gained in the project will be developed.

CyberSec4Europe is focusing the attention on:

- devising and implementing cybersecurity enablers and their development lifecycle;
- identifying and implementing techniques and methodologies for the construction of IT systems;
- exploring efficient deployment and management of trusted execution environments (TEEs)-based application in the cloud that will enable secure and private processing of massive amounts of data produced by IoT devices;
- strengthening the security of traditional authentication services;
- devising privacy-aware, interoperable and decentralized authorization in IoT environments;
- harmonizing security and privacy mechanisms;
- identifying and tackling major security and privacy challenges for edge computing.

In order to handle and process digital evidence in real-time and share this information considering trust and privacy requirements, the Project aims to implement security intelligence, adaptive security and usability solutions intended to deal with the unified management of electronic evidence end-to-end – from the devices to the core of the network.

Finally, the project is exploring the automation of the security processes.

Concerning Risk Assessment and Management the project will not develop any new methodology, thus the annex related to the assessment is not included.

The main objectives and research goals of this project, in particular of CS4E WP3 **[102]**, are reported below:

- **Privacy-preservation, TEE and IoT-Edge security**
    - Identity management and authentication;

- Security & privacy In Edge Computing;
- Reduce the system attack surface;
- Security based on (TEE);
- IoT Privacy Preserving Platform;
- Security & Privacy by Design;
- AAA in Blockchain – IoT;
- Privacy-Preserving critical data processing.

- **Software Development Lifecycle (SDL)**

  - Challenges, requirements and approaches in all stages of the lifecycle of software;
  - Secure-by-design and proactive methodologies;
  - Automated tools reduce security vulnerabilities and risks;
  - Certification of security products to cope with the dynamicity of security;
  - Software supply chain analysis.

- **Security Intelligence**

  - Mechanisms to share digital evidence;
  - Threat Intelligence Information Services,
  - Interoperability in privacy, requirements and regulations;
  - Threat detection and security analytics;
  - Security intelligence in defensive systems.

- **Adaptive Security**

  - Security modelling of dynamic systems (representation of assets, security requirements and threats);
  - Security situation computation, cybersecurity awareness;
  - Risk Assessment;
  - Explanations (assurances) about security controls adoption.

- **Usable Security**

  - Usability requirements in security design;
  - Assessing the effectiveness factor of usability;
  - Behavioural-based user authentication mechanisms;
  - Usable security controls;
  - Visualisation of the system/security status;
  - Usable privacy control, user informed consent.

- **Regulatory Management**

  - GDPR-compliant user experience;
  - Interoperability of identity technologies (e.g. eIDAS, GDPR, ePrivacy, PSD2);
  - Processing of personal data in cross-border and cross-sector dimensions;
  - Compliance of personal data processing;
  - Compliance of proposed Privacy by Design and Privacy by Default SDL.

Concerning the RA and RM activities, the tools adopted are enlisted and reported in the following sections as described in deliverable D3.1 Common Framework Handbook 1 - CyberSec4Europe **[102]**:

BadGraph

Capability: Identify.

Category: Risk Assessment.

Description: A tool for the quantitative analysis of probabilistic attack scenarios based on attack-defence trees.

BowTiePlus

Capability: Identify.

Category: Risk Management Strategy.

Description: Web-based RM tool for identifying preventive and reactive barriers to causes and consequences of unwanted incidents.

CORAS

Capability: Identify.

Category: Risk Management Strategy.

Description: A tool-supported risk management framework.

HERMES

Capability: Protect: develop and implement appropriate safeguards to ensure delivery of critical services.

Category: Information Protection Processes and Procedures.

Description: Fault-Injection for distributed (secure) systems.

OFMC/AIF

Capability: Protect.

Category: Information Protection Processes and Procedures.

Description: OFMC/AIF is a tool suite for automated security verification of protocols.

PLEAK

Capability: Identify.

Category: Business Environment, Risk Assessment.

Description: Analysis tool for the privacy audit of an existing system and the design of new privacy aware systems.

SEMCO

Capability: Protect.

Category: Information Protection Processes and Procedures.

Description: A methodological tool-support for engineering secure systems with patterns and models.

SOBEK

Capability: Protect: develop and implement appropriate safeguards to ensure delivery of critical services.

Category: Protective Technology.

Description: Introduction of introspection within the Android apps, via code injection using Aspect Oriented Programming (AOP), to transparently collect metering data that can be used to notify the user or/and sink into a secure backend (for enterprise solutions).

SYSVER

Capability: Protect.

Category: Identity Management & Access Control.

Description: The tool supports security administrators of large distributed systems in the verification of correct implementation of the security policies in the actual system. When conflicts are detected, the tool leverages the detailed analysis results to investigate possible changes to apply in the system to correct the anomalies (conflict resolution).

VEREFOO

Capability: Protect.

Category: Protective Technology.

Description: Automated refinement of network security requirements (security policies) into virtual security function configurations (e.g. firewall rules) with formal correctness guarantee.

IDMP

Capability: Protect.

Category: Identity Management & Access Control.

Description: HCI pattern for privacy-preserving identity management'.

4.3 EU Funded Projects

4.3.1 CYSM

CYSM project aims to develop an integrated security management system (for port operators) specifically oriented to port security and to the related risk assessment and management processes to address the security and safety requirements of the commercial ports' Critical Information Infrastructures (CII). The integrated system permits to identify, assess and treat security and safety problems in an efficient, harmonized and unified manner. In fact, the developed system enables asset modelling, risk analysis, anticipation/management of attacks, as well as stakeholders' collaboration.

CYSM Risk Assessment Methodology is aimed to:

- cover the security and safety requirements for commercial ports,
- assess both physical and cyber facilities required for the robust and uninterruptible operation of ports.

It supervises and manages security also for physical facilities such as buildings, platforms, gates, marinas, data centres, platform cyber facilities such as networks, equipment, satellites, servers, relay stations, tributary stations, information, etc.

CYSM Risk Assessment Methodology satisfies the following requirements:

- Compatibility with standards (e.g. ISO27001, ISPS code[30], etc.);
- Implements multi-scope risk analysis providing clear questionnaires and accurate results;
- Analyses sectoral, interconnected and interdependent threats;
- Ensures collaboration among port users through good and clear functional requirement, precise and measurable;
- Being easy to implement and well documented: all steps of the methodology are documented in clear format and outcomes for each step;
- Responsibility centric: Methodology has to be oriented to users' role.

The CYSM Methodology involves six phases:

- Facility Cartography;

[30]The International Ship and Port Facility Security (ISPS) Code is an amendment to the Safety of Life at Sea (SOLAS) Convention (1974/1988) on minimum security arrangements for ships, ports and government agencies. Having come into force in 2004, it prescribes responsibilities to governments, shipping companies, shipboard personnel, and port/facility personnel to "detect security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade

- Impact Assessment;
- Threat Analysis;
- Vulnerability Analysis;
- Risk Determination;
- Risk Mitigation.

The first phase comprises activities like the identification of the organizational structure, the classification of the employees (e.g. based on their roles or positions), the definition of the physical and ICT facilities to monitor and evaluate for the port (namely, the Risk Assessment boundary), the identification and categorization of the assets as well as of the correlations between elements (e.g. network and software, hardware and software/information, …), and finally the identification of controls (to be or already) applied in each asset.

Assets are evaluated according to seven impact criteria keeping into consideration: Financial Losses (direct, indirect and long-term financial consequences), Legal Consequences (privacy issues, sensitive and personal data, commercial data, competition-related issues, private and non-disclosure agreements issues, IPR and copyright issues, etc), reputation consequences like confidentiality issues regarding organizations, their suppliers or shareholders.

An important role lays the policy for the final estimation of impact for a given asset. Through a *personal impact assessment*, each user evaluates the assets based on the impact in case a given incident occurs. The impact value is set to the maximum value in the several scenarios which might involve the asset. This is done several times since impacts for an asset are evaluated depending on a set of criteria. The personal impact value of a specific asset for each participant is the maximum value of all criteria for the specific asset.

Then the *overall impacts assessment* takes place. The impact value of every asset for each department is calculated. The *final impact of a specific asset* is the maximum value of all departments

Starting from data analysis, e.g. the data produced by intelligence agencies, and sector specific scenarios an estimation of the likelihood of occurrence of each threat is provided, through scaling, identification and levelling. For each asset category, a list of threats is formulated taking into account both experience from incidents and past threat assessments and threat catalogues available from industry/standardization bodies, national governments, legal bodies etc. The identified threats are grouped into various categories (e.g. Physical Threats, Environmental ones, etc). Among them only three match the area of interest of ECHO:

- Technological Threats, related to Hardware Malfunctioning;
- Human Threats, e.g. Network Attacks, Virus Attack, Unauthorized Access;
- Lesion Data, e.g. Malicious Data Corruption or Unauthorized Access To Data.

Similarly, to asset assessment, the threat assessment is made following a *personal evaluation* where each user evaluates the threats of each asset. This step is followed by the *Overall Threat Assessment* through which the likelihood of occurrence of each threat to a specific asset derived from each department is calculated. The *Final Likelihood of occurrence* of each threat to a specific asset is the maximum value of all departments.

As far as concerns, the Vulnerability Analysis (phase 4), an estimation of the level of exploitation of a vulnerability from a threat taking into account the applied controls is produced by exploiting the outcomes of the usual scaling and identification activities. The identification of the vulnerabilities associated with the defined threats, obtaining a list of vulnerabilities, is formulated taking into account factors such as:

- Internal experience;
- Previous audit controls;
- Penetration tests;

- Vulnerabilities catalogues available from industry/standardization bodies, national governments, legal bodies.

Also for this phase, a *Personal Vulnerability Assessment* takes place. Each user evaluates the vulnerabilities of each asset according to the correlated threats. Then the *Overall Vulnerability Assessment* calculates the level of exploitation of a vulnerability from a threat derived from each department. Then, the Final level of exploitation of a vulnerability from a threat derived from all departments is calculated.

The Risk Determination (phase 5) provides the Calculation of the Risk Value (R) of each asset starting from three inputs:

- Likelihood of Threat exploitation
- Magnitude of Impact
- Adequacy of Current or Planned Controls

Specifically, this phase leads to two important outcomes: the *Risk Value Calculation* and *Risk Level Estimation*.

Since a list of countermeasures is required to be implemented in order to minimize the identified risks, Risk Mitigation (phase 6), starting from the list of countermeasures and controls currently available produces a selection of countermeasures and the list of recommended countermeasures for mitigation activities.

The methodology we summarized above shows several similarities with the ECHO approach for Risk Management. Some elements among the ones depicted above are extremely valuable and the ingestion of a similar technical solution in E-MAF will be evaluated. Please refer to Section 5 for a deeper level of detail.

Once the evaluation phase is completed, the Security Officer produces and review the results of the risk assessment process. He/She selects the interesting assessments and calculates the potential risk associated, taking into consideration also the answers of participants to the evaluation itself. The produced results then lead to the prioritization of countermeasures to be adopted to obtain an effective and efficient mitigation plan. Through Policy Reporting features included in CYSM system, he/she can also formulate the regulatory security/safety policies as foreseen by ISO 27001**[15]** and ISPS.

The CYSM Risk Assessment Toolkit is a software system implementing functionalities described above through a set of interconnected and integrated subsystems:

- The *Web Interactive Component*, a graphic environment where all needed applications can run in a consistently and systematic integrated way. The user-friendly HMI allows the user to inspect and retrieve information and content related to Risk Assessment (e.g. requirement, rules, recommendation, etc.); external applications can be integrated as information sources through RSS feed or subset of functionality. Implementation of Web Interactive Component exploit the power of Java Portlets and Portlet Containers assuring portability and compatibility through JSR-168 and JSR-286 standards, by which it is possible to state that a compliant portlet can be installed on (namely, deployed to) any portlet container. In order to support development of portlets, CYSM provides a Plugins Software Development Kit (SDK).
- The *Semantic Modelling Component*, integrating a collection of ontologies and taxonomies to model: the security and safety posture of the ports; the employees with respect to their behaviour, interaction with infrastructure, role and responsibilities as well as background knowledge and awareness; cyber and physical issues; etc. It allows the administrator to define content categories, and users to find content through their tree-like structure. Categories define how the content is organized from the port owner's point of view.

- The *Execution Engine Component*, integrating an automated workflow tool transparently processing requests defined by the CYSM Risk Management methodology. CYSM workflows are "step" procedures dedicated to produce, modify and publish web content.
- The *Workflow Engine*, allowing privileged users to define new workflows, deploy and manage them on the Portal. The key parts in a given workflows are:

    - Asset, a piece of content to be reviewed and/or approved within the workflow;
    - State, a single stage for the workflow (created, rejected, approved, …);
    - Transition occurring between states;
    - Task, steps in workflow where an action must be performed by the user.

- The *Interaction Component*, enabling standardization of information encapsulation; with the form of an enterprise service bus, it fosters communication among application, acting as an event-driven standard-based multi-purpose broker; with this component it is possible to manipulate, filter, send, … SOAP messages, binary and XML files, HTTP and HTTPS requests and responses, etc.
- The *Advanced Security Intelligence Engine* analysing activities, by providing a set of technologies to describe, enumerate, quantify, encapsulate data (e.g. risks, threats, vulnerabilities, countermeasures and their prioritization, etc.).

The CYSM system adopts a simplified and optimized methodology to risk assessment clearly competing against the traditional approach. The automated graphic approach and the several self-risk assessment processes are coupled with easy-to-use self-driven tools enabling collaboration among users and zeroing the need of external support. It can be considered an excellent starting point for the future ICT security management tools.

The following figure shows the high-level architecture of CYSM system.

Figure 13: The CYSM system architecture [100].

4.3.2 MEDUSA

Defining organisation-oriented Risk Assessment methodologies without considering the effects of multi-/cross-sectoral and cross-border dependencies among entities is quite common. For this reason the usual approaches focus on risks limited to organisation failing to capture the complexity of security within Supply Chain Services (SCSs) and entities involved into them. So, the need to extend and validate current framework and methodologies against the challenge of assessing risk in SCSs is still big and should start from modelling cascading effects, as ECHO WP2 has been doing since the beginning of the project.

Most of the standards, methodologies and framework assessed in the previous sections provide general considerations, guidelines, and/or specific guidelines for cyber risk in Critical Infrastructures or in IT. They are quite always sector-specific and do not provide quite often specific methodologies for SCSs RA. Moreover, since SCSs are strictly bound to the business context, dedicated RM methods and methodologies are usually quantitative and generally look to impact and financial cost. ISO 28001 is a Supply Chain security management standard. Applicable to all sizes of organisations, it enlists requirements for SC management systems taking into consideration, among others, also information management and financing issues. It also defines the certification requirements and the self-declaration of conformance. By design, it defines a generic methodology at the entity level, without going deeper to assets definition and guidelines to verticalize it. Also, NIST provided its own vision of securing SCSs by defining (in NIST IR 7622) a set of methods and practices for SC assurance representing a SC security management system for federal information systems. Unfortunately, no methodology was defined by NIST.

The EC project MEDUSA (Multi-ordEr Dependency approaches for managing cascading effects in ports' global supply chain and their integration in risk Assessment frameworks) developed, under the CIPS program, developed an innovative methodology for SCSs Risk Assessment to be coupled with a security management tool also provided by the project. Despite the proliferation and advancement of risk assessment methodologies for Critical Information Infrastructures (CIIs) most risk assessment frameworks do not adequately address the various cascading effects that are associated with security incidents occurring from interacting entities. This gap is very critical in the case of ports' security, given that ports are CIIs characterized by significant interdependencies at multiple levels (infrastructural, national/intra-sectoral). The main goal of the MEDUSA project is to alleviate the above-mentioned gap, through introducing, specifying and validating multi-dependency approaches to risk assessment, while also using them in the scope of risks assessment frameworks for ports' CIIs. MEDUSA will therefore open new horizons in the area of port security, through producing and sharing knowledge associated with the identification and assessment of cascading effects in the global ports' supply chain, with a view to predicting potential problems but also to minimize the consequences of diverge security incidents.

Moreover, MEDUSA (as CYSM) promotes collaboration between business partners. It puts in place an *Holistic View* of Supply Chain aimed to identify global threats including cascading ones within it. The organisation-centric perspective adopted by other methodologies does not allow to do this.

The MEDUSA Risk Assessment system **[68] [69] [70]** simultaneously operates on two factors:

- improving capability and awareness among the business partners;
- enabling coordination in identifying and treating their risks.

So, MEDUSA system simultaneously:

- fosters and promotes partners' interaction in the SCSs while threat identification and analysis run;
- supports security risks assessment (even partial or overall) and orchestrate the security controls selection process in a way they fit all partners' needs;

- assesses risk of cascading threat scenarios by taking into consideration all relations of a potential source of a threat together with the (weighted) role (business) of partners.
- enables SC participants to fine-tune cybersecurity policies depending on their (business) role in the SCS.

There ISO standards that are related to the security management of the supply chains: ISO 28000:2007 **[63]**, ISO 28001:2007 **[64]**, ISO/IEC 27005:2008 **[65]**, ISO/IEC 27001:2005 **[66]**, 27002:2005 **[67]**. The ISO standards define a minimal framework describing requirements, for the RA process itself, for the identification of the threats and vulnerabilities allowing to estimate the risks, their level and then to be in a position to define an effective treatment plan.

ISO standards do not define methods for Risk Management or other important aspects such as the collaboration among the users. In this scenario Medusa Project developed a novel SC risk assessment methodology that complies with ISO28001, ISO27001 and ISPS.

MEDUSA system comprises 4 logic and conceptual layers representing the pillars for the design and implementation of the ICT tools which support modelling and visualization of security risks and their interdependences:

- System Users (Layer 1), enlisting the following user groups (having different access rights to tools):
    - Security Manager: in charge of system initialization with globally available information including the system vocabularies (closed lists) to be used by other layers;
    - SCS Security Office: responsible for the initiation of RA and specification of the SCSs, of the business partners, and of their processes;
    - Business Partner Representative representing actors taking part to SCSs evaluation process (customs, shipping companies, etc.), providing information on threats, vulnerabilities and controls.
- Information Assets (Layer 2), where user groups provide initial information on threats and threat scenarios, vulnerabilities, security controls, dependencies, consequences, etc including scales for them (where necessary, e.g. for threats, etc.)
- Components (Layer 3) accessing, managing and processing assets, such as.
    - Administration module: devoted to customize parameters, elements, and features (e.g., threats, vulnerabilities, controls) required for RA.
    - Initialization module, initializing RA and defining SCS to be examined.
    - Risk Evaluation module, assessing the risk level of business partners for the threat scenarios.
    - Risk Management module, enabling the review of the RA results and the calculation of the cumulative cascading dependency risk values for the threat scenarios.

Technological Infrastructure (Layer 4), comprising all subsystems, modules and services building the MEDUSA system.

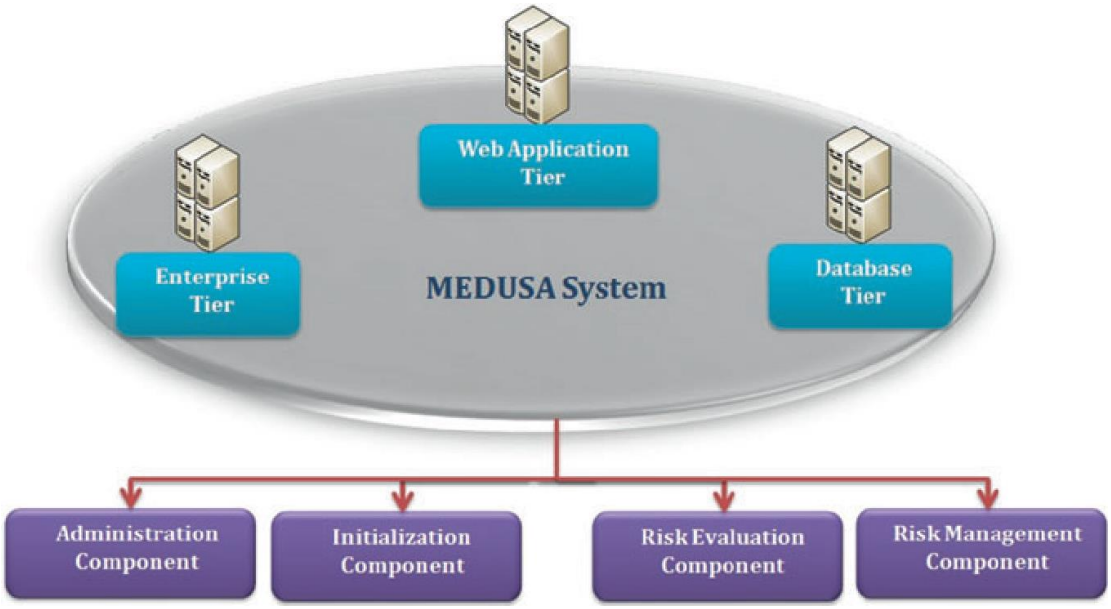

Figure 14: The MEDUSA architecture [100].

The MEDUSA system, as depicted in the Figure above, deploys a 3-tier architecture, composed by:

- the Web Interactive tier, providing graphical user interfaces representing the MEDUSA information and content as well as simple and intuitive access to the functionalities, in a very tight interconnection with Enterprise tier;
- the Enterprise (Application) tier, containing the business logic, and
- the Database tier, integrating the main Database and all information and contents related to risks.

The Enterprise Tier can be considered as the most critical one since it hosts a range of mechanisms, techniques, and components such as:

- The Risks, Assets, and Dependencies Modellers which:
  - integrates all the semantics (e.g. ontologies, taxonomies) representing dependencies and the other several possible relationships (e.g. interactions, interrelations, etc.) among issues, factors, indicators in order to model and run RM scenarios;
  - implements the algorithms to identify and model the multi-order dependencies inside and among business partners (maritime organisations and critical information infrastructure, in multi-sector and cross-border scenarios.
- The Impact Analysis and Visualization Tools where:
  - mechanisms, procedures, and interfaces to diagnose SCS threat scenarios and security events take place. These tools provide the necessary elements (methods, algorithms, standards, and technologies) for enumerating, describing, measuring/quantifying, and encapsulating data required by an integrated risk analysis process. In particular features for threats and risk identification, impact and threats evaluation, etc. are included.
  - a fast visual reference to risk values is provided: as an example an approach to visually browse risk analysis and thread identification outcomes.
- The Simulation Environment, responsible to design and execute risks and threats simulations in order to facilitate analysis, assessment, and mitigation of various threats and risks in SCSs; the component also provides access to simulation results for further analysis and use in mitigation plans.

- As concerns the Risk Assessment Methodology for Supply Chains, MEDUSA system provides to the supply chain operators advanced guidance on how to assess and organize their security issues in SCSs. The MEDUSA system encompasses and executes a risk assessment and evaluation process implementing 10 steps:

- Step 1: *SCS Risk Assessments (SCS RAs) Initiation and Specification* where the specification of the boundaries of the SCS Risk Assessment takes place; the SCS under examination, the partners involved, and the acceptable risk thresholds are defined.
- Step 2: *SCS Initiation and Specification* defining actors and dependencies within a SCS.
- Step 3: *Threat Scenario Identification* for the SCS under examination.
- Step 4: *Threat Analysis* providing the assessment of each relevant threat scenario in SCSs by estimating its probability of occurrence.
- Step 5: *Security Controls Declaration/Vulnerability Assessment* where the specification of the implementation level of the security controls for the threats related to SCS threat and the corresponding vulnerability values are set.
- Step 6: Consequence Assessment leading to evaluation of the worst-case consequences for a given partner, if a threat scenario is realized in any node within the SC.
- Step 7: Individual Risk Computation determining the expected risk levels for all partners and threat scenarios in a SCS.
- Step 8: Overall Risk Computation of the overall risk levels of the SCS for all threat scenarios.
- Step 9: Cascading Dependency Risk identifying all possible dependency chains and corresponding cascading dependency risk values.
- Step 10: Individual Risk Simulation to determine the security controls to deploy to satisfy the desired risk level (acceptable threshold).

4.3.3 MITIGATE

MITIGATE **[60] [61] [62]** addressed the task to contribute to create an effective protection system for ICT-based ports SCs. As discussed in the previous sections, the threats arise from the ICT interconnections and interdependencies between a large set of organisations cooperating in a maritime SC, such as port authorities, ministries, maritime companies, ship industry, customs agencies, maritime/insurance companies other transport Critical Information Infrastructures (like for airports, transport/energy/telecomm networks). In order to do this the ICT maritime SC risks are threaten as a dynamic experimental environment to be optimized through the involvement all relevant maritime actor and simulations. That way, MITIGATE facilitates processes like identification, analysis, assessment, and mitigation of organization-wise and interdependent cyber threats, vulnerabilities, and risks.

As described in the previous sections, cyber risk analysis and evaluation generally lay on a straightforward approach combining parameters and features such as the likelihood of events, their consequences, the exploitation level of a given vulnerability, etc. Mitigate provides rational decision making capabilities to the usual assessment approach in order to enhance RA through Rational Analysis. The latter is performed through information obtained from online repositories. Finally, we can state that MITIGATE objective is to promote a (more) rigorous, rational approach based on high-quality information which are either produced by simulation experiments or available online (e.g. NIST Repositories). In its underlying philosophy, the cyber issues is an inherently rational process relying on well-defined and widely acceptable security-related data; it is neither objective nor neutral and not based only upon individuals personal experience and judgment.

MITIGATE radically moves ahead in RM for the maritime domain by enabling a collaborative evidence-driven SC RA approach. This is reached by integrating an effective, collaborative, standards-based RM system for port's CIIs, considering all threats arising from the SC, including threats associated with interdependencies among critical information infrastructures and respective cascading effects.

As stated before, the MITIGATE system also enables security management based on the production of shared knowledge and also introduces an integrated and cost-effective way to identify, assess and evaluate cascading effect in ports SC, by fostering predictive capabilities as well as the ones to mitigate consequences of threats (cascading effects included). This goal can be reached through the melting of mathematical instruments and technologies as follows:

- techniques for reasoning, data mining, crowd-sourcing, and Big Data analytics: they leverage plenty of data sources and data types, empowering the system through the efficient handling of data even incomplete or uncertain;
- new mathematical methodologies and approaches to predict/analyse threats (e.g. patterns); and
- innovative visualization/simulation solutions and techniques to improve automatic data analysis.

They make collaboration between the various maritime agents easier and effective, and also enable them to:

- Identify and model fundamental objects for risk management in SCs like assets, risks, interactions, dependencies, etc.
- Analyse threats, vulnerabilities, and countermeasures from online sources and repositories.
- Identify, evaluate, and classify ICT-based risks and facilitate risk resolution.
- Design, execute and analyse simulation experiments in the SCs. It allows to identify attack paths consisting of vulnerability chains. Simulation results are to be used to formulate mitigation plans.
- Feed archives of open and distributed data.

To this end, a specific set of services need to be developed and integrated in order to enable cyber-attacks simulation and visualization, to set up the collaborative RA, to early identity potential attacks, etc., which are depicted in the following high-level architecture (see Figure **15**).

The following eight components comprise the MITIGATE system:

- The **Asset Modelling & Visualization** component allows partners' assets and (cyber) relationships declarations since a valid asset cartography (represented by a graph) is the first step towards a collaborative RA. The cartography will be automatically bound to known vulnerabilities and attack-types which are relevant to the assets.

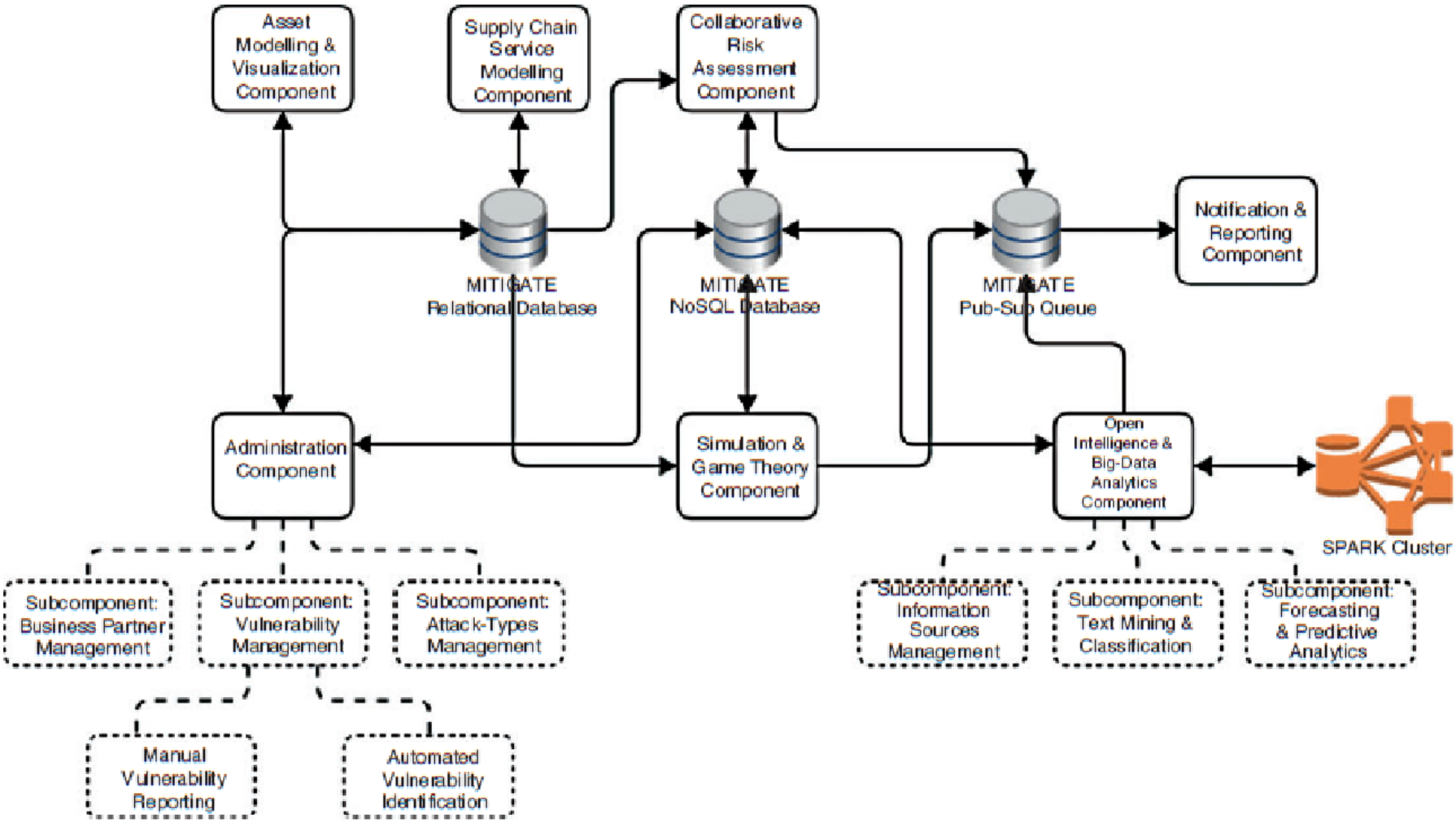

Figure 15: MITIGATE general architecture [100].

- The **Supply Chain Service Modelling** component modelling the SCSs, as a set of business processes. Since each business partner has a predefined role in SCSs involving specific cyber assets, this component relies on the output of the Asset Modelling component, playing a significant role during the calculation of risks.
- The **Simulation & Game Theory** component simultaneously responsible for both the discovery of attack paths (given a specific tuple: asset cartography and SCSs) and the proposal of the best defensive strategy, based on principles from game theory.
- The **Collaborative Risk Assessment** component is responsible to provide guidance for the conduction of a RA for a SCS and is based on a Supply Chain Risk Assessment (SCRA) methodology, a detailed multistep process **[60]**, introduced by MITIGATE in order to calculate the SCS-related risks.
- The **Open Intelligence and Big-Data Analytics** component providing near real-time notifications on potential vulnerabilities related to elements in the organisation's assets cartography to be generated based on the text-processing of open sources.
- The **Notification and Reporting** component in charge of notifications to business partners regarding any type of messages placed in the asynchronous pub/sub queue.
- The **Administration** component is responsible for the definition and management of the various "enumerations" used by component, like vulnerabilities, attack-types, and business partners.
- The **Access Control and Privacy** component implements the appropriate horizontal authentication, authorization, and encryption schemes required by the other components.

Two supportive architecture is complemented by:

- a pub/sub system, a message queue aimed to decouple the communication as well as eliminate any blocking communication that may be required, a prerequisite for a scalable system;
- a persistency layer consisting of:

    - one relational database (Mysql), for fully structured data that change rarely (e.g., credentials, business partners)
    - one NoSQL (MongoDB) storing semi-structured data that change frequently (e.g., vulnerability reports).

MITIGATE Security Assessment Services comprises the following functionalities:

- The Risk Assessment and the Visualization functionalities, to quantify the risks that derive from the various vulnerabilities associated to specific assets that participate in a SCS, according to three different qualitative risk levels:

    - The individual risk referring to the impact of potential exploitation of vulnerabilities at the asset-individual level.
    - The cumulative risk quantifies the effect of attacks at a vulnerability chain level.
    - The propagated risk quantifies the effect of an exploitation towards the adjacent network.

    The latter two take into consideration interconnections between assets.

- The Risk Management functionalities aim the generation of an optimal mitigation strategy given a specific SCS through a game-theoretic approach; it starts from considering the several offensive and defensive strategies related to a given set of assets.
- The Simulation functionalities facilitate the design, execution, and analysis of risk and threats simulation experiments.
- The open intelligence functionalities provide dynamically aggregated and indexed data relating to cyber-security from various web sources and social media.

- The prediction and forecasting functionalities provide automated discovery of potential vulnerabilities and pending attacks in the maritime SC.

The MITIGATE methodology is developed according to several objectives that take in accounts: 1) the identification of all cyber threats within a SCS; 2) evaluation of the individual, cumulative and propagated vulnerabilities; 3) forecasting of all possible attacks/threats paths and patterns within the SC cyber system by considering the various attackers' profiles, the existing vulnerabilities and the cyber assets' dependencies; 4) the assessment of the possible impacts, identification of priorities for cyber risks of the SC cyber assets; 5) elaboration of a proper mitigation strategy.

The following assumptions are made:

- the business processes of the SCS are linear (not cyclic) and thus the cyber assets are interconnected in one-way linear paths (thus cyclic attacks are not possible);
- the interconnected cyber assets are used only for the provision/delivery of the SCS and isolated from the partners' individual ICT infrastructure.

The MITIGATE SCRA methodology is triggered by any specific SCS and follows the standard RA six main blocks:

- Boundary Setting,
- Threat Analysis,
- Vulnerability Analysis,
- Impact Analysis,
- Risk Estimation,
- Mitigation Strategy.

Table **25**, extracted from **[60]**, shows main steps and sub steps of the MITIGATE SCRA methodology which are described in details in the following Sections.

Boundary setting	SCS cyber threat analysis	SCS vulnerability analysis	SCS impact analysis	SCS Risk estimation	Mitigation
S1.1: Goal and Objectives of the SCS	S2.1: SCS cyber threats' identification	S3.1: Identification of Confirmed Individual Vulnerabilities	S4.1: Individual Asset Impact Assessment	S5.1: Individual Asset Risk Assessment	S6: Risk Mitigation
S1.2: SCS business partners and participants identification	S2.2: SCS threat assessment	S3.2: Identification of Potential / Unknown (zero-day) Vulnerabilities	S4.2: Cumulative Impact Assessment	S5.2: Commutative Risk Assessment	
S1.3: SCS Modelling		S3.3: Individual Vulnerability Assessment	S4.3: Propagated Impact Assessment	S5.3: Propagated Risk Assessment	
		S3.4: Cumulative Vulnerability Assessment			
		S3.5: Propagated Vulnerability			

Table 25: SCRA main blocks and sub-steps.

Step 1: Boundary Setting

The SCS under examination is decomposed (Step 1.1) and all partners identified (1.2). Then is the identification and modelling of the main cyber or/and physical (controlled/monitored by a cyber system) processes comprising the SCS (1.3) where all cyber assets (e.g. Application Server, Desktop Application, Enterprise/Web Application, Mobile Application, Web Server, Operating System, Web Browser, etc.) required for the SCS and the corresponding SCSBPs are identified and reported; also the interdependencies modelling takes place in 1.3 (e.g. hosting, exchange data/information, storing, controlling, processing, accessing, installing, trusted, etc.).

Step 2: SCS Cyber Threat Analysis

As reported in **[60]**:'*All threats for the SCS cyber assets reported Step 1 are identified (Step 2.1) and evaluated (Step 2.2) in terms of their likelihood of occurrence. The methodology uses a five-tier scale: Very Low = 20%, Low = 40%, Medium = 60%, High = 80%, Very High = 100%. Evaluation process is based upon the three criteria enlisted below:*

- *the expected frequency of appearance (based on the history of previous incidents);*
- *the participants' intuition and knowledge; and*
- *the information retrieved from social media and existing repositories to be used in order to gather peripheral information and draw conclusions.*

The typical examples assumes that for a threat T, a participant believes (based upon his expertise) that the probability of occurrence of T to asset A is about 50% (threat level "Medium"). From information available on the social media, he also concludes that the probability is about 70%. In addition to this, T has a history of one incident in the last 12 months (threat level "High"). Thus, the Threat level assigned is High = 80%.

Step 3: SCS Vulnerability Analysis

The vulnerability analysis aims to identify, quantify, and prioritize the vulnerabilities that exist in the cyber assets of a given SCS. Two categories of vulnerabilities exist:

- confirmed vulnerabilities (3.1) already reported and retrievable from online databases;
- potential/unknown (zero-day) vulnerabilities (3.2) existing but non-disclosed yet.

Both categories will be accompanied with specific attributes (Access vector, Access complexity, Authentication, Threat and Vulnerability Categories, Exploitable). The severity of all vulnerabilities is then estimated (3.3) by:

- using the CVSS metrics (the Access Vector AV, the Access Complexity AC and the Authentication Auth) retrieved from the online databases for Individual levels (qualitative mapping from the CVSS metrics onto five-tier scale, ranging from "Very Low" VL to "Very High" VH); e.g., for a vulnerability V with an Access vector "Adjacent", an Access Complexity "Medium" and an Authentication "Single", the resulting Individual Vulnerability Level is "Medium".
- estimating the probability that an attacker successfully reaches and exploits each of the vulnerabilities in a given vulnerability chain (3.4) in a consequential multi-step attack as Cumulative Vulnerability Level CVL;
- evaluating the weakness of the vulnerability chains to be exploited due to exposure of a specific vulnerability as Propagated Vulnerability Level PVL (3.5);

Step 4: SCS Impact Analysis

As usual, Impact analysis refers to the assessment of the expected consequence if a malicious action is realized, like a successful exploitation of vulnerabilities to an asset. Again, Individual Impact level is calculated (4.1) for each vulnerability on the asset following the CVSS metrics available; in particular, a qualitative mapping is defined from the three security criteria (Confidentiality C, Integrity I, and Availability A) in the CVSS Impact metric onto a five-tier scale (from “Very Low” VL to “Very High” VH). Similarly to Step 3 we have:

- the Cumulative Impact Level CIL (4.2), that is the impact occurring after a specific asset/vulnerability combination has been exploited by an attacker;
- the Propagated Impact Level PIL (4.3), estimating the overall impact occurring when an attacker exploits a specific asset/vulnerability combination and further moves on into the network.

Step 5: SCS Risk Estimation

Risk estimations will be performed in this step by calculating the following levels:

- The Individual Risk (5.1) expressing how dangerous all threats are to a specific asset.
- The Commutative risk (5.2) referring to the risk of a threat s occurring due to a vulnerability z that exists in the asset given that all independent vulnerability chains starting from other assets have been exploited.
- The Propagated risk (Step 5.3) which refers to the risk of a threat s occurring due to a vulnerability v that exists in an asset given that v may cause the exploitation of various vulnerability chains.

Considerations on MITIGATE Methodology

Although we can find a plenty of cyber security and Supply Chain Security standards and conventions (see ISO27001**[15]**, 27005**[16]**, NIST CS Framework**[27]**, ISO28000, ISO28001, ISPS), none among them designs or implements a Supply Chain Risk Assessment methodology following those standards. MITIGATE provides an implementation that business partners can finally follow to estimate and govern risks and cascading effects. MITIGATE main characteristics are that:

- It provides a holistic view of the ICT infrastructure required for the provision of the supported SCS in order to identify and evaluate all SC cyber threats and risks within the SC.
- It aims to promote collaboration between business partners.
- It is Business-centric due to the importance of the role of business partners in the provision of the SCS and targeted results of RA.
- It is compliant with standards as ISO/IEC 27005, 27001, 27002, ISO 28000, 28001 and IMO ISPS.
- It adopts a sequential step-by-step approach with clear inputs and outputs so it can be easily implemented in an ICT tool.
- It is sector-independent, auditable (result are comparable with other RA methodologies), privacy aware.

4.3.4 Other Projects from Cyberwatching Radar

Here follows the assessment of a selection of projects from Cyberwatching Radar[31] part of the European observatory of research and innovation in the aim of cybersecurity and privacy providing access to project information.

AEGIS

The AEGIS Project has been shaped to reinforce the dialogues between Europe and the United States. The focus of the project is the exchange of views, policies and best practices to stimulate cooperation around cybersecurity and privacy R&I proposing a multi-stakeholder approach to engage relevant communities from both sides of the Atlantic. Thus, a Cybersecurity Reflection Group (CRG), a multi-stakeholder collaboration platform was created to set up an effective international collaboration platform. This platform is a tool to stimulate the discussion on progress and priorities, the setup of cybersecurity and international privacy research agendas, harmonization and sharing of policies, best practices, standards, knowledge and experience. The CRG and its Working Groups on Cybersecurity and Privacy R&I and Policies the project addresses critical issues for international cooperation in cybersecurity and privacy. The role of Working Groups in the AEGIS project is strategic because it brings together high-level experts from both sides of the Atlantic to address specific issues such as the identification of common approaches in addressing cybersecurity and privacy, challenges from an R&I as well as a governance and institutional perspective. By using this cooperation approach the project has developed a series of high-impact publications that provide recommendations to increase transatlantic cooperation. Here follows a list of official documents of interest:

- White Paper on Cybersecurity Policy
- Cybersecurity and Privacy Landscape in Europe
- Cybersecurity and Privacy Landscape in the US
- Report on Cybersecurity and Privacy R&I Priorities for EU-US Cooperation
- Policy Brief on Cybersecurity Policy
- Policy Brief on Research and Innovation in Cybersecurity
- White Paper on Research and Innovation in Cybersecurity
- Actions for EU-US Cyber Dialogue
- Guidelines for Innovation Partnerships in Cybersecurity and Privacy for EU-US Collaboration
- Benchmarking Report on the Cybersecurity and Privacy Landscape in the EU and the US

CANVAS

The project idea of CANVAS was developed according to the detected necessity in cybersecurity field of creating a community-building to unify different perspective that technology development in cybersecurity should incorporate European values and fundamental rights. In fact, for several years technology developers as well as legal and philosophical scholars and empirical researchers have dealt with cybersecurity issues from very specific angles. Thus, the major aims of the project it to establish an alliance for value-driven cybersecurity. CANVAS Consortium includes a wide number of partners having different scientific traditions – ethical, legal, empirical and technological – with unique competences and broad networks. The consortium will consider the following domains of application with unique value-profiles and complementing cybersecurity exigencies: the health system, business/finance, and law enforcement/national security. The expected results

[31] https://www.cyberwatching.eu

of the CANVAS include to structure existing knowledge, the creation of a network for exchanging knowledge and generating insights across domains, and the dissemination the insights gained.

The dissemination will be done through the development of a reference curriculum for value-driven cybersecurity (focusing on industry-training), briefing packages for policy stakeholders, and a Massive Open Online Course (MOOC) on value-driven cybersecurity.

Some interesting outcome related to CANVAS project are listed below:

- it brought together stakeholders from key areas of the European Digital Agenda for discussing challenges and solutions when aligning cybersecurity with ethics identifying several gaps with respect to ethical research and European cybersecurity regulation that need to be addressed;
- it supported fourteen workshops in which it has unified several dozen experts of cybersecurity with a particular focus on non-technical aspects providing a resource for future projects that want to focus on responsible research and innovation in cybersecurity;
- it developed teaching material providing the foundation that the future generation of cybersecurity experts obtains basic insights and knowledge on how to tackle ethical and legal dilemmas in cybersecurity.

The results of CANVAS focus on three target groups that are positioned in a critical position for promoting a secure and innovative ecosystem through fostering the creation of secure technologies in line with European values. For each of these groups a Deliverable document has been produced. Beside those three major output deliverables, CANVAS is producing White Papers and publications for advancing value-sensitive cybersecurity.

Being the project mainly oriented to community building, no Annex discussing specific methodologies introduced by CANVAS will be provided at the end of this document.

CertMILS

certMILS (http://www.certmils.eu/) project develops a security certification methodology for Cyber-physical systems (CPS). CPS are characterised by safety-critical nature, complexity, connectivity, and open technology. A common downside to CPS complexity and openness is a large attack surface and a high degree of dynamism that may lead to complex failures and irreparable physical damage. The legitimate fear of security or functional safety vulnerabilities in CPS results in arduous testing and certification processes. Once fielded, many CPS suffer from the motto: *never change a running system*.

The project increases the economic efficiency and European competitiveness of CPS development, while demonstrating the effectiveness of safety & security certification of composable systems. It aims to protect critical infrastructure against cyber-attacks by compositional security certification. It also delivers a certified MILS platform, for the first time in Europe. This is very similar to ECHO objectives at least for RA and Certification Scheme, also being focused on a multi-sector approach.

The project employs a *security-by-design* concept originating from the avionics industry: Multiple Independent Levels of Security (MILS), which targets controlled information flow and resource usage amongst software applications. certMILS reduces certification complexity, promotes re-use, and enables secure updates to CPS throughout its life-cycle by providing certified separation of applications, i.e. if an application within a complex CPS fails or starts acting maliciously, other applications are unaffected.

certMILS plans to reach the following objectives:

- Transfer know-how in compositional safety certification to security certification
- Make certification of composed systems affordable

- Preserve certified assurance
- Involve stakeholders in multi-sector industry domains
- Provide a certified European MILS platform
- Develop and apply compositional certification methodology on three industrial pilots
- MILS Platform Protection Profile
- Produce guidelines and templates for MILS certification

certMILS foresees to reach a major impact because of the technology-wise consortium, the high TRL, the adoption of proven MILS technology, and use of a system design approach tightly bound to both security evaluation and security certification, leading to development of early prototypes and enabling reuse of compositional certification results across national borders.

Security certification of complex systems to medium-high assurance levels is not solved today. The existing monolithic approaches cannot cope with the complexity of modern CPS. certMILS uses ISO/IEC 15408 and IEC 62443 to develop and applies a compositional security certification methodology to complex composable safety-critical systems operating in constantly evolving hostile environments. certMILS core results are standardised in a protection profile.certMILS develops three composable industrial CPS pilots (smart grid, railway, subway), certifies security of critical re-useable components, and ensures security certification for the pilots by certification labs in three EU countries with involvement of the authorities.

The certMILS project structures critical systems into partitions that run on a separation kernel (the MILS). Once a critical system is structured through a separation kernel, then this technical structuring should lend itself also to a similarly logically structured security and safety argument in certification. Similarly, the project white papers should mimic the same structure and provide a security architecture template that is to be used for the certification of that MILS system. The target audience for the white papers document is:

- Developers of systems, based on a MILS architecture, providing them a template about how to describe their MILS system.
- Security evaluators of a MILS-based system, giving hints about how the developer description can be used to argue for compliance to Common Criteria (CC) and IEC 62443.

This project is devoted to the provisioning of an innovative certification scheme and has no activity expressly focused on cyberrisk; so, even the project does worth to be mentioned, no Annex discussing specific methodologies will be provided.

COMPACT

COMPACT (COmpetitive Methods to protect local Public Administration from Cyber security Threats) will adopt an iterative development, integration, and prototyping strategy of various system components and implement them in the COMPACT platform, based on an easy-to-use interface and features of awareness raising and training, adapted to personnel with limited IT skills.

The project offers services which aim is to innovate at technological and process level the cyber security for Local Public Administrations (LPAs): at technological level it innovates real time security monitoring, security awareness training, information sharing, cyber-security gamification, risk assessment, and threat intelligence; while at process level, it adapts the Plan-Do-Check-Act cycle for LPAs to do iterative removal of security bottlenecks, conforming it with EN ISO/IEC 27001 and BS ISO/IEC 27005.

Improve the cyber security level of LPAs has become very important lately: cyber threats are, in fact, a very big risk for them. The mission of the project is to empower LPAs' cyber-resilience by effective tools and services

that COMPACT will provide, in order to remove security bottlenecks and give to the LPAs the first role in recognising cyber threats and prevent them.

Risk Assessment tool will be one of the tools and services offered by the technological platform, together with Education services, Monitoring services and Knowledge Sharing services. The Risk Assessment Tool will be tailored to LPAs context, in order to allow them to evaluate and monitor the risks and their exposure to cyber threats and to adopt preventive and reactive countermeasures.

The Risk Assessment Tool will be composed by: RATING tool for LPAs (Risk Assessment Tool for INtegrated Governance), Social Engineering (SE) Exposure Evaluation Service - TO4SEE and, Human Factor Profiling (AIT).

The RATING tool is responsible for the generation, and update, of the LPAs risk profiles, that will help them to prioritize the action they would DO to contrast basic cyber threats. The first prototype has been created in the context of the FP7 project named CYSPA3 (European Cybersecurity Protection Alliance) and it was validated for the usage in Energy, e-Government, Finance and Transport domains. One of the tool features is the targeting for both technical and non-technical profiles and the providing of a pre-filled list of possible threats and information, this allows even employees with low skills in cybersecurity to use it.

- Basically, the online self-assessment tool RATING allows users to:

- Recognise possible threats affecting their organizations;
- Self-evaluate their level of exposure thanks to the risk analysis they get from the tool;
- Look at a list of predefined threats;
- Provide themselves questions, information and references about the threats, as well as report new ones and give solutions to prevent or mitigate them, using the community interaction feature to enhance the community and improve the tool.

The Tool works with questions about the kind of assets managed by the organization and the security policies in place, as well as general information about the competences of the organizations' staff, resulting in a graphic of the threats-exposure of it. Furthermore, the tool gives the estimation of the accuracy of the assessment according to the questions that were answered.

RATING will be improved to include:

- The managing of assets from the tool (personal/sensitive information and its handling by classes of LPAs employees and/or IT systems), in order to estimate the threats for defined assets and to allow LPAs to focus on specific mitigation actions on the assets most exposed to risk.
- The review of the current knowledge base and the introduction of specific knowledge for LPAs.
- The support for the interaction with other COMPACT services (Threat Intelligence services, Business Process Monitoring and Real-Time Cybersecurity Monitor service, Security Training and Awareness service)
- The notification of the LPA personnel when the level of risk for a given threat exceed a given threshold.

Social Engineering (SE) Exposure Evaluation Service - TO4SEE tool consist of two parts, each one afferent to a different area of the phishing assessment.

Part 1 aims to mimic real-world phishing and emails and submit the stimuli/items to the employees of LPAs (attachments, links, visual appearance, and writing style) so that it would be possible to conceptually measure the ability of people in distinguish between legitimate and fraudulent emails.

Part 2 tries to find a measure to investigate the susceptibility of people to certain isolated and tightly controlled additional factors. The user will be submitted to a questionnaire composed just by part of emails and the results will show three measurements: the trustworthy of the email for the user, the choice to delete or not the email, the complying of the request.

Another part is reserved to the administrator, who can access to the setting page to manage users and questionnaires and to the statistics page to download the results in an excel file.

The COMPACT project will adapt the contents to the needs of the LPAs, also redesigning the quizzes according to the user and the work-environment.

Annex 1.9 shows the assessment table for COMPACT.

CS-AWARE

CS-AWARE offers a simple and cost effective cybersecurity awareness solution for Local Public Administrations (LPAs), non-Governmental Organization and Small and Medium Enterprises, in order to help them to understand their cybersecurity situation and protect them from cyberattacks.

The system offers solutions thank to the automatic detection and visualization of the incident, the exchange of information between national and EU level NIS (Network and Information Security) authorities, the self-healing of the system and the multilingual semantic support. It is based on cooperative cybersecurity that allows to gain information from others organisations.

In order to analyse cybersecurity requirements in the context of LPAs, it has been realized a detailed Threat Assessment, an analysis of relevant information sources (NIS Competent Authorities, Law Enforcement Agencies, Cyber Intelligence Sources and Information Sharing Tools, including Commercial Data Providers, Cybersecurity Intelligence Data, Malware Analysis, Vulnerability Data, Social Media, Cybersecurity Visualizations and Other Information Sources) and an analysis of the piloting scenarios of Larissa and Roma Capitale (through soft systems workshops conducted in place).

The detailed assessment they conducted within the project was based on the threat assessment perspectives of NIS competent authorities (ENISA threat Landscape Report 2016), law enforcement (The Europol Internet Organized Crime Threat Assessment report of 2017) and a threat assessment from a commercial security provider (McAfee Labs threats report of June 2017).

In short, the threat agents identified for LPAs have been cyber criminals (for monetary gain), Insiders (disgruntled or for monetary gain), Hacktivists (problem with a policy decision), and script kiddies (bored teenager as well as disgruntled citizen). These agents would possibly use the following threats: Malware, Physical manipulation/damage/theft/loss, data breaches and Identity theft; Web-based attacks, web application attacks, DoS, Botnets, Phishing, Spam, Ransomware and Information leakage; Insider threat, Exploit kits and Cyber espionage. The assessment followed with the identification of the risks in three levels (low, medium and high), based on relevant threats, relevant threat actors and their motivation.

Also External Information Sources have been analysed in order to identify cybersecurity relevant information sources to be utilized by CS-AWARE system. This allowed to better understand the global threat landscape, to gather information about possible vulnerabilities and attacks and finally to better support the assessment of the risks associated to those factors in the LPA context. The analysis results showed that the most valuable cybersecurity related information (or cybersecurity intelligence) for CS-AWARE could be found from official organizations (NIS competent authorities or law enforcement organizations) as well as from private efforts (for-profit companies or non-profit communities/ projects). Moreover, social media or data visualization focused data sources can provide more generalized data.

A set of indicators/metrics was defined to assess, on a qualitative level, the quality of the relevant information sources. The CS-AWARE Quality Indicators for information sources are the following:

1. Quality of Data (Indicators, Sightings, Courses of Action, Vulnerabilities);
2. Provider Classification (Data Feed Provider - Provides Original Data and Provides Aggregated Data - , Intelligence Platform, Report Provider);
3. Licencing Options (Open (Publicly available), Restricted use, Commercial, Information Reuse – Commercial use allowed, Academic use allowed and Personal Use allowed -);
4. Interoperability/Standards (STIX1, STIX2, TAXII, OpenIOC, RSS, JSON, CSV, Plain Text);
5. Advanced API (Filtering based on time, Filtering based on content);
6. Context applicable content (Vulnerabilities, Threats, Campaigns, Hashes, Recommendations, Incidents (Sightings)).

DEFeND

DEFeND project focus on improving existing software tools and frameworks aiming to develop a new 'integration software', driven by market needs, to deliver a unique organizational data privacy governance platform. Thus, a novel Data Privacy Governance for Supporting GDPR (DEFeND) platform supporting organizational-focused privacy governance and addressing challenges faced by organisations when complying with GDPR is investigated. A new paradigm the so called 'Model-Driven Privacy Governance' (MDPG) enables building (from an abstract to a concrete level) and analysing privacy related models following a Privacy-by-Design approach. This approach includes two levels, the Planning Level and the Operational Level, and three management areas, i.e. Data Scope, Data Process and Data Breach. The DEFeND platform will empower organisations in different sectors to assess the compliance status, plan the achievement of the GDPR compliance. Moreover, the platform will provide key services such as 'Data Process Management Service', 'Data Scope Management Service', 'Data Breach Management Service', 'GDPR Planning Service and GDPR Reporting Service'. These services are crucial for organizations enabling them to collect, analyse and operationalise different aspects and articles of the GDPR and provide appropriate reporting capabilities. The platform is composed by five back-end components, where each component includes a number of modules aiming to deliver functionalities.

Among the several objectives, some are interesting to ECHO, such as:

- Privacy Risk Assessments (PIAS/DPIAS) because it concerns design and implement processes to conduct and manage PIAs/DPIAs and risk assessments according to legal and regulatory requirements;
- Selection of an appropriate security technical and organisational measures because it put in practice physical, technical, and administrative measures to keep personal data secure and confidential through adequate standard or certification.

The innovative approach in Risk Assessment could also monitor cyber-risk. This objective would overlap the work on-going in ECHO.

DISCOVERY

DISCOVERY Project is developed to foster cooperation process and dialogue between Europe and North America (US and Canada) through collaborative ICT R&I both under Horizon 2020 and under US and Canada funding programmes. Thus, the project proposes a radically new approach to engage more actively and strategically ICT R&I cooperation. The institution of the Transatlantic ICT Forum is one of the most important action of the DISCOVERY that will be established as a sustainable mechanism to support policy debate, to provide opinions and recommendations for purpose-driven and mutually beneficial cooperation between Europe and North America. The project will focus on key aspects such as funding mechanisms, ICT policy and

regulations, and ICT priority areas of strategic interest for future partnerships in R&I, giving particular attention to cyber security is one of the most important aspects.

Moreover, the project aims to stimulate industry engagement and innovation partnerships between the industry, research and academia, by reinforcing networking and innovation partnerships. A unique set of participatory and co-creative methods and people-centric facilitation techniques is used to stimulate interaction among the groups of participants, such as the ICT Discovery Lab and well-targeted capacity-building workshops.

The DISCOVERY consortium has the potential to support action and dialogues contributing to reinforce ICT R&I cooperation between Europe and North America.

Being a project finalized to establish an International forum no Annex discussing criteria or methodologies implemented by Discovery project is provided.

PROTECTIVE

PROTECTIVE**[109]** aims to achieve enhanced Cyber Security Awareness (CSA), which consist in improving an organisation's ongoing awareness of the risk posed to its business by cyber security attacks. Threat Intelligence (TI) sharing and risk awareness are fundamental for the PROTECTIVE system, which is designed to provide solutions for public domain Computer Security Incident Response teams (CSIRTs) and Small to Mid-size Enterprises (SMEs). Key target groups of the PROTECTIVE project are also National Research and Education Networks (NREN) service providers, Managed Security Service Providers (MSSPs) and Managed Service Providers (MSPs).

The PROTECTIVE system wants to achieve CSA through two key contributions: increasing of the CSIRT's threat awareness (improved security monitoring, enhanced sharing of threat intelligence within a community), ranking critical alerts based on the potential damage on threatened assets and on the organizations business. Combining these two measures, PROTECTIVE prepares organization to better handle incoming attacks, malware outbreaks and other security problems and guides the development of the prevention and remediation processes.

The ambition of PROTECTIVE system is to raise organisational CSA by developing a comprehensive solution trough the improvement of security alert correlation and prioritisation, the connecting of the criticality of an organisation asset to its mission, the institution of a threat intelligence sharing community. It wants to do so by developing a computing platform that will provide the CSA functions related to the following key concepts:

- Threat Awareness (detailed overview of threats, internal and external; effective security monitoring; access to external sources of intelligence to recognize potential impending threats on operations; sharing TI inside of a trusted community);
- Mission Awareness (organisational assets as function of the business, assigning a criticality indicator; measure of the vulnerability exposure of the asset; providing of capability to make informed decisions on meta-alerts or on remediation);
- Constituency Awareness (accurate inventory of the configuration and operational status of hard infrastructure assets and contact and reachability details (e.g. IP address) for the served user base for CSIRTs);
- Context Awareness (summarising threat information and placing them into the perspective of the organization's mission or business).

The correlation between these concepts can be better understood from the figure below. TI is an input, as well as internal TI/security alerts, and an output of the “Threat Awareness” function. Correlated meta-alerts pass then to the Risk Awareness function where they combine with Asset Information, generating a ranked list of prioritized (meta) alerts ready to be passed along to the CSIRT operator for triage.

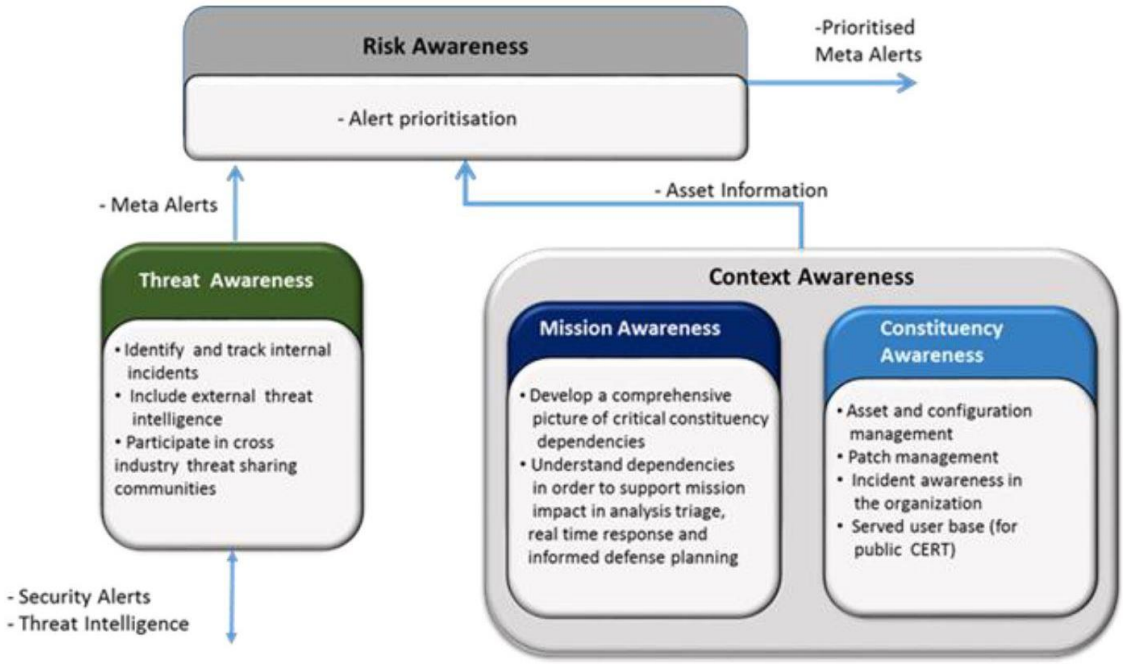

Figure 16: PROTECTIVE Cyber Situational Awareness Model (adopted from Mitre15) [109].

The security alerts are processed by PROTECTIVE, it insert detection indicators and low-level alerts only in the Ingestion subsystem, which receives data from both internal network sources (IDS, IPS, firewalls, network probes, system logs, honeypots) and third-party sources like other security alert systems (IntelMQ or n6, e-mail reports, etc.).

Critical alerts will be categorised and ranked by PROTECTIVE depending on the potential damage inflicted on the threatened assets and so on the organisation business by an attack. The assessment of potential damage is based on host criticality, vulnerability exposure, and level of trust to the alert sources. Furthermore, the damage can be measured in multiple ways for various perspectives such as operational (number of damaged devices, a decrease of efficiency, downtime) or business (lost revenue, loss of customer trust).

To prioritise meta-alerts PROTECTIVE takes information (about the risks related to criticality of the assets, damage potential and trust of the sources) from the Mission Impact Assessment module and the Asset State Management module, and takes scores from TI Trust component, all developed within the project. This approach is coherent with ENISA (European Union Agency for Network and Information Security) suggestions.

The project applies ranking methods in addition to the simple prioritisation that can be applied as follows:

1. To create priority groups for meta-alerts depending on the priorities previously assigned to them;
2. To create priority groups based on composite measures;

To rank meta-alerts without priority groups, in order to complement prioritisation techniques (next level of handling support. **Annex 1.10** contains assessment table for PROTECTIVE.

4.4 Concluding Remarks

With the goal to compare objectives and targets of the assessed methodologies and approaches, we should mainly focus on the three main EU project analysed (CYSM, MEDUSA, and MITIGATE). An official comparison between the projects has already been produced by Prof. N. Polemi, who served as technical and/or project manager of the three, and Prof. Spyridon Papastergiu in **[100]**, from where we take the following table as a reference.

Area	CYSM	MEDUSA	MITIGATE
Scope & context-boundaries	CYSM emphasizes on the protection of port facilities, based on the provision of a dynamic risk management methodology for ports' CII considering their physical-cyber nature	MEDUSA focuses on the protection of the port supply chain. It defines a Methodological approach for the identification of Multiorder dependencies of security risks, in the scope of multisector cross-border scenarios	MITIGATE enhances CYSM & Medusa towards protecting port facilities in the scope of interacting supply chains. MITIGATE adopts an evide-nce-driven maritime supply chain risk assessment model in order to capture and deal with cascading effects risks, threats, and vulnerabilities, associated with the ICT-based maritime supply chain
Threats landscape	CYSM supports identification and measurement of organization-wise threats. These include internal threats pertaining to the ports' ICT and physical infrastructure	Medusa supports identification and measurement of cross-sectoral and cross-border threats, including threats associated with cascading effects	MITIGATE supports the identification and measure-ment of combined cross-sectoral and cross- border attacks/threats paths and patterns arising from the ports' supply chain, both organization-wise and interdependent cyber threats deriving from the interconnection of the ports with other entities (e.g., ships, port authorities, maritime/insurance companies, customs, ship-industry) are evaluated
Impact analysis model	CYSM is based on models that determine the value of the corporate assets and estimate the potential impact of threats in terms of specific criteria (availability, confidentiality, integrity) and based on various organizational scenarios (cost, legal, technical, ...)	MEDUSA aims at modeling, visualizing, and simulating security scenarios and their cascading effects across CIs that are dependent on port CIs	MITIGATE enhances CYSM and Medusa in order to perform impact analysis for threats/assets involved in supply chain operations. This requires the integration of appropriate assurance models that are able to capture cascading effects and business factors in a multisector, multistake-holder maritime environment
Countermeasures	CYSM introduces countermeasures for reducing ports' risks	Medusa identifies and documents security measures that could	MITIGATE introduces additional countermeasures towards reducing risks

Area	CYSM	MEDUSA	MITIGATE
		minimize the consequences of cascading effects in multi-sector cross-border port security scenarios	associated with the whole supply chains. The countermeasures are produced based on the results of various simulation experiments, thereby exploiting the proposed evidence-based risk assessment approach
Cartography capabilities	CYSM operates on the based on the identification and representation of the ports' architectural structure	Medusa introduces algorithms for identifying multiorder dependencies between entities involved in the maritime supply chain	MITIGATE introduces algorithms and techniques for capturing and analyzing the multiorder dependencies between ports' ICT infrastructures and multiple critical information infrastructures (CIIs) participating in the global SC
Risk analysis	CYSM's risk analysis of the ports' facilities is based on a straightforward approach that relies only on the ports' users knowledge	MEDUSA assesses security risks, in the scope of multisector cross-border scenarios	Risk analysis in MITIGATE for the ports' supply chain is based on a more rigorous, rational approach that relies on high-quality scientific- and experimental-based data (e.g., simulation results, indicators,recommendations) and security-related information available at online repositories
Risk computational model	In CYSM a multicriteria group decision-making model has been developed and adopted in order to calculate the actual risk factor. The proposed model takes into consideration a set of criteria and parameters as well as the opinion of various users' groups with different vision angle	MEDUSA adopts an approach based on game theory and graph theory techniques to minimize the consequences of cascading effects in multi-sector cross-border port security scenarios	MITIGATE leverages simulation models (based on game theory and graph theory techniques) combined with a multicriteria group decision-making approach in order to produce timely, accurate, objective, reliable, relevant, and high-quality information associated based on which the multi-dimensional risks will be assessed
Standards compliance	CYSM is in-line with the requirement, rules, and obligations imposed by security and safety-related standards (ISO 27001, 27005, ISPS) that focus on the protection of the ports' facilities	Medusa's emphasis on the supply chain will be reflected in the provision of support for ISO28000	MITIGATE leverages and implements existing security standards (such as ISO 27001, 27005, 2800, 28001, ISPS) associated with the protection of the maritime ICT-based maritime SC
Predictive and forecasting capabilities	CYSM evaluates a predefined list of threats associated with ports' ICT and physical infrastructures	Medusa evaluates a predefined list of threats associated with ports supply chain	MITIGATE leverages appropriate simulation models and processes for the representation and

Area	CYSM	MEDUSA	MITIGATE
			prediction of the possible attacks/threats paths and patterns. These models are used to measure their effectiveness and applicability, as well as to and to determine the exploitation, resilience, and reliability level of ports' SC
Risk Assessment (RA) tool	The CYSM RA tool is based on a set of interactive and collaborative technologies	MEDUSA tool is based on a set of visualization tools and techniques to model and simulating ports supply chain scenarios	The MITIGATE RA tool adapts and integrates a number of risk management components, modules, and subsystems developed in the CYSM and MEDUSA and also incorporates a set of ICT technologies, including semantic web technologies (for ontology management, context management, and profiling), cloud computing and BigData, and crowd-sourcing technologies (i.e., in order to collect and analyze open information from public resources)

Table 26: Comparison between CYSM, MEDUSA, and MITIGATE methodologies.

Table **26**describes ten functional areas revealing the evolution of results across the projects, from CYSM to MEDUSA and finally to MITIGATE. In fact, it should be noted that the MITIGATE system has been built upon the security and safety management system developed in CYSM and MEDUSA, also adding a number of advances during MITIGATE implementation and integration. In fact, on top of the RA and RM implementation, MITIGATE exploited recent ICT and very innovative technologies like e.g.:

- Cloud computing for the development of the web-based service-oriented and on-demand collaborative infrastructure;
- Big Data technologies for threat analysis, including threat prediction, and
- Semantic web technologies (including ontologies) for the representation of assets, risk models, and assurance models, including the representation of data from open intelligence sources (i.e., social network and crowd-sourcing).

Nevertheless, it should be noted that the RA approach produced by CYSM is limited to the port's domain and does not consider cross-sectoral, cross-border threats from SCs. So, the MEDUSA project has introduced an innovative and scalable RA environment adopting a number of configurable and flexible functions and facilitating the creation of an effective and efficient solution for SCSs through the estimation and remediation of possible consequences. The MEDUSA system successfully passed an extremely wide validation phase.

The recent ICT-empowering opens to more complex and demanding methodologies, consequently requiring further innovation in Risks and Vulnerabilities Assessment paradigms as well as in Risk Management

methodologies. Since MEDUSA does not deal with security management, evaluation, and mitigation of IT-based (cyber) risks, it cannot be considered a methodology for cyber RA. On the other side, MITIGATE introduces a RA methodology enhancing the protection against ICT-related threats in the form of a more complex global risk assessment framework also able to deal with cascading effects risks

The valuable methodology for final impact estimation for a given asset based on an initial *personal impact assessment* followed by an *overall impacts assessment* does worth to be taken into consideration. As in CYSM, also in E-MAF, a list of threats is formulated taking into account both experience from incidents and past threat assessments and threat catalogues available from industry/standardization bodies, national governments, legal bodies, etc. The identified threats are grouped into various categories, whose description will be introduced when discussing the Logical Model adopted in E-MAF (see Section **5.3**). It is also worthwhile of consideration the threat assessment made through a *personal evaluation* followed by the *Overall Threat Assessment* to determine the likelihood of occurrence of each threat to a specific asset from each department as well as the *Final Likelihood of occurrence* of each threat as the maximum of all departments. A similar statement could be done for Vulnerability analysis in ECHO where MEDUSA approach must be mutated and melted with the ECHO specific design. *Personal Vulnerability Assessment* and *Overall Vulnerability Assessment* leading to the calculation of the Final level of exploitation of a vulnerability represents a valuable approach. Risk determination in ECHO will happen in a similar manner with respect to CYSM but the explication of the multi-sector dependencies must be considered. For this reason, getting inspired from MITIGATE steps 4 and 5 for SCS Impact Analysis and Risk Estimation seems to be a valuable approach. Taking into consideration the Cumulative and Propagated impacts as well as the Commutative and Propagated risk to be merged with Individual analysis and estimations shows to be an also interesting approach.

The cyber threat analysis, in the context of ECHO project, could exploit approaches fostered by MITIGATE and CS-AWARE projects. In both cases information retrieved from social media and existing sources/repositories play a very important role to gather peripheral information and draw conclusions.

The community-building activities made in the aim of the CANVAS project are also valuable. Even not directly related to Risk Assessment the policies for alliance and self-organization leading towards tackling open questions are issues worth to be evaluated, also because a multi-domain approach took place in the project providing a very interesting resource for following projects aimed to innovate cybersecurity.

The certMILS project aims to facilitate the building and certification of complex critical systems by using a certain architecture for structuring these systems into partitions that run on a separation kernel, called MILS (Multiple Independent Levels of Security/Safety). Lesson learned during the project should be taken into consideration when E-MAF will be supporting the definition of the ECHO Certification Scheme (T2.7).

The Risk Assessment activities and Data Breach Management Service in the DEFeND project focus on a set of issues which overlap the cyber threats affecting GDPR and Privacy issues in the aim of independent and transversal issues as defined in ECHO. For this reason, the project outcomes should be monitored while developing and fine-tuning E-MAF.

WP2 should also inspect highlights on key focus areas and hot topics contained in DISCOVERY Cybersecurity Policy Brief document in order to consequently monitor the on-going cooperation between EU, US and Canada.

5. The ECHO Multi-sector Assessment Framework

5.1 Methodology for design and implementation of E-MAF

The ECHO Multi-sector Assessment Framework provides the means to analyse transversal, multi- and inter-sectoral challenges and opportunities while assessing the risk an organisation is subjected to. In addition to this E-MAF proactively supports the development of the Technology Roadmaps in ECHO by providing a dynamic means to evaluate and analyse effects of governance actions during the design and the implementation of the roadmaps.

This section will depict the designed multi-tier (three tiers as will be discussed in Section **5.2**) architecture of the E-MAF describing the underlying vision as well as the tight interaction between WP2 tasks in order to improve its implementation towards the full achievement of the foreseen outcomes as described in [GA]**.** This deliverable covers just a partial set of outcomes as foreseen in ECHO time-schedule. For this reason, the remaining ones (risk scoring, support to training programs, contribution to the certification scheme, etc.) will be discussed in the following version of the D2.2 deliverable whose delivery is foreseen on M45, even they will be obviously impacting the architecture of E-MAF and impose adjustments on it. At the time of this writing, some activities of these already started; description of requirements to be fulfilled or challenges to be faced as well as solutions to mitigate associated risks are under development, and related tasks are consolidating their outcomes. All of this information will be included in the last version of D2.2 while developed features are going be ingested along with the several implementation enhancement phases T2.2 puts in place.

So, the delivery of E-MAF consists of a number of prototypes where each subsequent prototype enhances the preceding one by e.g. increasing the set of features offered, tuning the operating parameters or algorithms, and/or improving global risk level determination.

Being an important element in ECHO, E-MAF's first prototype is eagerly requested. The development phase started together with the first release of this deliverable (November 2019) and is constantly following improvements in the design. The prototype delivery is imminent and opens the path for a demo during the next review meeting in September/October 2020.

Adoption and deployment of E-MAF prototype do not simply relate with WP2 tasks. It is expected to support also a number of other WPs in ECHO such as:

- WP3 in the aim of the Governance Model definition;
- WP4, to refine the analysis of transversal technical cybersecurity challenges (task T4.1) and to support the development of inter-sector technology roadmaps (T4.2);
- WP5 for the implementation of Early Warning System and the definition of its Demonstration Cases;
- WP6 for the implementation of Federated Cyber Ranges and the definition of its Demonstration Cases.

Interim versions of this deliverable were already presented to the respective WP teams. Furthermore, the continuous release of improved versions of E-MAF along the project lifetime will take into consideration the feedback and the requirements coming from all of these tasks and will include key updates.

In the following it is worth recalling that the E-MAF **leverages cyber risk management fundamentals** as the basis for the framework. In order to get this, the T2.2 exploits the advantages of:

- having in the ECHO consortium a large multi-domain community and rich of expertise, so that an approach based on virtuous cycles of innovation can easily take place;
- using the *concept of operations* (CONOPS) methodology in T2.2 and T2.3; CONOPS involves a human-centered approach to understand the roles of human, organisational, technical and material resources in operations, particularly those that involve inter-organisational dependencies. It is quite

easy to find examples of military and emergency management interpretations of CONOPS but the standard here is more closely relevant to software development. Since T2.3 is proposing and designing a further improvement of CONOPS methodology in order to improve sensitivity and capability to adhere to cyber security issues, T2.2 is monitoring and fostering T2.3 activities. The evolved CONOPS methodology will be adopted in T2.2 representing a important step ahead towards the enhancement of effectiveness for E-MAF design at the price of an acceptable increase of complexity in user-centred approach.

Frameworks for the **assessment of cyber-risks** are being developed in various industries and contexts, in most cases with a common root in the NIST CSF **[27]** framework or the ISO 27000 series, and are typically structured around 5 key functions well depicted in**[27]**:

1) **Identify** function determines all assets and processes requiring protection in the deploying entity systems;
2) **Protect** function organises all means already in place to enable protection for those assets/processes function;
3) **Detect** function enlists all the applicable techniques for incidents detection;
4) **Respond** one takes into consideration all the options to respond and limit the unwanted consequences of those incidents;
5) **Recover** function enables to restore processes and recover the full functioning assets.

Even most of the other Risk Management and Assessment method/methodologies assessed in Section **2** refer to those frameworks or deploy a similar structure.

So, according to the Grant Agreement [GA], **the ECHO Multi-sector Assessment Framework** refers to the analysis of challenges and opportunities derived from sector specific use cases, transversal cybersecurity needs analysis and development of inter-sector Technology Roadmaps involving horizontal cybersecurity disciplines. Since a Risk Management framework must include Risk Assessment, which is just the first and initial part of the whole Risk Management process, in the core of E-MAF is the **cyber Risk Assessment Methodology** and its corresponding implementation, the **cyber Risk Assessment framework** with their

additional functionalities. Figure **17** describes how the E-MAF Risk Assessment elements, one of the basic set of elements of E-MAF, fits into the high-level design of the ECHO Risk Management service.

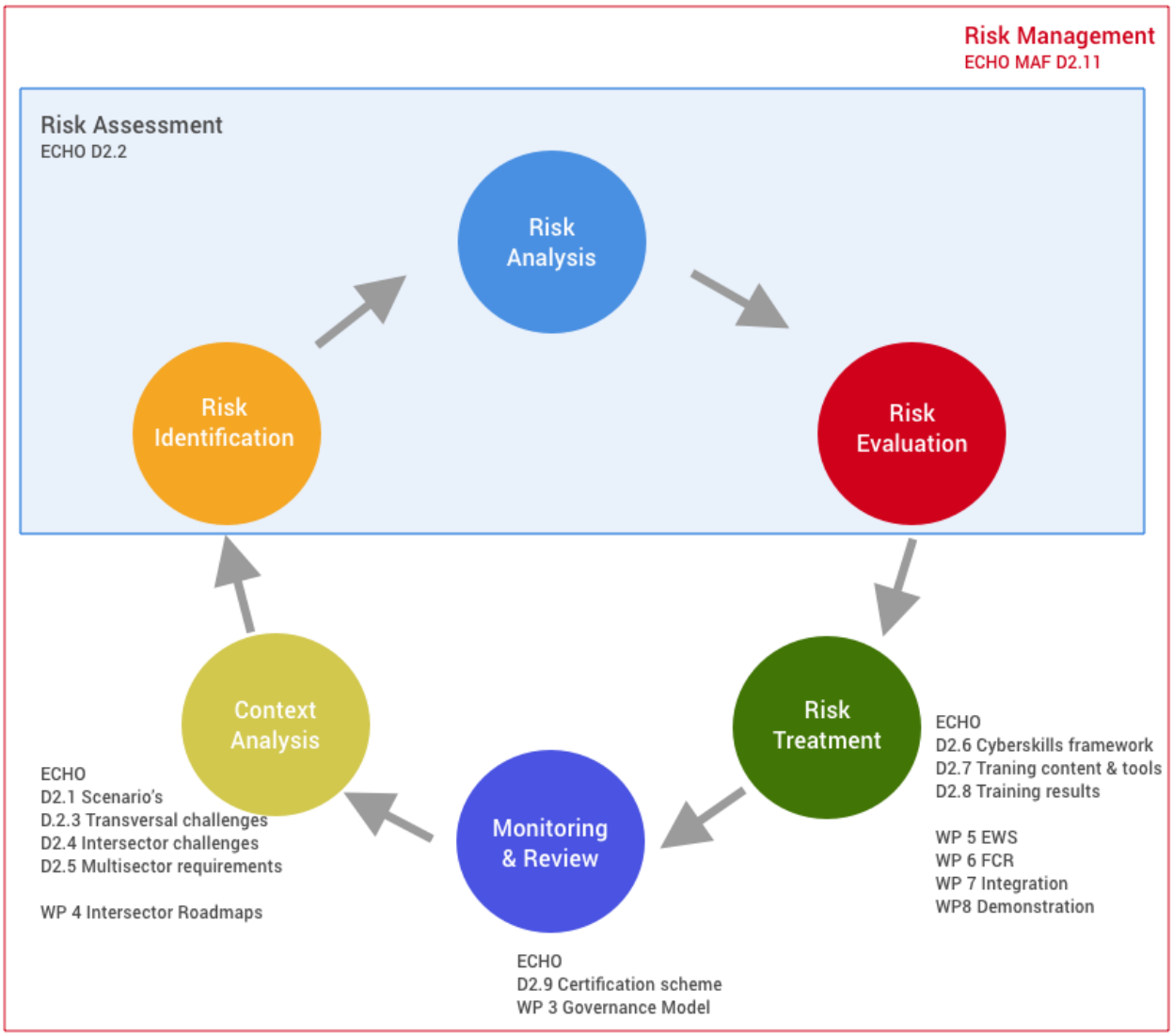

Figure 17: ECHO Risk Management high-level design.

In the Risk Assessment three important steps take place**[19]**:

- **Risk Identification**, the process of determining, document and communicating risks that could potentially prevent an organisation or a process from achieving the foreseen objectives;
- **Risk Analysis**, which means identifying and analysing potential issues which could negatively impact processes or systems in order to support organizations in avoiding or mitigating those risks;
- **Risk Evaluation**, by comparing the results of the risk analysis with the risk evaluation criteria to determine whether the level of cyber-risks is acceptable.

According to ISO31000-2018 **[19]** (see Section **2.2**), the purpose of Risk identification is "*to find, recognize and describe risks that might help or prevent an organization achieving its objectives*". In order to do this, the organization refers to plenty of techniques and methodologies that, based on up-to-date information, is aimed

to identify risks possibly affecting objectives. This activity is performed by focusing factors like the following ones and the relationship between them, independently from the chances to control their sources:

- tangible and intangible sources of risk;
- causes and events;
- threats and opportunities;
- vulnerabilities and capabilities;
- changes in the external and internal context;
- indicators of emerging risks;
- the nature and value of assets and resources;
- consequences and their impact on objectives;
- limitations of knowledge and reliability of information;
- time-related factors;
- biases, assumptions and beliefs of those involved.

In the same document **[19]**, the goal for Risk Analysis (see Section **2.2**) is defined as "*to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk*" in an environment where multiple cause can generate a risk determining multiple consequences and affecting multiple objectives. This cannot obviously be done without detailed consideration of "*uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness*". It is clear how Risk Analysis can be undertaken with varying degrees of detail and complexity, depending on the purpose and the available information, and consider factors like:

- likelihood and consequences;
- nature and magnitude of consequences;
- complexity and connectivity;
- time-related factors and volatility;
- effectiveness of existing controls;
- sensitivity and confidence levels.

Risk analysis strongly depends on the quality of information (e.g. assumptions and exclusions) available, human factors (opinions, perceptions of risk, etc.) and mainly on the techniques (even in combination). The outcomes of Risk Analysis are an input to Risk Evaluation, the purpose of which is to support "*decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment strategy and methods*". This is done by comparing the results of the risk analysis with the established risk evaluation criteria and determining whether any additional action is necessary in light of the consequences perceived by internal and external stakeholders. The decision can be to**[19]**:

- do nothing further;
- consider risk treatment options;
- undertake further analysis to better understand the risk;
- maintain existing controls;
- reconsider objectives.

In order to fully define the new ECHO Risk Management Methodology, T2.2 will, in addition, need to address the issues (according to ISO31000-2018**[19]**, see Section **2.2**) related to the following three processes (see non-RA-related processes in Figure **17**):

- **Risk Treatment**, all actions aimed at selecting and implementing options for addressing risk; this process obviously modifies risk through actions like: i) avoiding the risk by ceasing to perform the

activity generating the risk; ii) taking risk in order to pursue different goals or opportunities; iii) removing the risk source; iv) changing the likelihood;
- **Monitoring and Review** to assure and improve the level of the quality and effectiveness of design, implementation and outcomes of Risk Management as a periodic process;
- **Context Analysis**, by establishing the scope, the context (both internal and external), and all necessary criteria to tune the Risk Management process and, within this, validating and refining risk assessment and risk treatment policies.

These additional processes will be discussed in more detail in the next section, while depicting the architectural design of the final E-MAF.

Through the implementation of the three processes composing the Risk Assessment (i.e. Identification, Analysis and Evaluation), T2.2 instead defines the **first prototype of the E-MAF**, focused on the implementation of the ECHO Risk Assessment Framework, which will be defined by combining results from top-down methodologies assessment and bottom-up domain assessments and then optimized through the outcomes provided by other tasks in WP2. In fact, as it is going to be discussed in the next section, E-MAF consists of several elements (tiers and their internal layers). Those elements analyse and assess cyber security challenges starting from one sector (domain) and expanding to others with respect/focus also on:

- Transversal opportunities and challenges (T2.3),
- Technical challenges (T2.4) and
- Multisector dependency/relations (T2.5).

As a proof for the need for E-MAF, as highlighted in Section **2**, the analysis of existing frameworks (T2.2) concluded that current Risk Assessment Frameworks do not take into account relations between sectors and are not able to address multi-domain and transversal issues in an effective and transparent way. In the meanwhile, T2.3, T2.4, T2.5 and partially T2.6 in parallel develop related (internal) methodologies to assess different cyber security issues and aspects.

E-MAF design process started to grad these methodologies from respective tasks, which started at M9, and analysed, merged, clustered, etc. them. They create complementing elements of the E-MAF and serve as foundation (together with the Risk Assessment Framework) of the E-MAF Risk Management.

The analysis of existing frameworks and methodologies as well as current or previous projects, both dealing with critical infrastructure cybersecurity issues and challenges, is one of the main pillars of the E-MAF. Based on this analysis, current state of the art and existing gaps will be clearly identified. Following this, E-MAF has elements/layers to take into account specific issues in critical infrastructures. Based on a multi-sector, inter-sector, and transversal issues focused approach it aims to address them.

E-MAF is not and will never definitely be an updated version of currently existing Cyber Security Frameworks (e.g. NIST CSF**[27]**, TOGAF **[30] [33]**, etc.). But **it refers to them to take inspiration in defining a new approach based on a multi-sector, transversal reference to cybersecurity Risk Management** (and consequently assessment).

The final version of the E-MAF (D2.11, M45) will also be the outcome of several effective and fruitful iterations between the T2.2 and the other WP2 tasks. Figure **18**depicts the elements involved in the *first iteration* between the T2.2 (E-MAF) and other task in WP2 as well as the contribution it will provide to WP3, WP4, WP5, and WP6 through the first prototype deployment.

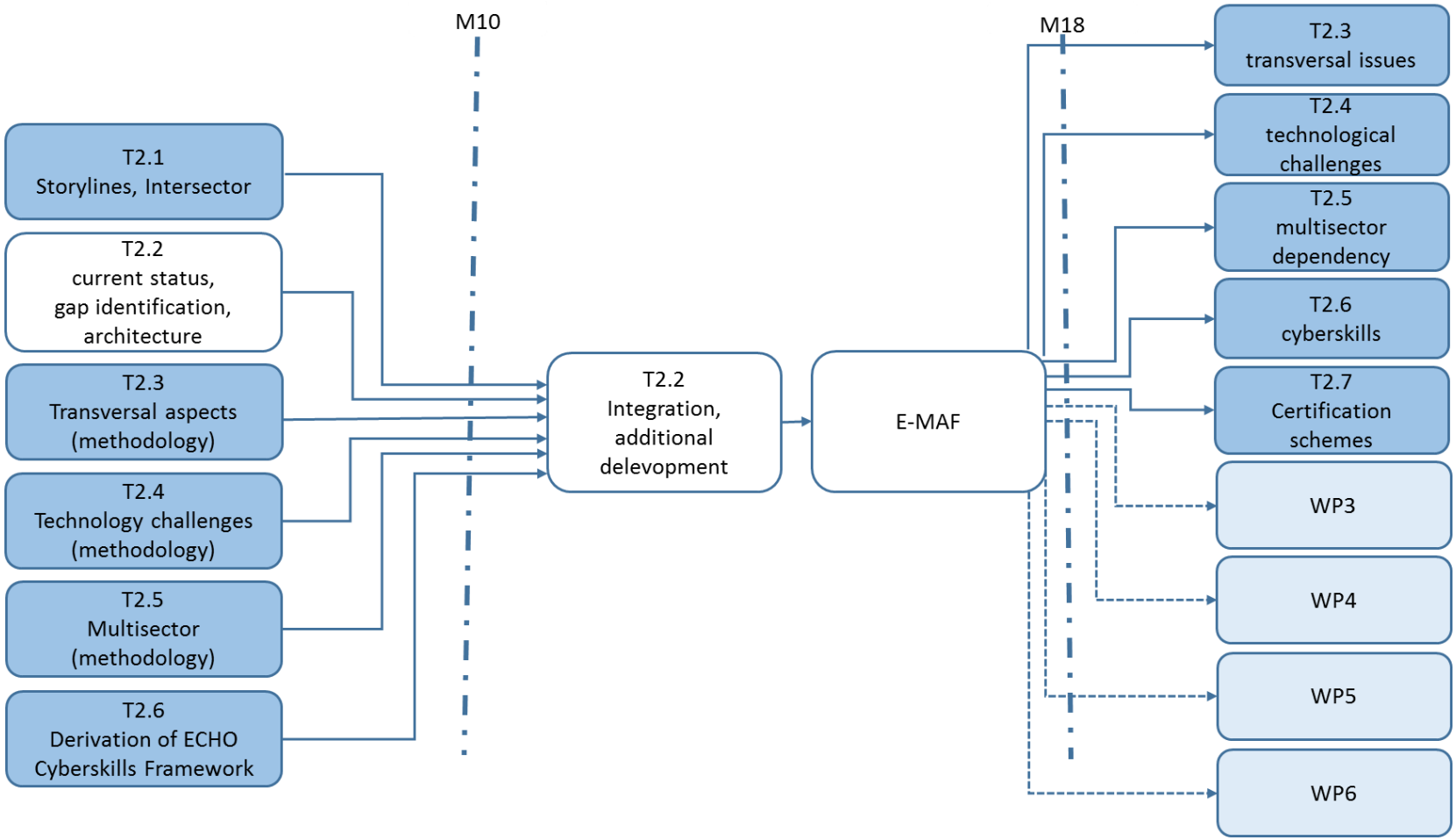

Figure 18: The first iteration between E-MAF and other tasks of WP2 and ECHO.

The first iteration feeds the integration and development process in T2.2, which will be the outcome of a multi-level collaboration between:

- The StoryLines described by T2.1 (D2.1 **[1]**); they provide sector-specific scenarios and use case analysis, ingesting in E-MAF important information on best practices, requirements elicitation and analysis, multi-sector and inter-sector based deployment scenarios will be derived from sector specific instances of cybersecurity breaches.
- The assessment activities, the identification of gaps and the architectural design internally provided by T2.2 and discussed in this report (D2.2).
- The methodology identified in conducting analysis of transversal cybersecurity challenges (T2.3); common challenges and opportunities, as identified and documented in D2.3 **[2]**. These include, but are not be limited to, policy and regulatory aspects, legal and ethics aspects, privacy/data protection, human factors, psychological aspects, educational and training aspects, etc.
- The methodology established in technology-based approach (D2.4 **[3]**) in order to ensure inter-sector cybersecurity (T2.4).
- The methodology applied in T2.5 to identify inter-sector cybersecurity challenges that appear prevalent and have an impact on multiple sectors (D2.5 **[4]**).

Further, initial outcomes from T2.6 (Derivation of ECHO Cyberskills Framework and related trainings) serve as inputs in the forthcoming T2.2 activities. In fact, starting from the key elements of the preliminary analysis activities related to competence framework for professionals in the cyber security domain (Cyberskills Framework), the cybersecurity educational portfolio and related training programmes elements (together with training and assessment methodologies, content, etc.) will be defined. This will happen also setting up a feedback process between T2.2 and T2.6 to systematically monitor and update the set of competences foreseen to improve the effectiveness of E-MAF, from one side, and to deal with it, from the other one. As an example, outcome of preliminary analysis activities will be used to align the Cyberskills Framework with EU level competence frameworks.

An integrated/comprehensive E-MAF is currently under development based on analysis, designed architecture, identified applicable Risk Assessment Methodology, and will include among others a methodology for identification of transversal cyber security challenges and opportunities (D2.3 **[2]**), cybersecurity technical risk challenges (D2.4 **[3]**), and multisector dependency (D2.5 **[4]**) as well as the identification of inter-sector dependency (D2.1 **[1]**).

The short term goal is to feed the E-MAF prototype with developed use-cases (StoryLines) and run Risk Assessment. As an output of this execution (analysis, exercises, etc.), E-MAF produces inputs respectively needed by T2.3 **[2]**, T2.4 **[3]**, and T2.5 **[4]**. In addition to this, E-MAF prototypes produce outputs which could be suitable for improvement of:

- T2.6 **[5]** for the ECHO Cyberskills Framework with training;
- T2.7 **[6]** for the ECHO Certification Scheme;
- WP3, for support in decision making within the Governance Model;
- future Technological Roadmaps (in WP4);
- WP5 for the Early Warning System; and
- WP6 in the Federated Cyber Range.

In order to obtain this T2.2 will develop and use methods to describe:

- organisational security functional and assurance requirements;
- product security functional and assurance compliance to requirements;

- test and evaluation procedures to validate whether or not a product meets the organisational security functional and assurance requirements.

The *iteration process* leading to the release and deployment of the several prototypes of E-MAF will continue until the end of ECHO project, through several virtuous cycles of innovation and enhancement for the E-MAF itself. With tight reference to the Grant Agreement [GA] the methodology to develop the E-MAF will also comprise the following steps:

1. Finalization and Optimization of the prototype through the comparison against existing Risk/Cybersecurity Management Frameworks as:

   a. ISO/IEC 27001**[15]** and 27002 providing a high-level set of controls that can be implemented as a baseline by any type of organization;
   b. NIST SP 800-53**[103]**, although intended for US federal agencies; SP 800-53**[103]** controls and provides a comprehensive and detailed information security RM framework.
   c. National CSF frameworks (e.g. Italian)

2. Starting from the RA methodology, development of operational guidelines involving both traditional cybersecurity factors and financial/economic ones;

3. Development of advanced specific metrics, scoring of risks levels;

4. Development of checklists and operational plans;

5. Development of recommendations for risk financing strategies;

6. Study of certification and assurance procedure; and

7. Final development of a multi-sector cybersecurity framework with focus on EU specificities and policy targets, compatible with Member States policies and regulations and taking into account cross-border risks.

Willing to fully match the Grant Agreement [GA], the non-trivial challenge for ECHO Multi-sector Assessment Framework is to finally aim at:

- supporting improvement of multi-sectorial management processes for mitigation of cybersecurity risks;
- providing the international community with the definition of the transversal and inter-sectoral skills as well as qualifications needed;
- developing the basis of a new and effective cybersecurity educational portfolio and related training programmes;
- defining a new methodology for assessment of transversal and inter-sectoral technology challenges and opportunities;
- developing a risk-based methodology, including cybersecurity and financial factors, to assess inter-sectoral cybersecurity technology challenges and risks as well as defining risk financing strategies for the residual risk;
- developing a method to mitigate inter-sector challenges through optimization of technology roadmaps involving horizontal cybersecurity disciplines;
- providing leverage to guide actions related to development of technology roadmaps and provide confidence in programs and actions taken; and
- helping to benchmark initiatives.

So, another main element in this discussion is that, in addition to the Risk Assessment, the ECHO Multi-sector Assessment Framework will also support multi-sector dependencies management as elaborated above.

Starting from the methodologies identified for transversal cybersecurity challenges (T2.3) and technology-based approach (T2.4) for inter-sector aspects, the E-MAF Framework will employ a **standardised methodology for risk assessment and scoring**, both from a qualitative and a quantitative point of view, tailored to specific requirements coming from domains and to the evolution of user-centred CONOPS approach. This is done with the constant goal to make the framework both certifiable and assurable.

Since both StoryLines defined in T2.1 and Technological Roadmaps to be defined by WP4 will continuously evolve throughout the ECHO project in order to adhere to real need of organisations in terms of cyber risk management and governance, they represent the most probative test bed for the **E-MAF Validation**. Validation will be possible at every iteration.

As far as it may concern the **development approach for Educational Portfolio and Training Programmes**, the information provided by T2.6 (see Figure **18**) are combined with the analysis of most recent and innovative approaches in Training and with the identification of the key element of Education Portfolio in order to create the best fitting Education and Training.

5.2 Architectural Design of the Multi-sector Assessment Framework

As described in Section **5.1**, T2.2 does not aim to develop an updated version of existing Cyber security frameworks. Thanks to the assessment activities, it exploits valuable approaches, methodological aspects, and controls in an innovative solution just taking inspiration in experiences coming from a multi-sector domain and transversal reference to cybersecurity Risk Management (and consequently Risk Assessment). The meaning of Framework as a voluntary guidance to assess, manage, and reduce cyber risks will obviously persist. E-MAF fosters RA-related and cybersecurity management communications being strictly linked to ECHO Early Warning System (WP5). In addition to this, it is designed to be customized by different sectors and individual organizations to best suit their risks, situations, and needs.

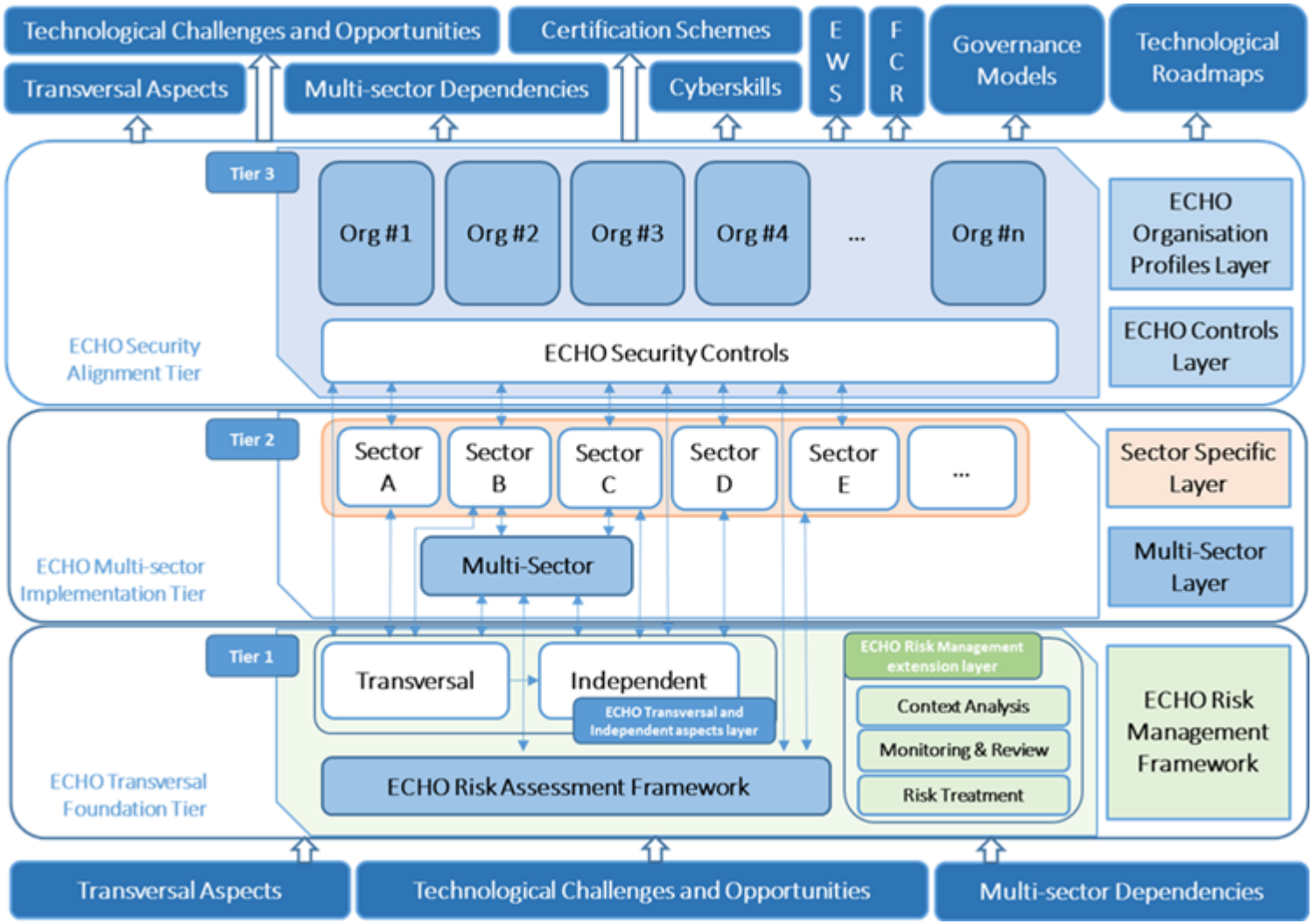

Figure 19: The Architectural Design of the ECHO Multi-sector Assessment Framework.

As described in the Grant Agreement [GA] organizations and sectors will still have unique risks (different threats, vulnerabilities, risk tolerances) and implementation of practices to achieve positive outcomes. So, the E-MAF will not be implemented as an uncustomized checklist or a one-size-fits-all approach for all critical infrastructure organizations but as an integrated tool where the ***overlay of the three different complex subsystems*** takes place. For this reason, the architectural design of ECHO Multi-sector Assessment Frameworks deploys a **three-tier architecture** comprising:

- the ECHO MAF **Transversal Foundation Tier** (E-MAF **TFT**), guiding organizations in managing and reducing their cybersecurity risks in a way that complements an organization's existing cybersecurity and risk management processes; here the Risk Management Framework described in this section concretizes and also the transversal and independent aspects are identified and isolated;
- the ECHO MAF **Multi-sector Implementation Tier** (E-MAF **MIT**), where all the multi-sector and inter-sector specific aspects are managed; this tier will support organizations by providing context on how they view cybersecurity risk management (risks, priorities, budgeting); and
- the ECHO MAF **Security Alignment Tier** (E-MAF **SAT**) where ECHO Security Controls will be defined and implemented; also specific organization's alignment to ECHO MIT and TFT will take place by identifying and prioritizing opportunities for improving cybersecurity in a general and in a Use Cases-driven manner (T2.1, CONOPS).

As far as the possible delivery formats for E-MAF, information are available in Section **5.4**.

Figure **19**depicts all the elements of the E-MAF and highlights the dependencies between them, as well as inputs to E-MAF and output it provides to other actors/processes in ECHO project. E-MAF requires as an input information on:

- **Transversal aspects** produced by the detailed analysis of transversal cybersecurity challenges that appear prevailingly independent of industrial sector and serve to identify common challenges and opportunities
- **Technological challenges and opportunities** provided by the application of the technology-based approach to ensure inter-sector cybersecurity and which raises both opportunities and challenges. They will have to be considered, taking into account the specificities of each sector and how security, law and policies influence it.
- **Multi-sector dependencies** which are outcomes of the detailed analysis of inter-sector cybersecurity challenges that appear prevalent and touch on multiple sectors, like horizontal cybersecurity disciplines related issues.

These represent the basic information for the multi-domain added value for the RM approach in ECHO.

In the top section of Figure **19**the outputs or the processes benefitting of outcomes produced by the adoption of E-MAF are depicted. First of all, in the top right end side, four entities (which are external to E-MAF) are shown:

- The **Governance Model definition**, and in particular the **Information sharing models definition** activities, since the ECHO services (e.g. E-EWS) will produce the unavoidable review of information sharing and trust models from within the cyber domain and the other domains involved (e.g., healthcare information sharing models). Information produced by E-MAF supports the effective information sharing model within ECHO.
- The **Inter-sector Technology Roadmaps** design and development activities, where the E-MAF outputs will act as input in the further analysis of transversal technical cybersecurity towards the identification, and categorisation of the most pressing security concerns and treats leading to a shared

vision on the current and emerging technical cybersecurity challenges for multiple and complementary horizontal cybersecurity disciplines.
- The **Early Warning System** whose future research, development and implementation activities will benefit of results from E-MAF.
- The **Federated Cyber Range**, where the E-MAF will support future Research, Development and Implementation through the results produced.

In addition to this and to support the continuous iterative process for information exchange depicted in the Section **5.1**, the remaining elements in the top section describe that the outputs produced by E-MAF application cyclically represent the input for other project activities during the several iterations in order to improve all project outcomes in terms of:

- **Transversal aspects** by fostering the transversal cybersecurity challenges and opportunities definition through the enhancement of detailed analysis process applied to prevalent transversal cybersecurity challenges.
- **Technology challenges and opportunities** to enhance activities ensuring inter-sector cybersecurity methodologies and improve outcomes of its application.
- **Multi-sector dependencies** by feeding and enhancing analysis of inter-sector cybersecurity challenges prevalent and touching on multiple sectors.
- **Cyberskills** by providing key information to develop learning outcome-based competence framework for professionals in the cyber security domain.
- **Cybersecurity certification scheme** by fostering the matching of the diverse needs of sector specific and inter-sector issues in the development of the ECHO Cybersecurity Certification Scheme.

The multi-tiered architecture presented above allows, by the analysis of StoryLines and UseCases in D2.1 **[1]** through the E-MAF, to identify and define transversal and inter-sectors challenges for ECHO which are driving the final definition of Risk Management Methodology and Framework implementation in T2.2.

In the aim of **ECHO MAF Transversal Foundation Tier** we can identify three different layers:

- The **ECHO Risk Assessment Frameworklayer**, defined by combining results from the assessment of methodologies, information coming from the domains, and outcomes provided by other WP2 tasks as described in Section **5.1**; according to the processes described above, this layer implements solutions for:

    - **Risk Identification**,
    - **Risk Analysis**, and
    - **Risk Evaluation**.

  Please refer to the previous section for a detailed definition of the three abovementioned processes.
- The **ECHO Transversal and Independent aspects layer** where two different modules take place:

    - The **transversal aspects module** enables focus on horizontal technologies and cybersecurity in critical sectors, addresses inter-sector cybersecurity disciplines and transversal security aspects that are independent of sector or discipline; transversal cybersecurity factors include those which are present regardless of industrial sector (e.g., personal data privacy protection, regulations, policies, addressed in T2.3) while inter-sector factors are those which may be sector related, but span more than one sector (addressed in T2.3); the research outcomes contained in D2.3 **[2]** will be uses as a basis for research and implementation activities in implementation of the module.

- In the same manner, the **independent aspects module** focuses on technical and technological factors which are independent from the industrial sector and commonly present.

- The **ECHO Risk Management extension layer**, complementing the RA layer towards the implementation of a full Risk Management Framework. It comprises implementation of processes for:

  - **Risk Treatment**, where the clear purpose is to select and implement the proper option(s) to address a specific risk. This is often done through an iterative process involving several phases: i. listing and selection of options by also balancing the potential benefits with respect to the achievement of objectives against costs, effort or disadvantages of implementation; ii. planning and implementing treatment; iii. assessing effectiveness of intervention; iv. evaluating residual risk and eventually opting for a new iteration; the selection should take available resources and organizations' objectives into consideration and clarify that: no "always appropriate" option exists, treatments sometimes produce unexpected consequences, stakeholders should always be aware of the remaining risk after treatment; if no treatment options are available or the residual risk is not small enough, the risk should stay under "ongoing review" and be well documented waiting for further treatment.

  - **Monitoring and Review**, where constant monitoring and periodic review of the cyber risk takes places (in all stages of a given process) through provisioning of monitoring plans, information analysis, effective reporting of results and feedbacks. The goal is assuring and improving the level of the quality and effectiveness of design, implementation and outcomes of Risk Management as a periodic process as stated in the previous section; when applying a risk treatment, new risks can arise, so monitoring and review can be ensured not only on residual risk. This module will provide solutions for recording and reporting risks so that the decision making process could be based on valid information, sensitivity as well as external and internal context. Reports planning should properly define: i. frequency and cost of reporting; ii. reporting methods; iii. relevance analysis of information to be provided.

  - **Context Analysis**, establishing the scope and context (meant as defining external and internal parameters to be taken into account when managing risk) as well as criteria for the risk management policy. The external context is the environment (social, political, technological, trends, external relationships, etc.) where the organisation operates to achieve its objectives. The internal context is instead strictly related to internal factors like contracts, relations with internal stakeholders, the available resources and knowledge, the organisation governance and structure, etc.). The context analysis allows to tune the Risk Management process and, within this, validating and refining risk assessment and risk treatment policies. Effective customization of risk management, through proper risk assessment and treatment, passes through the appropriate comprehension of context and definition of scopes, in terms of objectives and decisions to be made, consequences of actions to be done, risk assessment methodologies and tools adopted, etc. By properly understanding context, the risk management policies are correctly located in the organisational context and risk arising from organisational factors could be prevented. Thus, the risk management process may be seen as an element of a complex system of relationships (the whole organisation).

The ECHO MAF **Multi-sector Implementation Tier** deploys two layers:

- The **ECHO Multi-sector layer**, identifying and isolating multi-sector aspects (not sector-dependent ones) which are common to two or more domains (possibly, not to all); the goal is to provide instruments to fulfil corresponding technology requirements by identifying a common foundation for multi-sector needs.

- The **ECHO Sector Specific layer** where the multi-sector approach will be complemented by the set of additional implementation features needed in order to fulfil the specific needs for a given sector. The sector specific implementation must face all specific needs of the possible sectors deploying the E-MAF. Within the aim of the ECHO project, doing this requires managing several possibilities, for example, when a sector shows to be sensible to:

    - transversal cybersecurity factors only (**Sector A**);
    - independent cybersecurity factors in addition to transversal ones (**Sector D**);
    - multi-sector cybersecurity factors in addition to transversal ones (**Sector B**);
    - multi-sector cybersecurity factors in addition to independent ones (**Sector C**);

    The last case is when a given sector does not introduce any specific need in terms of transversal, independent, multi-sector aspects. This could not happen since transversal and independent aspects should be present in all sectors. Unfortunately, a lack of knowledge in or a wrong assessment could lead to this situation (**Sector E**). This situation should be properly managed. Anyway, the layered architecture will be able to handle this option also.

The ECHO MAF **Security Alignment Tier** comprises the final two layers:

- The **ECHO Controls layer**, implementing the plenty of controls that *adequately mitigate* cyber *risks that the organization finds unacceptable and unavoidable need to be controlled* (ISO/IEC 27008: 2019) **[17]**. Cybersecurity controls should be “fit-for-purpose”. The controls will make reference to the whole Risk Management process and obviously implement all the actions referred to transversal, independent, multi-sector factor and sector-specific issues.

- The **ECHO Organisation Profiles layer** where Organizations will implement governance of their specific risks related to threats and vulnerabilities, and proper risk tolerance levels, which are different from ones related to other organizations as well as practices to achieve positive outcomes. As stated in the NIST Cyber Security Framework **[27]** documentation “*Profiles are an organization's unique alignment of their organizational requirements and objectives, risk appetite, and resources against the desired outcomes of the Framework Core. […] Profiles are about optimizing the Cybersecurity Framework to best serve the organization*”.

The overlaying of these three main components (tiers), the tight cooperation between their layers as well as the longitudinal and transversal interaction among the components (modules) are aimed at defining and implementing a full cybersecurity risk governance at hosting organisations by providing a huge added value through adoption of a multi-sector approach, definition of Curricula and Skills, and binding with Technology Roadmaps.

5.3 Logical Model for ECHO Risk Management

In addition to the architectural design, defining the modules the E-MAF comprises, it is necessary to describe what are the key functions and elements to be “targeted” by each of them in a coordinated way. In order to obtain this, the design of a **logical model** of the ECHO Multi-sector Assessment Framework is presented. Though it, two main goals are pursued:

1. to present the key factors and considerations in cyber risk assessment in their relationship; and
2. to make explicit the scope of E-MAF and the topics to be covered in the lifetime of the ECHO project.

E-MAF, like most of the existing frameworks and standards (e.g. MAGERIT**[20]**, ISO31000 **[18][19]**, ISO27005**[16]**, NIST 800-37**[25]**), goes beyond Risk Assessment *per se*, and supports *Risk Management* decision-making, i.e. it provides a framework for understanding cyber risks and, on that basis, supports decisions on where to invest human, technological and financial resources to reduce those risks to an acceptable degree.

Resource allocation decisions are most often taken at organisational level. However, E-MAF goes beyond the level of an individual organisation and will support Risk Management at sectoral level, cross- (aka inter-) and multi-sectoral level, national and pan-European levels. Towards a full understanding, it worth to recall the meaning in these pages of some key (and recurrent) terms.

'*Sectorial*' here may mean either a 'sector', as for example the 'Energy' sector defined in Directive 2008/114/EC **[71]**, or a 'sub-sector', e.g. 'Electricity' (including "infrastructures and facilities for generation and transmission of electricity in respect of supply electricity" **[71]**) or the 'Rail transport' sub-sector of the 'Transport' sector.

'*Cross-sectoral*' (also referred to as inter-sectoral in this deliverable) are resource allocation decisions taking into account cross-sector effects resulting from interdependencies between interconnected systems and infrastructures **[71]**. Among the examples here are the interdependencies between telecommunications and electricity distribution or the dependence of banking and financial services on the digital infrastructure.

'*Multi-sectoral*' are, on one hand, the cases accounting for interdependencies among three or more sectors and potential cascading effects of a cyberattack. On the other, multiple sectors can benefit from the application of a certain measure to reduce cyber risks. An example would be the institutionalization of an accredited training program providing cybersecurity competencies needed in several sectors. Such cases are designated below as 'transversal'.

Finally, E-MAF may be used at national and European Union levels in the elaboration of policies and measures aiming to reduce the cyber risks in the design and operation of Critical Infrastructures and the provision of essential services.

This scope of E-MAF is presented in the first row of Figure **20** below, followed by two groups of 'Risk Assessment' and 'Risk Mitigation' element, examined in the following sub-chapters. Issues listed in the cells with dark-gray background are considered in the initial version of E-MAF (starting with the first prototype, in August 2020), and those in cells with light-blue background in the further versions of the framework (starting from Y3, March 2021). Due to resource and time limitations, the issues in white cells will not be treated in detail during the lifetime of the ECHO project.

Coverage	Organisational	Sectoral	Cross-sectoral	Transversal	EU/national
Risk assessment					
Threats	Cyber threats	Cyber-Physical interdependencies		Natural hazards, industrial accidents, terrorist attacks	
Vulnerabilities	Hardware	Software	Networking	Organisation	
Impact	Negative consequences		Opportunities/ benefitsof risk mitigation measures		
Negative consequences	*Direct (physical, loss of information, financial)*	*Injuries,death, health & safety*	*Reputational*	*Lost opportunities*	*Social impact*
Risk estimation	Qualitative	Quantitative	Combination of Qualitative & Quantitative		
Risk mitigation					
Measures to enhance:	Awareness	Protection	Response and recovery	Resilience and adaptiveness	Prevention
Decisions on measures	Selective	Prioritisation	Optimisation		
Application	Ad-hoc	Recurring	Proactive (based on predictive analytics)		

Figure 20: The Logical Model of the ECHO Multi-sector Assessment Framework.

5.3.1 Risk Assessment

In the traditional understanding, reflected for example in ISO 27005**[16]**, risk is defined by the *likelihood of the occurrence of an unwanted event and the consequences that would follow from that event*. This understanding is directly incorporated for dealing with risk in some security fields, for example in capabilities-based planning methodologies and guidelines used in defense **[72]**, homeland security **[72][73]**, and the wider security sector **[74]**. Determination of risk of all these examples is based on a set of plausible, and agreed, scenarios[32], describing one or a series of interrelated events in their context. TOGAF also incorporates capability-based planning, and the use of business scenarios to discover and refine capability requirements **[30] [75]**.

The number of scenarios used in a planning cycle can range from fifteen in the case of the U.S. Department of Homeland Security **[73]** to several dozens. The use of scenarios is beneficial in representing uncertainty, providing transparency, and involving senior decision-makers. However, by itself, the process of elaborating and selecting a set of scenarios cannot guarantee *comprehensive* treatment of all risks, especially in a diverse, ill-defined and evolving field as cybersecurity **[76]**.

In a similarly diverse and evolving[33] field of disaster risk management, the assessment of risk covers natural and human-induced *hazards*, *exposure* of humans, infrastructure and ecosystems, systems' *vulnerability*, and the impact of a disaster **[77]**.

[32] The equivalent term used in ECHO would be 'use case'.
[33] To reflect, among others, climate change and recent sources of disasters such as terrorist acts.

"Hazard – exposure – vulnerability" is not the only structuring suitable for comprehensive treatment of risks. The risk assessment and treatment process in ISO 27001 **[15]** is based on "asset – threat – vulnerability" analysis **[13]**. ISO 27005 **[16]** further specifies that:

(1) the examination of an asset involves its valuation,
(2) the impact of an information security incident is estimated with account of direct and indirect, operational and future business effects from a full or partial loss of an asset, and
(3) in the first assessment (when no new security measures are considered) the estimate of an impact is very close to the value of the concern asset**[16]**.

A similar approach is also adopted in CYSM (Section **4.3.1**), MEDUSA (Section **4.3.2**), and MITIGATE (Section **4.3.3**) systems, where a valuable approach to SCSs take place along the corresponding projects.

This relation between a broadly defined asset value and the estimated impact, or consequence, of an incident allows to assess cybersecurity risk using the '**triplet**' of "threat – vulnerability – consequence" **[78]**. The same simple framework is used in related security fields, for example, in the risk analysis conducted by the U.S. Department of Homeland Security **[79]**. For these reasons, this is the structuring adopted in the E-MAF logical model.

5.3.2 Threats Identification

Threats can be classified in a number of ways, e.g. depending on the intent of the attacker (group of attackers), his or her knowledge and skills, selected targets, attack vectors, tactics, techniques and procedures, etc. **[80]**

At highest level, E-MAF distinguishes between three groups of threats:

1. cyber threats *per se*, e.g., threats of DDoS attacks, malware, social engineering, etc.;
2. threats as a result of cyber-physical interdependencies, e.g., power outage, disruption of communications (due for example to an electromagnetic storm), etc.; and
3. threats of physical destruction or disruption as a result of either deliberate actions (e.g. terrorism, warfighting, sabotage, vandalism, theft, traffic accidents) or unintentional (natural disasters, industrial accidents).

For more detailed classification of threats E-MAF builds on several sources:

- ENISA's Threat Taxonomy **[81]**;
- The classification of threats derived from D2.1 Scenarios **[1]**;
- Other existing Threat Taxonomies for the cyber security.

In the last group, two taxonomies were very interesting in the scope of ECHO project: the Agari Threat Taxonomy for cyber-attacks **[106]** and the Open Threat Taxonomy **[107]**.

Agari's classification system identifies types of cyber threats (a threat taxonomy) related to attacks conducted by email or other messaging services. They distinguish them by two main factors:

- how they are carried out, and
- the goal attackers want to achieve.

Agari approaches threat classification with the adoption of different perspectives. The classification begin with the attempt to identify the message either as malicious, spamming or as a grey mail element. Then the sender authenticity is inspected. When the sender is known, the next necessary step is to state whether he/she is

using either an imposter email account, a compromised address, or a temporary one. These two questions alone could be enough to describe common threads in an effective way. Additional dimensions details other useful but not fundamental information such as sender identity, recipient, delivery mode, and motivation.

Figure **21** depicts the general definition of the Agari Threat Taxonomy **[106]**.

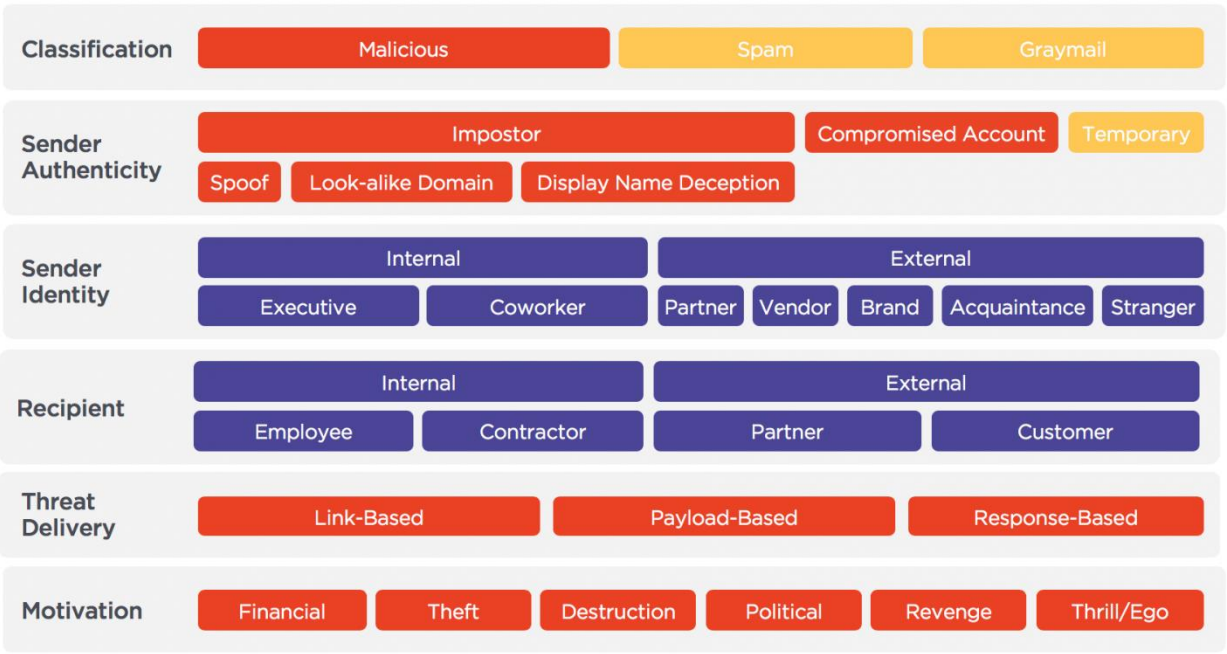

Figure 21: General definition of the Agari Threat Taxonomy [106].

The Open Threat Taxonomy has been defined with the contribution of 150 organisation, belonging to diverse domains (NATO, International Governments, US Department of Defence, US Federal Agencies, Banks, Healthcare, Energy, Industry, University and Education, Internet Security, etc.), and aims to create a general purpose threat taxonomy for Information Systems, with the secondary goal to demonstrate that is not true that every industry/organisation needs its own specific taxonomy. This is the same goal ECHO move towards: setting up a threat taxonomy for the whole ECHO universe: whoever uses a given asset is subjected to the same threats, regardless of the type of organisation or industry.

As described in **[107]**, threats have been divided into four categories:

- Physical: *threats to the confidentiality, integrity, or availability of information systems that are physical in nature. These threats generally describe actions that could lead to the theft, harm, or destruction of information systems.*
- Resource: *threats to the confidentiality, integrity, or availability of information systems that are the result of a lack of resources required by the information system. These threats often cause failures of information systems through a disruption of resources required for operations.*
- Personnel: *threats to the confidentiality, integrity, or availability of information systems that are the result of failures or actions performed by an organization's personnel. These threats can be the result of deliberate or accidental actions that cause harm to information systems.*
- Technical: *threats to the confidentiality, integrity, or availability of information systems that are technical in nature. These threats are most often considered when identifying threats and constitute the technical actions performed by a threat actor that can cause harm to an information system.*

For each of these categories, a detailed list of threats is provided as well as a specific rating for all of them. Even the rating does not matches with the approach ECHO depicts for estimation activities, this taxonomy represented a good starting point.

The ECHO E-MAF cyber threat identification plans also to exploit outcomes of MITIGATE and CS-AWARE projects. In both of them, information on threats are retrieved from social media and existing sources/repositories and contribute to the creation of a dynamic taxonomy of threats.

ECHO activated a task force for the definition of Taxonomies (and Vocabularies), Ranges and Scales which are key elements for the global interoperation of all products of ECHO ecosystem. The ECHO Threat Taxonomy is not yet finalized at the time of this writing. The E-MAF prototype is designed to be easily tuned on taxonomy updates which are planned to be periodically updated along the project lifetime.

5.3.3 Vulnerabilities Identification

Cyber vulnerabilities can also be classified in a number of ways. For example, ENISA, reflecting on the 1998 report by John Howard and Thomas Longstaff of Sandia National Laboratories, considers *design*, *implementation*, and *configuration* vulnerabilities **[82]**.

More focused studies, e.g. on cybersecurity of in the context of Industry 4.0 **[83]**, distinguish vulnerabilities related to:

- Operating systems or firmware;
- Application software;
- Industrial communication protocols; and
- Smart devices (embedded sensors and actuators).

In the ECHO project, in compliance with D2.4 **[3]**, D2.5 **[4]**, and D2.6 **[5]** as well as to provide for compatibility with other activities, e.g. the development of the cyber skills framework, E-MAF implements a vulnerability taxonomy including four main groups:

1. ***Hardware-related vulnerabilities***, e.g. use of unencrypted personal devices;
2. ***Software-related vulnerabilities***, e.g. use of unpatched operations systems and applications;
3. ***Networking vulnerabilities***, e.g. related to the use of Wi-Fi, VPNs, remote access;
4. ***Organisation-related vulnerabilities***, e.g. related to skills and level of awareness of personnel, business processes on cyber threats, timing.

In vein with this, Figure **22** shows the vulnerability taxonomy categories and subcategories as currently depicted by ECHO E-MAF after analysis of StoryLines in D2.1 **[1]**.

ECHO activated a task force for the definition of Taxonomies (and Vocabularies), Ranges and Scales which are key elements for the global interoperation of all products of ECHO ecosystem. The ECHO Vulnerability Taxonomy is not yet finalized at the time of this writing. The E-MAF prototype is designed to be easily tuned on taxonomy updates which are planned to be periodically updated along the project lifetime.

1.Organisational	2.Software	3.Hardware	4.Network
1.1 Staff Awaireness and Training	2.1 Off-the-shelf Software vulnerabilities	3.1 Unencrypted personal devices	4.1 Internet or radio connections
1.2 Staff credentials/logins release process	2.2 Proprietary Software vulnerabilities	3.2 Connected devices vulnerable to remote access (Hv	4.2 SAT connections
1.3 Weak Password and Security policies	2.3 Unpatched Software and OS	3.3 Main and auxiliary system driving operation (Hw)	4.3 Wi-Fi, VPN, Remote Access
1.4 Weak or absent Security Monitoring	2.4 Misconfigurations or Default Password issues	3.4 SCADA supplier systems. HMIs and servers	4.4 Lack of Network Segregation
1.5 Security acquisition and provisining policies	2.5 Connected devices vulnerable to remote access (Sw)	3.5 Shared software modules among devices (Hw)	4.5 Lack of Network Segmentation
1.6 Compliance requirements for 3rd party supplie	2.6 Main and auxiliary systems driving operation (Sw)	3.6 Malicious Firmware	4.6 Wi-Fi dongles and cards
1.7 Slow or absent security patching cycles	2.7 Supplier Systems Software	3.7 Hardware Maintenance Errors	4.7 Open-source components
1.8 Unsecure Protocols	2.8 Lack of Software System Segregation		4.8 Shared Topology
1.9 Design deficiencies/flaw	2.9 Lack of "Security by Design"		4.9 Data Encryption
1.10 Knowledge of Infrastructure and Assets	2.10 Shared software modules among devices (Sw)		4.10 Network Management Policies
1.11 Shared Infrastructure and Assets	2.11 Cross-site scripting and forgery		4.11 Network Maintenance Errors
1.12 Untrusted information for decision-making	2.12 Software Maintenance Errors		
1.13 Timing in servicing			

Figure 22: ECHO E-MAF Vulnerability Taxonomy.

5.3.4 Consequences

In the traditional understanding, risk is equated to the "chance or probability of loss". This focus on 'loss' is reflected, for example, in ISO/IEC 27005:2008 **[16]** which examines the negative impact of an information security incident. Since its 2009 version, ISO 31000 **[18][19]** defines risk as "*effect of uncertainty on objectives*" allowing thus to consider negative as well as positive consequences of uncertainty.

Respectively, the E-MAF logical model examines two main groups of consequences:

1. ***Negative consequences***;
2. **Positive consequences** in terms of opportunities and benefits of risk mitigation measures, e.g. higher general competences of personnel that has undergone cybersecurity training or new business opportunities resulting from investments in the development and/or implementation of a certain cybersecurity technology.

A negative consequence may result from a damaged or fully destroyed device, loss of data or communications and lead to reduced effectiveness, adverse operating conditions, loss of business, reputation, etc. **[16]**. Without making a claim for comprehensiveness, ISO 27005 **[16]** recommends to consider operational consequences of incident scenarios in terms of:

- *Investigation and repair time;*
- *(Work)time lost;*
- *Opportunity lost;*
- *Health and Safety*
- *Financial cost of specific skills to repair the damage;*
- *Image reputation and goodwill***[16]**.

The E-MAF logical model implements the following high-level classification of negative consequences:

- *Direct consequences, including physical damage, loss of data and information, disrupted business process, and short-term financial losses;*
- *Injuries, death, health and safety;*
- *Reputational damage;*
- *Lost business opportunities;*

*Social impact, e.g. disruption to people's daily lives, widespread anxiety or loss of confidence in online services or technology more generally***[84]**.

5.3.5 Risk Estimation

Depending on the available information and capacity, the estimation of both likelihood of a cybersecurity incident and its consequences may be qualitative, quantitative, or through a combination of the two **[18][19]**. This is also the classification of approaches and methods to risk estimation adopted in the E-MAF logical model.

In qualitative terms, the consequences of an incident are estimated using a scale of qualitative attributes. In its simplest form, the scale includes 'Low,' 'Medium,' and 'High'. The same scale may be used to assess the likelihood of occurrence of those consequences. ISO/IEC 27005 **[16, p. 50]** provides an example of the use of five-degree scales and how qualitative estimates can be transformed into numbers.

Related security fields (e.g. in the development of the national security strategy of The Netherlands **[85]**) provide relevant examples of use of other scales of qualitative indicators:

- 'very rare,' 'rare,' 'unlikely,' 'possible,' 'probable' in estimating likelihood; and
- 'insignificant,' 'minor,' 'moderate,' 'significant,' 'catastrophic' in estimating impact.

Often qualitative estimation is used first to identify major risks and obtain a general indication of the level of risk **[16]**. The reliance on qualitative estimates is unavoidable if historical data or data from rigorous modelling of events and their impact is lacking.

Quantitative estimation may include estimates of the probability or a frequency of cybersecurity incidents over a given time period and assessments of the actual impact of such incidents, preferably based on verified historical records. Other source of information that can be used for quantitative estimates are the cybersecurity exercises and the results of rigorous modelling. In some cases, one can use statistical approaches and methods, e.g. the Delphi method[34], to process expert opinions and derive quantitative data.

While adding rigor and transparency to risk management, the accuracy of quantitative estimates depends on the completeness and reliability of historical data and models. When models are not validated, or historical incident data incomplete or unreliable, the quantitative approach may create an illusion of worth and accuracy of the risk assessment**[16]**.

E-MAF provides estimates through a combination of qualitative and quantitative methods. With the accumulation of experience and data, these opportunities will grow, allowing for example a combination of qualitative scorecard assessment to determine the level of cyber risk exposure and a Bayesian network to model the financial loss of cyber incidents **[86]**.

E-MAF examines relevant aspects of the "risk mitigation" activity, described as part of "risk assessment" in ISO 31000 **[18] [19]** and ISO 27005 **[16]**, in the following sub-section.

5.3.6 Risk mitigation

"Risk mitigation" is one of the synonyms of the "Risk treatment" activity – a term used in ISO 31000 **[18] [19]** and ISO 27005**[16]**. "Risk mitigation" is preferred as it already denotes a broad variety of strategies and measures that can be used to reduce cyber risks. Just as "risk treatment", this term allows the recommendations in ISO 31000 **[18] [19]** to be taken into account by:

- *avoiding the risk by discontinuing or not starting the risk generating activity;*
- *taking or increasing risk in order to pursue an opportunity;*
- *removing the source of risk;*
- *changing the likelihood of occurrence;*
- *taking measures to reduce the consequences;*
- *sharing the risk with another party or parties (including contracts and risk financing)[35];*
- *taking an informed decision to retain the risk***[18] [19]**.

Longer-term measures such as developing training programmes or new risk mitigation technologies and solutions are to be taken into consideration too.

[34] https://www.rand.org/topics/delphi-method.html

[35] ISO 27005 emphasises "risk transfer" to another party, e.g. by insurance.

Measures

The above list may be used as a starting point to design a taxonomy for cyber risk reduction measures.

E-MAF however adopts a structure of existing and potential risk reduction measures with five main groups of measures aiming respectively to:

- increase *awareness* of policy makers, staff or wider society on cyber risks;
- enhancing the *protection* of assets and systems, including by remedying identified vulnerabilities and reducing exposure to cyberattacks;
- strengthening the capacity for *response and recovery*, e.g. by increasing the use of predictive analytics to enhance agility in responding to incidents **[87]**;
- enhancing *resilience and adaptiveness*, e.g. through collaboration **[88]**, design measures such as compartmentalization of information systems and networks, redundancy and diversification **[89]**, organizational agility allowing to adapt quickly to changing circumstances **[90]**;
- *preventing* the realization of cyber threats by deterrence **[91]**, performing active defensive functions in cyberspace **[91]** or other measures.

Decisions on measures to be implemented

Decisions on what strategies and measures to apply to reduce cyber risk can be taken by:

1. focusing *selectively* on one or a small number of issues, usually related to high-visibility cases on the attention of decision makers, for example a recent, high-impact attack in the same industry sector **[93]**;
2. prioritization among competing demands, e.g. on the basis of prioritized gap analysis **[94]**;
3. optimisation of already available ones, e.g. by increasing efficacy or performances.

Applicable ISO standards recommend at least prioritization of risks and measures (controls); yet, option 1 may be the only available option for the elaboration of policies common for a given sector or a number of interdependent sectors.

Any of these options requires an understanding of the costs and benefits of the application of risk reduction measures. Decisions in options 2 and 3 are set in a resource constraint framework, and require the use of an agreed number of risk evaluation criteria, against which to compare potential risk mitigation measures.

Application of measures

ISO 27005 recommends to conduct Risk Assessment and take respective risk mitigation decisions in two or more iterations: first, to carry out a high-level assessment to identify potentially high risks that justify further assessment; and then to conduct in-depth analysis, possibly using a different method**[16]**.

The cycle may include monitoring the implementation of risk mitigation measures and incorporation of lessons learned on the results and performance of measures implemented in previous cycles**[77]**.

This whole iterative cycle may be applied *ad-hoc*, on a *recurring* basis, or *proactively* to meet foreseen risks. These are the three respective fields in the E-MAF logical model.

Ad-hoc is the application carried out the first time an organisation decides to certify it according to one or more relevant standards. This decision may be based on organisational strategy, newly introduced legislative requirements, or may be triggered by a high-impact cyber incident involving the organisation itself or other

organisations in the same sector or using similar technologies. At least initially, ad-hoc would be the application on sectoral or multi-sectoral level.

Recurring is the application carried out when a company, a sectoral or inter-sectoral network of organisations have procedures in place to conduct risk assessment regularly or upon considerable changes in the risk management environment, e.g. in the wake of an attack with sizeable consequences, a new significant threat or the discovery of a crucial vulnerability.

Proactive is the application carried out when the organisation has a predictive analytics system in place. Predictions may be based on time series analysis **[95]**, dynamic real-time probabilistic risk data and cyber risk analysis **[96]** and other methods, applying Artificial Intelligence, Machine Learning approaches and techniques.

5.3.7 Implementation of the E-MAF Logical Model

Unlike most of the existing frameworks and standards, E-MAF covers not only the needs of a single organisation, but also of parties that are interested in sectoral, multi-sectoral, national, and even multinational (e.g. European Union) level. These may be sectoral or cross-sectoral associations, national governments or EU agencies concerned with the provision of cybersecurity.

The logical model of the framework is sufficiently broad to account for known historical events, threats and vulnerabilities, but also for future threats and vulnerabilities, e.g. new attack surfaces as a result of the proliferation of IoT devices **[97]** or potential emergent behavior in meshed 'systems-of-systems' **[98]**.

The comprehensiveness of the framework provides flexibility to select both threats, assets, and interdependencies to be accounted for in a risk management cycle, while the use of scenarios remains the state-of-the-art approach in risk assessment and planning aiming to optimise risk **[99]**. That includes the design of scenarios and use cases in the ECHO research, and adding new scenarios throughout the life of the project.

A very interesting aspect will be the coordinated manipulation of information among the different layers and modules involved in the determination of the global risk levels and also in intermediate ones (e.g. level related to specific transversal issues, etc.). The different elements of E-MAF put in place a cooperative model through a « set and get » activity set in order to tune values from the several PoVs the different layers have on the risk posture for a given organisation. The shared information propagates values among layers and modules as a sort of shared memory model (e.g. like global variables or parameter passing). This mechanism can be improved by plugging a different sharing model depending on further implementation choices

	ECHO Transversal Fundation Tier				ECHO Multi-sector Implementation Tier		ECHO Security Alignment Tier	
	Risk Management FW				Multi Sector Layer	Sector Specific Layer	Controls Layer	Organisation Profiles Layer
	RA FW			RM Ext Layer				
	Basic	Transv Layer	Independ. Layer					
Coverage								
Organisational			✓					✓
Sectoral	✓	✓		✓		✓	✓	
Cross-Sectoral	✓	✓	✓	✓	✓		✓	
Transversal	✓	✓		✓				
Risk Assessment								
Threats								
Cyber threats	✓	✓		✓	✓	✓	✓	✓
Cyber-Physiscal Interdep.	✓	✓		✓	✓	✓		✓
Vulnerabilities								
Hardware	✓	✓			✓	✓		
Software	✓	✓			✓	✓		
Organisational	✓		✓		✓	✓		
Network	✓	✓			✓	✓		
Impact								
Negative Consequencies	✓	✓	✓	✓	✓	✓	✓	✓
Opportunities + benefits	✓	✓	✓	✓	✓	✓	✓	✓
Risk Estimation								
Qualitative	✓	✓	✓		✓	✓		✓
Quantitative	✓	✓	✓		✓	✓		✓
Combination of former	✓	✓	✓		✓	✓		✓
Risk Mitigation								
Measures to Enhance								
Awareness	✓	✓	✓	✓	✓	✓		
Protection				✓	✓	✓	✓	✓
Decision on measures								
Selective/subjective				✓	✓	✓		
Prioritisation				✓	✓	✓		
Process								
Ad-hoc					✓	✓		✓
Iterative					✓	✓		✓

Table 27: Sharing of information between elements of E-MAF.

Table **27** shows the cooperation and interaction process between layers and modules in E-MAF through information sharing.

5.4 Delivery of E-MAF

As described in the previous sections, E-MAF is inspired by several important experiences (methodologies, methods, approaches, and projects) which have addressed the extremely challenging goal to innovate and enhance Risk Assessment and Management. In addition to this, E-MAF faces multi-domain services and for this reason, its architecture must be flexible and scalable by design.

The ECHO T2.2 activities have to face several challenges as depicted in [GA] in an effective and efficient manner addressing several goals which a flexible approach which could be fast in adapting to the several innovative outcomes continuously produced by the project. For this reason, the architectural design activities approached the problem to design E-MAF in a way it could be easy to implement and demonstrate, still maintaining the chance to implement the Framework as an innovative software tool. A very valuable inspiration comes from the approach based on the three tier architecture deployed by CYSM (**Section 4.3.1**), and then improved by MEDUSA (**Section 4.3.2**) and MITIGATE (**Section 4.3.3**) projects in order to operate in a cross-domain environment.

Since the ECHO approach is directed towards a methodological innovation, in addition to technological implementation, the division in tiers is devoted to isolate and manage the different elements contributing to the system on the point of view of the cross-sector (inter-) and multi-sector application and not from the service point of view. This is demonstrated by the Architectural Design depicted in **Section 5.2**.

The main goal is to demonstrate that a different, more innovative methodological approach could lead to the highlighting of inter- and multi-sector issues, with a global improvement of effectiveness for all players (business partners), and simultaneously to an efficient risk mitigation/governance. In order to get the methodology validated and facilitate the use of E-MAF as an input to other ECHO WPs and tasks, it is necessary to provide a fast implementation of the framework and foster its adoption to several scenarios, starting from the ones defined in D2.1 **[1]**. In addition to this, in ECHO WP2 also the technological enhancement in terms of innovative multi-sector Frameworks for RA and RM is planned to be investigated, in line with time constraints and availability of effort.

For this reason, the E-MAF prototypes do and will exploit a general architecture allowing them to be delivered in two different formats:

- as an Excel file enabling fast, efficient and effective implementation and deployment of RA and RM in the involved organisations;
- as a software tool possibly developed in WP2 or WP4, to be inspired to the abovementioned implementations (web services, java portlet, containers, JSR 168 and 286 standards, etc.).

Both “models” allow to put in place consolidated features of software development like *inheritance*[36] and *polymorphism*[37] in this field by mimicking this from usual “object oriented” programming (OOP) methodologies.

[36] Inheritance implies the capability for an object (a class) in OOP to inherit features (meaning attributes and methods) from another object (class).

[37] The term ‘polymorphism’ means "many forms”; it occurs when classes relate to each other by inheritance. Polymorphism uses those methods to perform different task, a single action in different ways.

The concepts being the pillars enable security service mapping at organisational level to be meant as a typical verticalization of software, e.g. classes in a Java environment. With the idea of an open source community, organisations could exchange improvements and localisation of RA and RM implementations with an enormous impact on RM activities and security levels.

In short, the first prototypes of E-MAF will be distributed as a Microsoft Excel file where different elements of the architecture will contribute to the global risk estimation by following the methodology (the logical model) depicted in the previous section. The advantage provided by this format lays in the immediate availability of the framework for internal deployment, as stated above, and also in the promptness by which the implementation could respond to change requests, extensions, and anomalies.

In the next months, thanks to engagement of new partners in ECHO and to the exploitation of the remaining effort on T2.2, a software tool implementation activity will be evaluated and eventually planned.

As usual, the users will be the domain experts, who will have to face and answer questions implementing the security controls. They will express personal estimation of the necessary elements to implement the Risk Assessment, as depicted in the previous sections and in the ECHO E-MAF logical model. The user will not be required to have any particular expertise on cross-sectoral issues, as the system will be configured to provide automatic support for interrelationships, regardless of whether they are interconnections or interdependencies.

In fact, the ultimate goal of E-MAF is to strongly improve RA by introducing no additional requirements (in terms of expertise) on extra-domain aspects of our experts. Introducing such a gain in cyber risk assessment will put in place an amplifying effect in risk governance, where the target security level could be reached with the minimum effort possible from organisation.

The E-MAF tool by design comprises a set of fourteen Excel sheets, namely the **E-MAF Analytical Model**, each one of them deals with a specific aspect of Multi-tiered Architectural Design in Section **5.2**Error! Reference source not found.. In particular within the E-MAF Analytical Model we can identify 4 groups of Excel sheets:

- **ECHO TFT RA Framework Layer;**
- **ECHO MIT Layer;**
- **ECHO SAT Layer;**
- **ECHO TFT RM Framework Layer.**

The **ECHO TFT RA Framework Layer** sheets include:

- The **ECHO MAF Main** sheet, representing the access and main page of the tools and its results and belonging to ECHO TFT RA Framework General Module. It defines the organisation main information and enables selection of the sector the organisation belong to. Also results of global, local or partial risk level determination will be presented here. The selection of the sector makes the remaining sheets update and adapt correspondingly.
- The **Configuration** sheet, where configuration of operational parameter and formulas takes place. It enlists the categories of controls available in the E-MAF and couples them with corresponding taxonomies, ranges, and scales. It belongs to ECHO TFT RA Framework General Module.
- The **Taxonomies** sheet enlisting the adopted taxonomies. The taxonomies and vocabularies will be presented here (threats, vulnerabilities, consequences, etc.). This sheet is part of ECHO TFT RA Framework General Module as well.
- The **Ranges and Scales** sheet defining Ranges and Scales adopted in E-MAF and whose values are accepted by the tool. It is part of ECHO TFT RA Framework General Module.
- The **Independent** issues sheet, related to independent aspects and providing the estimates related to them. Even they are not related to technological aspects, the sheet is included for completeness. It currently builds the ECHO TFT Independent Module.

- The **Transversal** issues sheet, managing transversal aspects. It defines and enlists the set of transversal aspects to analyse and the estimates related to them. It is currently the only component of the ECHO TFT Transversal Module.

The **ECHO MIT Layer** sheets set comprises:

- The **Cross-Sector** sheet, presenting the Multi-Sector and Inter-Sector aspects and allowing to ingest the related estimates. It builds the ECHO MIT Multi-Sector Layer.
- The **Sector-Specific** sheet dealing with the sector-specific aspects and estimating them. It is the only component of ECHO MIT Sector Specific Layer.

The **ECHO SAT Layer** is composed by:

- The **ECHO Security Controls** sheet, containing the set of security controls to identify and evaluate the Risk Posture. It belongs to the ECHO SAT Security Controls Layer.
- The **Organisational Controls** sheet, showing the additional controls from Organisational Profile. The list of organisation specific controls is used for tuning the Risk Posture further. This sheet builds the ECHO SAT Organisation Profile Layer and together with the previous one makes the ECHO SAT Layer.

The final set of sheet provides the **ECHO TFT RM Framework Layer** comprising:

- The **Risk Management** sheet enlisting Risk Management elements dealing with the aspects related to Context Analysis, Risk Treatment, Monitoring and Review functions. This sheet composes the ECHO TFT RM Extension Layer.
- The **Governance Measures** sheet containing the definition of Risk Governance Measures in the aim of the ECHO TFT RM Framework General Module.

The E-MAF also requires **auxiliary additional sheets**, e.g.:

- The **Parameters** sheet, hiding with operational and management parameters definition and respective value calculations as well as enabling the “watch” feature during troubleshooting.
- The **Formulas** sheet, hiding formulas definition and calculations. It can be used to enable the “watch” feature during troubleshooting.

Table 28 summarizes the set of Excel sheets in the E-MAF, while **Figure 23** shows the information sharing model among them.

	Name	Mapping E-MAF Module	#	Information Sharing Map													
Source	ECHO MAF Main	ECHO TFT RA Framework General	1	■	•	•	•	•	•	•	•	•	•	•	•	•	•
	Configuration	ECHO TFT RA Framework General	2		■	•	•	•	•	•	•	•	•	•	•	•	•
	Taxonomies	ECHO TFT RA Framework General	3			■	•	•	•	•	•	•	•	•	•		
	Ranges and Scales	ECHO TFT RA Framework General	4				■		•	•	•	•	•	•	•	•	•
	Independent	ECHO TFT Independent Module	5	•				■				•	•	•	•		
	Transversal	ECHO TFT Transversal Module	6	•					■			•	•	•	•		
	Cross-Sector	ECHO MIT Multi-Sector Layer	7	•						■		•	•	•	•		
	Sector Specific	ECHO MIT Sector Specific Layer	8	•							■	•	•	•	•		
	ECHO Security Controls	ECHO SAT Security Control Layer	9	•								■	•	•	•		
	Organisational Controls	ECHO SAT Organisation Profile Layer	10	•									■	•	•	•	•
	Risk Management	ECHO TFT RM Extension Layer	11	•										■	•	•	•
	Governance Measures	ECHO TFT RM Framework General	12	•											■		
	Parameters	N/A	13	•	•	•	•	•	•	•	•	•	•	•	•	■	
	Formulas	N/A	14	•	•	•	•	•	•	•	•	•	•	•	•	•	■
					1	2	3	4	5	6	7	8	9	10	11	12	13	14
					Destination													

Figure 23: Information sharing process between the elements of E-MAF Analytical Model.

#	Sheet Name	Short Description	Content	Mapping E-MAF Element	Visible
1	ECHO MAF Main	Main page and results.	Definition of Organisation and Sector. Results of global, local or partial risk levels calculation. The selection of sector will make the remaining sheets adapt correspondingly.	ECHO TFT RA Framework General	Yes
2	Configuration	Operation params and formulas configuration.	Types of controls will be coupled with corresponding taxonomies, ranges, and scales.	ECHO TFT RA Framework General	Yes
3	Taxonomies	Enlists the taxonomies.	The taxonomies and vocabularies will be presented here (threats, vulnerabilities, consequences, etc.).	ECHO TFT RA Framework General	No
4	Ranges and Scales	Defines Ranges and Scales accepted.	Definition of accepted types of Ranges and Scales.	ECHO TFT RA Framework General	No
5	Independent	Independent aspects.	The set of independent aspects and related estimates.	ECHO TFT Independent Module	Yes
6	Transversal	Transversal aspects.	The set of transversal aspects and related estimates.	ECHO TFT Transversal Module	Yes
7	Cross-Sector	Multi-/Inter-Sector issues.	The set of cross-sector aspects and estimates related.	ECHO MIT Multi-Sector Layer	Yes
8	Sector Specific	Sector-Specific aspects.	The set of sector-specific aspects and related estimates.	ECHO MIT Sector Specific Layer	Yes
9	ECHO Security Controls	ECHO Security Controls.	The list of security controls to identify and evaluate the Risk Posture.	ECHO SAT Security Control Layer	Yes
10	Organisational Controls	Additional Controls from Organisation.	The list of organisation specific controls to finetune the Risk Posture.	ECHO SAT Organisation Profile Layer	Yes
11	Risk Management	Risk Management elements.	The aspects related Context Analysis, Risk treatment, Monitoring and Review.	ECHO TFT RM Extension Layer	Yes
12	Governance	Governance Measures.	Definition of Risk Governance Measures.	ECHO TFT RM Framework General	Yes
13	Parameters	Operational parameters definition and watch.	Auxiliary sheet hiding parameters management. It can be used to add watch features during troubleshooting.	N/A	No
14	Formulas	Formulas definition, calculation and Watch.	Auxiliary sheet hiding formulas management. It can be used to add watch feature during troubleshooting.	N/A	No

Table 28: Example structure of the E-MAF Analytical Model.

5.5 E-MAF Taxonomy

A *Taxonomy* is a scheme (or an 'instrument') of classification. It is aimed to knowledge organization and establishes and maintains a set of terms (words) that have been organized to regulate and control their use within a given subject field. Those terms are put in a *Vocabulary*, offering necessary features to store and retrieve its items from an internal repository. A Taxonomy, as a specific implementation of a Knowledge Organization System (KOS), is usually specific to a topic, knowledge domain, subject, or enterprise area.In the case of E-MAF, it classifies information, assets, events (e.g. cyberattacks), impacts, threats, vulnerabilities, etc. in the aim of the multi-domain cybersecurity.

Cybersecurity is an interdisciplinary domain, and this is reflected in the ECHO project and the design of E-MAF. So, one of the problems is the use of cybersecurity terms in different sectors, but also methodologies and standards with different meaning. Therefore the purpose of this section is to define a set of common definitions of the cyber security terms that will be used in a coherent manner by the E-MAF, but also in the description of the use cases in D2.1 **[1]** and the other ECHO deliverables across all sectors. The definitions are distinguished in:

- Taxonomy: catalogue of assets, threat (event), threat actors, vulnerabilities, and any other item concurring to the performance of the risk assessment;
- Vocabulary: definition of security key words used in ECHO;
- Semantics: semantics of cybersecurity related challenge activities (such as threat, crime, and attack), physical sectoral scenarios and specific contexts, aimed to find transversal and inter-sector needs as well as requirements (Section **5.5.3**).

The E-MAF Taxonomy strongly relates with the work performed by the Taxonomy, Scales and Ranges task force whose products are periodically merged with the Taxonomy presented in the following sections. It also accepts and integrates choices specifically made in the aim of E-MAF activities in terms of Threats, Vulnerabilities, Consequences taxonomies, as well as scales and ranges for estimates.

5.5.1 ECHO Cybersecurity Framework Taxonomy

In the last years JRC provided a high level set of definitions and a categorisation of domains that are proposed so that they can be:

- used by the EC cybersecurity initiatives;
- referred by cybersecurity activities (operation, training, education, …) in all sectors (including ECHO ones);
- used to index the cybersecurity research entities;
- compliant with international cybersecurity standards;
- sustainable, easily modifiable and extensible.

These are the key reasons why ECHO has chosen, for the beginning of the project, to adopt European Cybersecurity Centers of Expertise Map JRC Technical Report, Definitions and Taxonomy v.1 (2018) **[51]** as the main reference and source for its own taxonomy and definitions. Later, the JRC Technical Report v.2**[108]** has been released,so the ECHO vocabulary and taxonomy have been adjusted in compliance with the latter version.

Since the classification of concepts or things may vary when classification principles change, it is commonly agreed that there is a no uniquely valid taxonomy for a specific domain. It must be also understood that a given taxonomy can represent its domain more or less effectively depending on the context.

In consideration of the fact that the multi-sectoral approach followed by ECHO officially refers to the selected domains (Healthcare, Energy, Maritime, Defense and Space) but the approach is devoted to a full multi-sectorial landscape, all the elements of the JRC taxonomy are kept. In the following the sectors and subsectors written in black color are the ones included in the current four-domain multi-sector implementation. The remaining ones, written in grey color, are the ones complementing the whole taxonomy. As the JRC one, the ECHO Taxonomy collects numbers of existing concepts and terminologies to define a new cyber security taxonomy which is:

- unifying,
- holistic and
- forward-looking.

The traditional approach to the definition of a taxonomy follows a number of well-defined steps. The reader could refer to **[2]** for a more detailed description of these steps. The following pages list sectors and subsectors proposed for ECHO cybersecurity taxonomy.

ED.01 - Defense	ED.02 - Digital Infrastructure	ED.03 - Energy
ED.01.01 - Aeronautics;	ED.02.01 - IXPs;	ED.03.01 - Electricity;
ED.01.02 - Space;	ED.02.02 - Domain Name Service (DNS) providers;	ED.03.02 - Distribution system operators;
ED.01.03 - Electronics;	ED.02.03 - Top Level Domain (TLD) name registries;	ED.03.03 - Transmission system operators;
ED.01.04 - Land systems;	ED.02.04 - Telecomm Infrastructures.	ED.03.04 - Energy Production Operators;
ED.01.05 - Telecommunications;		ED.03.05 - Energy prosumers;
ED.01.06 - Shipbuilding;		ED.03.06 - Energy Third party services;
ED.01.07 - Cyber defense;		ED.03.07 - Smart meters and equipment;
ED.01.08 - Dual-use cybersecurity technologies;		ED.03.08 - Energy Critical Information Infrastructures (Energy CIIs);
ED.01.09 - Critical Information Infrastructures (CIIs).		ED.03.09 - Oil;
		ED.03.10 - Operators of oil transmission pipelines;
		ED.03.11 - Operators of oil production;
		ED.03.12 - Refining and treatment facilities, storage and transmission;
		ED.03.13 - Gas;
		ED.03.14 - Distribution system;
		ED.03.15 - Transmission system operators;
		ED.03.16 - Storage system operators;

ED.01 - Defense	ED.02 - Digital Infrastructure	ED.03 - Energy
		ED.03.17 - LNG system operators and services;
		ED.03.18 - Natural gas undertakings;
		ED.03.19 - Operators of natural gas refining and treatment facilities;
		ED.03.20 - Green Energy.
ED.04 - Government and public authorities	**ED.05 - Health**	**ED.06 - Maritime**
ED.04.01 - Data collection;	ED.05.01 - Health care settings (including hospitals and private clinics);	ED.06.01 - Surveillance services;
ED.04.02 - e-Government systems and services;	ED.05.02 - Healthcare supply chain;	ED.06.02 - Border control services;
ED.04.03 - Law enforcement;	ED.05.03 - Medical devices industrial sector;	ED.06.03 - Environmental protection;
ED.04.04 - Governmental Critical Information Infrastructures (Gov CIIs).	ED.05.04 - Pharmaceutical industry;	ED.06.04 - Fisheries;
	ED.05.05 - Evaluation and Management Coding in Health (E/M Health);	ED.06.05 - Port Authorities
	ED.05.06 - Health Critical Information Infrastructure (HC CIIs).	ED.06.06 - Port services;
		ED.06.07 - Maritime supply chains.
ED.07 - Smart Ecosystems	**ED.08 - Space**	**ED.09 - Supply Chain**
ED.07.01 - Smart infrastructures (like Industry 4.0);	ED.08.01 - Space industry;	ED.09.01 - Natural resources;
ED.07.02 - Smart cities, vehicles, infrastructures, objects;	ED.08.02 - Satellite operators, including ground based stations;	ED.09.02 - Raw materials;
ED.07.03 - Smart environments;	ED.08.03 - Positioning and timing information;	ED.09.03 - Components;
ED.07.04 - Smart governance;	ED.08.04 - Navigation services;	ED.09.04 - Retails.
ED.07.05 - Smart energy;	ED.08.05 - Earth observation;	
ED.07.06 - Smart Networks (like Home Networks).	ED.08.06 - Satellite data providers, including data storage.	

Table 29: Sectors and subsectors proposed for ECHO Cybersecurity Taxonomy.

Here follows the complementary set of sectors and sub-sectors for future use:

ED.10 - Audiovisual and media	ED.11 - Financial	ED.12 - Nuclear
ED.10.01 - Broadcasting;	ED.11.01 - Credit institutions;	ED.12.01 - Radiation protection;

ED.10 - Audiovisual and media	ED.11 - Financial	ED.12 - Nuclear
ED.10.02 - Publishing;	ED.11.02 - Operators of trading venues;	ED.12.02 - Transport of radioactive substances and waste;
ED.10.03 - Internet.	ED.11.03 - Central counterparties (CCPs);	ED.12.03 - Waste management;
	ED.11.04 - Banking services;	ED.12.04 - Safeguarding nuclear materials;
	ED.11.05 - Insurance services;	ED.12.05 - Safety of nuclear installations;
	ED.11.06 - Financial Critical Information Infrastructure (Fin CIIs);	ED.12.06 - Nuclear research and training activities.
	ED.11.07 - Brokerage services.	
ED.13 - Public Safety	**ED.14 - Tourism**	**ED.15 - Transportation**
ED.13.01 - Fire services;	ED.14.01 - Accommodation;	ED.15.01 - Air transport;
ED.13.02 - Rescue services;	ED.14.02 - Food and Beverage Services;	ED.15.02 - Air carriers;
ED.13.03 - Medical services;	ED.14.03 - Recreation and Entertainment Infrastructures and Services;	ED.15.03 - Airport managing bodies;
ED.13.04 - Police;	ED.14.04 - Travel Services.	ED.15.04 - Automotive industry;
ED.13.05 - Emergency communications;		ED.15.05 - Traffic management control operators;
ED.13.06 - Civil protection;		ED.15.06 - Rail transport;
ED.13.07 - Inspections services;		ED.15.07 - Infrastructure managers;
ED.13.08 - First Responders.		ED.15.08 - Railway undertakings;
		ED.15.09 - Water transport;
		ED.15.10 - Inland, sea and coastal passenger and freight water transport companies;
		ED.15.11 - Managing bodies of ports;
		ED.15.12 - Operators of vessel traffic services;
		ED.15.13 - Road transport;
		ED.15.14 - Road authorities;
		ED.15.15 - Operators of Intelligent Transport Systems;
		ED.15.16 - Sea transport;
		ED.15.17 - Container Ships;
		ED.15.18 - Passenger's Ships-Cruise Lines;
		ED.15.19 - Fisheries;
		ED.15.20 - Multi modal transport;
		ED.15.21 - Transport Critical Information Infrastructures (Transport CIIs).

ED.16 - Training, Competence and Situational Awareness	ED.17 - Education
ED.16.01 - Training Simulation	ED.17.01 - Information Security Systems
ED.16.02 - Cyber-Range	ED.17.01 - Student Management Systems
ED.16.03 - Federated Cyber-Range	ED.17.01 - Learning Management Systems
ED.16.04 - Cyber-Range Infrastructure	ED.17.01 - Cloud-based Solutions
ED.16.05 - Performance Management Infrastructure	ED.17.01 - Application Master Systems
ED.16.06 - Online Learning Website	ED.17.01 - Research Repositories
ED.16.07 - MOOCs	ED.17.01 - Physical Monitoring Systems
	ED.17.01 - Recognition and Identification Systems

Table 30: Complementary sectors and subsectors for ECHO Cybersecurity Taxonomy.

Both lists are meant as the initial definition of the ECHO Taxonomy that will be updated and enhanced along the whole duration of the project. Beyond these, the taxonomy list below has emerged around ECHO technological roadmaps.

5.5.2 ECHO Cybersecurity Framework Vocabulary

In addition to the categorisation and taxonomy, this sub-section provides overall ECHO cybersecurity framework vocabulary. Cybersecurity Framework Vocabulary addresses the key definitions used in ECHO and especially in ECHO eMAF creation.

Access control

(ISO/IEC 27000) means to ensure that access to assets is authorized and restricted based on business and security requirements.

Acquisition

(ISO/IEC 27037:2012) process of creating a copy of data within a defined set (the product of an acquisition is an evidentially reliable copy of the original source data).

Audit

(ISO/IEC 27000:2016) systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled (An audit can be an internal audit or an external audit, and it can be a combined audit).

(ISA 62443-1-2) independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Asymmetric cryptographic algorithm

(ISO/IEC 10181-1:1996, definition 3.3.1) algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ.

Attack

(ISO/IEC 27000:2016) attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

Authentication

(ISO/IEC 27000) provision of assurance that a claimed characteristic of an entity is correct.

Availability

(ISO/IEC 27000:2016) property of being accessible and usable upon demand by an authorized entity.

Biometrics Attack

(ISO/TR 18307:2001) use of specific attributes that reflect unique personal characteristics, such as a fingerprint, an eye blood-vessel print, or a voice print, to validate the identity of entities.

Boundary Protection

(NIST Special Publication 800-53Revision 4**[103]**) Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., gateways, routers, firewalls, guards, encrypted tunnels).

Boundary Protection Device

(NIST Special Publication 800-53Revision 4**[103]**) A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) provides information system boundary protection.

Category

The subdivision of a Function intro groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. For example “Access Control” and “Detection Processes”.

Certification

(Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency") Certification consists of the formal evaluation of products, services and processes by an independent and accredited body against a defined set of criteria standards and the issuing of a certificate indicating conformance. Certification serves the purpose to inform and reassure purchasers and users about the security properties of the products and services that they buy or use.

Collection

(ISO/IEC 27037:2012) process of gathering the physical items that contain potential digital evidence.

Confidentiality

(ISO/IEC 27000:2016) property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Conformity

(ISO/IEC 27000:2016) fulfilment of a requirement.

Control

(ISO/IEC 27000:2018) measure that is modifying risk (3.61)

Note 1 to entry: Controls include any process (3.54), policy (3.53), device, practice, or other actions which modify risk (3.61).

Critical Infrastructure

(NIST, Cybersecurity framework, 2014) Physical or virtual vital systems and assets that the incapacity or destruction os such systems and assets would have a debilitating impact to cybersecurity on cybersecurity, national economic security, national public health and safety or any combinations of those.

Cryptanalysis

(ISO/IEC 7498-2:1989, definition 3.3.18 and ISO/IEC 18033-1 2015) the analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including cleartext.

Cryptology

(Computer Security – Dieter Gollmann – Johnson Wileys and Sons) Cryptology groups together by definition of Cryptography (i.e. “the science of secret writing”) and Cryptanalysis (i.e. the science of “breaking ciphers”). For the scope of this taxonomy, under this domain go not only the mathematical foundations, but also the technical implementations of cryptographic algorithms and architectures, as well as the implementation of cryptanalytic methodologies, techniques and tools.

Cybercrime

(ISO/IEC 27032:2012) criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime.

Cyber-risk

(also cybersecurity risk)

(ISO 31000:2009(E)) A cyber-risk is the potential of harm or loss related to ICT systems or usage of technology within an organization. A cyber-risk is caused by a cyber-threat.

Cybersafety

(ISO/IEC 27032:2012) Condition of being protected against a physical, social, spiritual, financial, political, emotional, occupational, psychological, educational, or other types or consequences of failure, damage, error, accidents, harm of any other event in the cyberspace which could be considered non-desirable.

Cybersecurity

(ISO/IEC 27032:2012) preservation of confidentiality, integrity and availability of information in the Cyberspace (JRC taxonomy).

Cybersecurity Event

(NIST, Cybersecurity framework, 2018) The process of protecting information by preventing, detecting and responding attacks.

Cyber-incident

(NIST SP800-61) A cyber-incident is a cyber-event that has been determined to impact organizational operations, typically through an act of violating organization ICT system's (explicit or implied) security policy with the purpose of affecting its integrity or availability and/or (failed or successful) unauthorised access and use.

Cybersecurity Incident

(NIST, Cybersecurity framework, 2018) A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.

Cyber-Threat

(also cybersecurity threat) Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or nations through an ICT system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Cyber-Range Platform

(ECHO Consortium, WP6) A safe environment for cyber-attack scenario simulation and test. Offers the capability to create realistic cyber simulations useful for: Cyber training and exercise: Equip cyber analysts and operators with advanced cyber skills; Cyber research and development: Prototype development in realistic cyber scenarios; Cyber test and evaluation: Adaptable test framework for certification testing.

Cyber-Range Scenario

(ECHO Consortium, WP6) Multi-layered description in a human readable format (JSON, XML) of an instance of a cyber-range environment leveraging one of the envisioned functionalities of the cyber-range (training, testing and R&D). It may encapsulate business, application and ICT topologies for setting up simulated

environment, and eventual pedagogical/testing aspects of the instance. It may encompass assets from more than one cyber-range.

Cyber-Range Infrastructure

(ECHO Consortium, WP6) A set of virtual and/or physical resources dedicated to hosting simulated environments for cyber-range exercises.

Cyber-Range Service

(ECHO Consortium, WP6) With Cyber-Range Service we intend the combination of the technical offering of one or more (federated) Cyber-Ranges in terms of cyber-range scenarios and the related service offering leveraging the cyber-range scenario. In other words, a Service is not composed only by the technical offering (the cyber-range scenario), but also any support service eventually provided with it. A Cyber-Range Service could then be a combination of available capacity/capability forming a coherent offering. Cyber-Range Services are offered as possible contents for Customer with the Marketplace.

Cyber-Range Sector-Specific Extension

(ECHO Consortium, WP6) Sector-specific extensions as physical or virtual devices or systems that can be added to a cyber-range to enhance its simulation capabilities by provisioning means of connectivity to real or simulated physical or software systems, specific to a given sector. For example, they could provide access to non-IP-based communication networks like SCADA systems, sensor networks, satellite communication or security systems. Sector-specific databases or control systems are part of this definition

Cyber-Risk management

(NIST Cybersecurity Framework) The process of identifying, assessing, and responding to (mitigating) a cyber-risk.

Data

(ISO/IEC 27000:2016) collection of values assigned to base measures, derived measures and/or indicators.

Digital evidence

(ISO/IEC 27037:2012), stored or transmitted information or data in binary form that may be relied on as evidence.

Digital signatures

(ISO/IEC 14888) process which takes as inputs the message, the signature key and the domain parameters, and which gives as output the signature.

Digital Rights Management

(ISO/IEC 5127:2017) digital technology that is separate to the product form of a specific digital publication and which is used to control access to content.

Distributed System

(Coulouris, George; Jean Dollimore; Tim Kindberg; Gordon Blair (2011). Distributed Systems: Concepts and Design (5th Edition). Boston: Addison-Wesley. ISBN 0-132-14301-1) A distributed system is a model in which components located on networked computers communicate and coordinate their actions by passing messages. In this context cybersecurity deals with all the aspects of coordination, message integrity, availability and (if required) confidentiality. Message authentication is also in the scope.

ECHO Multi-sector assessment framework

(ECHO Consortium, WP2) The ECHO-Multisector assessment framework represents an approach to identify transversal, multi-sector and inter-sector cyber security challenges and opportunities leading to identification of technology roadmaps and requirements.

ECHO Cyberskills framework

(ECHO Consortium, WP2) The ECHO-Cyberskills framework represents and approach to describe the cyberskills requirements needed to develop the training curricula to equip cybersecurity professionals with needed expertise to address the identified transversal, multi-sector and inter-sector cyber security challenges.

eIDAS

(Regulation (EU) No 910/2014) EU regulation proposed to ensure that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available.

Framework

(ECHO Consortium, WP2) A framework identifies universal elements that any theory, approach or methodology related to the same class of phenomena would need to include to help achieve the objective and to achieve the desired outcomes of that framework.

(NIST, Cybersecurity framework, 2018) A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the “Cybersecurity Framework”.

Framework Core

(NIST, Cybersecurity framework, 2018) A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.

Governance of information security

(ISO/IEC 27000:2016) system by which an organization’s information security activities are directed and controlled.

Hash functions

(ISO/IEC 10118-1:2016) Hash-functions map strings of bits of variable (but usually upper bounded) length to fixed-length strings of bits, using a specified algorithm. They can be used for reducing a message to a short imprint for input to a digital signature mechanism, and committing the user to a given string of bits without revealing this string.

Human errors

Mistakes that unwittingly create opportunities for cyber hackers to exploit.

Identity

(ISO/IEC 24760-1:2011) set of attributes related to an entity.

Identity management

(ISO/IEC 24760-1:2011) processes and policies involved in managing the lifecycle and value, type and optional metadata of attributes in identities known in a particular domain.

Indicator

(ISO/IEC 27000:2016) measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to defined information needs (2.31).

Identification

(ISO/IEC 27037:2012) process involving the search for, recognition and documentation of potential digital evidence.

Information

(ISO/IEC 27000: 2018) Information is an asset that is essential to an organization's business and consequently needs to be protected. Information can be stored forms as digital form (e.g. data files stored on electronic or optical media), material form (e.g. on paper), as well as unrepresented information in the form of knowledge of the employees. Information can be transmitted or shared by various means including: courier, electronic or verbal communication. Whatever form information takes, or the means by which it is transmitted, it always needs appropriate protection. Information is dependent on information and communications technology. Technology is often a crucial element in the organization and assists in facilitating the creation, processing, storing, transmitting, protection and destruction of information.

Information security

(ISO/IEC 27000:2018) Preservation of confidentiality, integrity and availability of information. Information security is achieved through the implementation of an applicable set of controls, selected through the chosen risk management process and managed using an ISMS (Information Security Management System) consisting (policies, processes, procedures, organizational structures, software and hardware to protect the identified information assets). (ISO/IEC 27032:2012) Information security consist (Network security, Internet security, CIIP (critical information infrastructure protection).

Information security control

(ISO/IEC 27008:2019) Adequately mitigates information risks that the organization finds unacceptable and unavoidable need to be controlled. Information security controls should be "fit-for-purpose". (ISO/IEC 27008: 2019) Performs Guidance on how to review and assess information security controls being managed through an Information Security Management System specified by ISO/IEC 27001. E.g., NIST Special Publication (SP) 800-53A**[104]** is related publication for the information security controls.

Information security continuity

(ISO/IEC 27000:2016) processes and procedures for ensuring continued information security operations.

Information security event

(ISO/IEC 27000:2016) identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant.

Information security incident

(ISO/IEC 27000:2016) single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Information security incident management

(ISO/IEC 27000:2016) processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.

Information system

(ISO/IEC 27000:2016) applications, services, information technology assets, or other information handling components.

Information Security techniques

ICT readiness is a crucial component for many organizations in the implementation of business continuity management and information security management. As part of the implementation and operation of an Information Security Management System (ISMS) specified in ISO/IEC 27001 and Business Continuity Management System (BCMS) respectively, it is critical to develop and implement a readiness plan for the ICT services to help ensure business continuity.

Information Security Management System (ISMS)

An Information Security Management System (ISMS) describes and demonstrates an organisation’s approach to Information Security (and privacy management).

Informative reference

(NIST, Cybersecurity framework, 2018) A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each Subcategory. An example of an Informative Reference is ISO/IEC 27001 Control A.10.8.3, which supports the “Data-in-transit is protected” Subcategory of the “Data Security” Category in the “Protect” function.

Integrity

(ISO/IEC 27000:2016) property of accuracy and completeness.

Key management

(ISO/IEC 11770-1:2010 PART 1, definition 2.28) administration and use of generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy.

Level of risk

(ISO/IEC 27000:2016) magnitude of a risk (2.68) expressed in terms of the combination of consequences (2.14) and their likelihood.

Likelihood

(ISO/IEC 27000:2016) chance of something happening.

Malware

(ISO/IEC 27033-1:2015) malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability (E.g., viruses and Trojan horses).

Management

Management involves activities to direct, control, and continually improve the organization within appropriate structures.

Management system

(ISO/IEC 27000:2018) Uses a framework of resources to achieve organization´s objectives. Set of interrelated or interacting elements of an organization to establish policies, objectives, and processes to achieve those objectives. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

Message authentication

(ISO/IEC 9797-1) process to authenticate a message, often done through Message authentication codes (string of bits which is the output of a MAC algorithmality, integrity and/or availability.

Metadata

(Special Publication 800-53Revision 4**[103]**) Information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels).

Monitoring

(ISO/IEC 27000:2016) determining the status of a system, a process (2.61) or an activity.

National Security System

(Special Publication 800-53Revision 4**[103]**) Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency.

Network security

(ISO/IEC TR 29181-5) Network security is concerned with hardware, software, basic communication protocols, network frame structure, and communication mechanisms factors of the network. Information Security in the network context deals with data integrity, confidentiality, availability and non-repudiation while is sent across the network.

Organization

(ISO/IEC 27000:2016) person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives.

Outsource

(ISO/IEC 27000:2016) make an arrangement where an external organization performs part of an organization's function or process.

Personally Identifiable Information (PII)

(ISO/IEC 24745:2011) any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains; from which identification or contact information of an individual person can be derived, or that is or might be directly or indirectly linked to a natural person.

Policy

(ISO/IEC 27000:2016) intentions and direction of an organization as formally expressed by its top management.

Process

(ISO/IEC 27000:2016) set of interrelated or interacting activities which transforms inputs into outputs.

Protect (function)

(NIST, Cybersecurity framework, 2018) Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

Privacy

(ISO/TS 25237:2008) freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual.

Privacy Enhancing Technology

(PET) (ISO/IEC 29100:2011) privacy control, consisting of information and communication technology (ICT) measures, products, or services that protect privacy by eliminating or reducing personally identifiable information (PII) or by preventing unnecessary and/or undesired processing of PII, all without losing the functionality of the ICT system.

Recover (function)

(NIST, Cybersecurity framework, 2018) Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Respond (function)

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event (NIST, Cybersecurity framework, 2018).

Risk

(ISO/IEC 27000:2016) effect of uncertainty on objectives. In the context of information security (2.33) management systems, information security risks can be expressed as effect of uncertainty on information security objectives. Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

(NIST, Cybersecurity framework, 2018) A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Risk Acceptance

(ISO/IEC 27000:2016) informed decision to take a particular risk. Risk analysis (ISO/IEC 27000:2016) process to comprehend the nature of risk and to determine the level of risk. Risk assessment (ISO/IEC 27000:2016) overall process of risk identification, risk analysis and risk evaluation. Risk evaluation (ISO/IEC 27000:2016) process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Risk Identification

(ISO/IEC 27000:2016) process of finding, recognizing and describing risks. Risk management (ISO/IEC 27000:2016) coordinated activities to direct and control an organization with regard to risk.

Risk Level

(ISO 31000:2009E) The magnitude of risk as derived from the chance from something to occur and the impact of a cyber-incident on an asset, in terms of harm or reduced value of the asset (anything of value in the ICT system).

Risk Monitoring

(Special Publication 800-53 Revision 4**[103]**) Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions.

Risk management process

(ISO/IEC 27000:2016) systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk Mitigation

(NISTIR 7298, Rev. 2) Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

Risk owner

(ISO/IEC 27000:2016) person or entity with the accountability and authority to manage a risk.

Risk treatment

(ISO/IEC 27000:2016) process to modify risk (eg. Avoidance, removal, change, share, retain, mitigation). Scale (ISO/IEC 27000:2016) ordered set of values, continuous or discrete, or a set of categories to which the attribute is mapped.

Security management policy

(ISO/IEC 28000:2007) overall intentions and direction of an organization, related to the security and the framework for the control of security-related processes and activities that are derived from and consistent with the organization's policy and regulatory requirements.

Security Measurements

(NIST SP800-55) Information security measures are used to facilitate decision making and improve performance and accountability through the collection, analysis and reporting of relevant cybersecurity performance-related data. The purpose of measuring performance is to monitor the status of measured activities and facilitate improvement in those activities by applying corrective actions based on observed measurements.

Security Target

(ISO/IEC 15408-1:2009) implementation-dependent statement of security needs for a specific identified Target of Evaluation (TOE).

Threat

(ISO/IEC 27000:2016) potential cause of an unwanted incident, which may result in harm to a system or organization.

Traffic light protocol (TLP)

(ENISA) The Traffic Light Protocol (TLP) is a means for someone sharing information to inform their audience about any limitations in further spreading this information. It is used in almost all CSIRT communities and some Information Analysis and Sharing Centres.

Trust

(ISO/IEC 25010:2011) degree to which a user or other stakeholder has confidence that a product or system will behave as intended.

Verification

(ISO/IEC 27000:2016) confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.

Vulnerability

(ISO/IEC 27000) weakness of an asset or control that can be exploited by one or more threats.

USA –related publications that can be implemented in Europe with minor changes.

Guide for Applying the Risk Management Framework to Federal Information Systems

NIST Special Publication 800-37r1 provides guidelines for applying the Risk Management Framework (RMF) to federal information systems. The six-step RMF includes security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. The RMF promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes. It provides senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions and integrates information security into the enterprise architecture and system development life cycle.

NIST Special Publication 800-37 r2 provides risk Management Framework for Information Systems and Organizations

Publication describes the Risk Management Framework (RMF) and provides guidelines for applying the RMF to information systems and organizations. The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. The RMF includes activities to prepare organizations to execute the framework at appropriate risk management levels.

Guide to Cyber Threat Information Sharing

NIST Special Publication 800-15 provides guidelines for establishing and participating in cyber threat information sharing relationships. This guidance helps organizations establish information sharing goals, identify cyber threat information sources, scope information sharing activities, develop rules that control the publication and distribution of threat information, engage with existing sharing communities, and make effective use of threat information in support of the organization's overall cybersecurity practices

Security and Privacy Controls for Federal Information Systems and Organizations (Special Publication 800-53 Revision 4**[103]**)

The publication provides a catalogue of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors.

5.5.3 ECHO Cybersecurity Framework Semantics

It is important to understand the ontology and semantics around phrases used in the eMAF development. Ontological and sematic considerations enhance to get prepared and mitigated with risks towards future challenges and threats. In addition, the previous sub-chapters provides the basics for eMAF language, and this sub-sections aims to increase this knowledge more in details and background.

Among practitioners, researchers and professionals there is rather little consensus existing about what the terms “cyber”, “security” and “cybersecurity” include, refer to, or how those are being used differently by different experts in different contexts. It was no coincidence that had begun to disappear from the forefront of the academic debate by the early 2000s, only to be replaced by the ‘cyber’ moniker as the go-to concept for discussing and analysing the security challenges of the latest information age.

Originally or traditionally, the word or definition “cyber” can be traced back to Ancient Greece and *Kybernetes*, when it meant “the art of steering” (Tabansky 2011, p. 76) **[52]**. Nobert Wiener (1948) **[53]** published *Cybernetics* as a study of the importance of systems in both, living and artificial machines. In the 1980s there was at the same time, a cyberpunk movement and a spread of sophisticated computers for military operations by U.S. In the 1995, the investigation revealed some vulnerabilities in U.S. critical national infrastructure, and a phrase “cyber” was chosen to capture the challenges posed by computer vulnerabilities. (Kaplan 2016, p. 45–46) **[54]**. The definition *cyberwar* grow from Information Warfare (IW), Information Operations (IO) and revolution in military (Collins & Futter, 2015) **[55]**.

The language of IW and IO begun to disappear from academic debate in early 2000s. The definition “cyber” had replaced these, as an overall concept to discuss and analyse security related challenges in the information age. Cybersecurity has emerged from precise langue and the concept already has and will have even more complexity, activities, phenomena and dynamics to label.

The discussion around the term “cyber” provides an idea on how the cyber security domain refers to a knowledge that is complex, rapidly changing, and difficult to manage. Several factors contribute to this situation:

1) Cyber Knowledge ‘human sources’ are different, from IT security providers to attackers (i.e. criminals, competitors, state-sponsored actors).
2) Cyber Knowledge ‘physical sources’ are different too: from defensive products to guidelines, policies and standards, from known vulnerabilities to unknown ones (“zero-day”), which have in turn spread across various technologies.
3) Cyber Knowledge is subject to continuous changes, caused by the technological evolution of products and methods developed to address attacks.

In the context of ECHO Cybersecurity Framework, “cyber” connotes with a strong relationship with Information Technology and relates to characteristics of Information Technology and virtual reality culture (often referring to the “cyber world”) in different contexts. The definition varies naturally from narrow conceptions to broader framework. The conceptualisation to physical/mechanical, logical, informational and human/cognitive (e.g. Futter, 2016) **[56]**, is not enough in ECHO Cybersecurity Framework. Beyond

- physical infrastructure and hardware;
- command of control;
- collection/store/generate/rely of system data or information;
- human beings and their interactions with computers, machines and technology.

ECHO Cybersecurity Framework addresses the semantics of cybersecurity related challenge activities (such as threat, crime, and attack), variety of physical sectoral scenarios and specific contexts, and it aims to find transversal and inter-sector needs as well as requirements. In order to specify how comprehensive the

concepts are, the definition of cyber-attack is commonly used in tactical, operational, academic and political discourses. Often, the original purpose of the defined cyber-attack in practice can be to indirectly mislead or spark to crisis rather than aiming to damage computers, technology or machine.

ECHO Cybersecurity Framework Taxonomy and Vocabulary provide words and definitions to understand the overall picture more in details. As indicated in this subsection, there is not one size/service suitable for all solutions, we also tend to use only one formulation or phrase. The semantics of phrases “cyber” and “cybersecurity”, reveal the complexity and comprehensiveness of the vocabulary and taxonomy used. The challenge is only increasing when we aim to conceptualise them in several sectors and link their inter-connectedness. The original purposes of these meanings are based on leadership and importance of both, physical and virtual technology domains. ECHO Cybersecurity Framework and Multi-Assessment Framework offer to look more comprehensively at the reality of cybersecurity concept and practices that are highly nuanced. The taxonomy and vocabulary provide reality-based definitions for strategical and political levels of responsibilities. Semantics, taxonomies and vocabularies offer better and more precise language for entire domain and frameworks. Lumping all terms under Cybersecurity Framework draws the direction.

The pace of technological change will only continue faster development, and the understanding of differences (through analysing activities, means, methods, capabilities, threats and responsibilities) is required especially from academic and political actors to provide more precisely and clarity.

The work in ECHO will be then devoted to design conceptual structures and concepts able to address this continuous evolution, providing the right level of flexibility required to add new threats and corresponding (technological, human, social and so on) countermeasures. Research in this field can be directed to define and apply reasoning methods specifically to identify and manage, on the basis of previous, known threats, new forms of cyber-attacks or, at least, new, related entities, concepts, able to enrich and support defensive actions in several application domains **[57].**

The work on the ECHO cyber ontology is carried out in WP6.

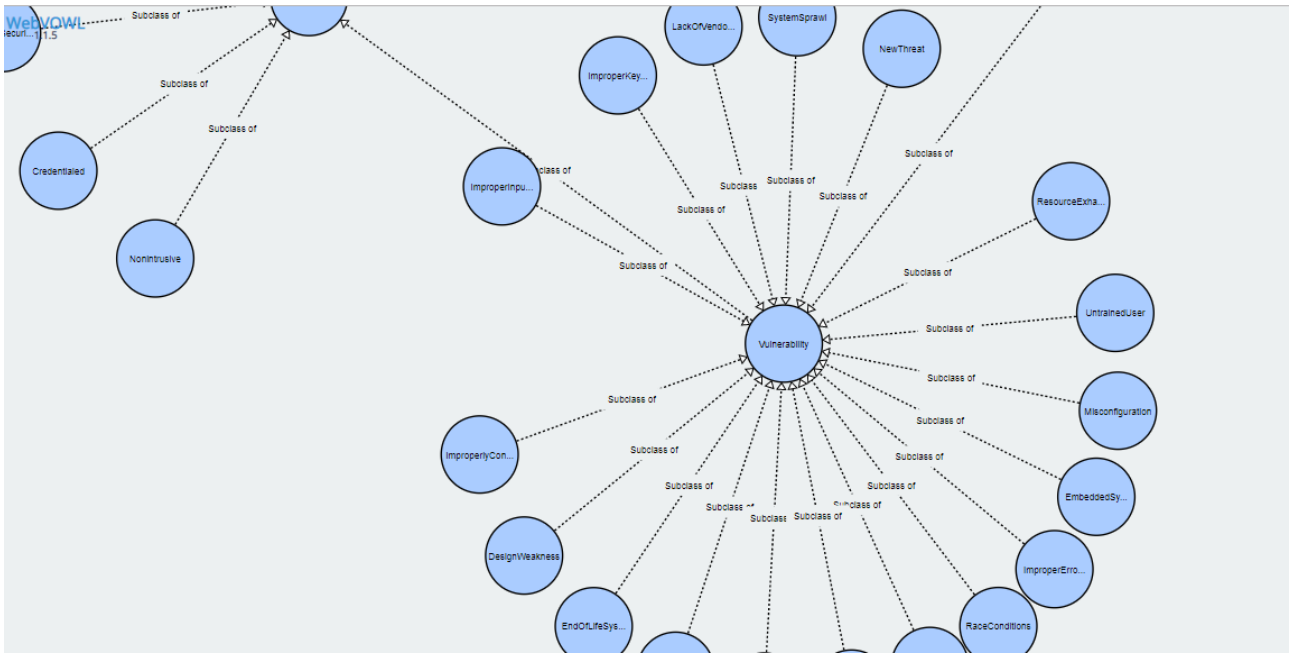

Figure 24: ECHO Cyber Security Ontology.

ECHO E-MAF ontology and semantic work has begun and will continue following the JRC-based taxonomy (described in the previous subsection), academic discussions and our work in relation to technological roadmaps of ECHO project. New entities, new relations between entities will be added, enriching the ontology

on the basis of the evolutions reported in the further versions of deliverables D2.1 **[1]**, D2.3 **[2]**, D2.4 **[3]** and D2.5 **[4]**, which register the advancements on history-line and use cases, transversal and inter-sector cybersecurity challenges and opportunities, multi-sector requirements and demonstration cases.

The work on the ECHO ontology will be distributed throughout the project, with some internal milestones to check structure and contents at 12, 24, 36 and 48 months. The continuous working process requires enhanced collaboration among engineers, developers, practitioners, researchers, political decision makers and industry. European pilot projects in cybersecurity provides a platform also for ontological and semantic analyses. This work aims to provide comprehensive understanding to pilot projects and their technology roadmaps in future. The current ontology covers all the cybersecurity-related terms and concepts, currently without the relations between them. An update is planned to be provided with the relations towards the end of 2019 (except "sub-class of" relations). WP2 and WP6 collaborate in order to reach the finalization of ECHO ontology by the end of 2020, as regards what is needed by E-MAF.

5.6 Roadmap for E-MAF implementation

Here follow the next steps of the Roadmap for E-MAF implementation:

Step #1 (M10, Dec 2019)

Start of the first iteration. Ingestion of Methodologies for Transversal aspects (T2.3), technology challenges (T2.4), multi-sector (T2.5) in designed architecture for improvement.

Step #2 (M11, Dec 2019)

Finalization of the comparison of existing Risk Management Frameworks. Comprising: ISO 27001**[15]**, NIST Cyber Security Framework**[27]**, NIST SP 800-53**[103]** Controls, National Frameworks (e.g. Italian Cyber Security Framework). Finalization of defense/space domain-specific CSF adoption analysis.

Step #3 (M13, Feb 2020)

Finalization of the assessment of previous and current EU funded projects as required by reviewer's comments after first project review.

Step #4 (M14, March 2019)

Review of the Risk Assessment Framework Architectural Design with preparation of the ingestion of D2.1 StoryLines.

Step #5 (M19, August 2020)

Implementation of the First Prototype (RA). Development of a risk assessment methodology and operational guidelines involving both traditional cybersecurity factors and financial/economic factors. Release of the first prototype to interested WPs and tasks.

Step #6 (within M21, Oct 2020)

Finalization of the adoption of E-MAF in WP2 tasks. The E-MAF will be fed by StoryLines and results of RA will be used by WP2 Tasks. In the meanwhile external WPs will also have the chance to exploit results of E-MAF.

Step #7 (M23, December 2020)

Collection of results from T2.2, other tasks in WP2, external WPs. End of first iteration.

Then, the iteration process will continue until the end of ECHO project leading to several virtuous cycles of innovation and enhancement for E-MAF.

Step #8 (M23)

Start of second iteration. Development of specific metrics, scoring of risks levels. Start of improvement of RA Framework. Start of Risk Management Framework implementation.

Step #9 (M25)

End of Risk Assessment improvement. Risk Management Implementation. Second release of E-MAF transmitted to WP2 Tasks, external WPs.

Step #10 (M26)

Collection of results from T2.2, other tasks in WP2, external WPs. End of second iteration.

Step #11-#12 (M27-M30)

Start of third iteration. Development of checklists and operational plans. Development of recommendations for the risk financing strategies. Start of new improvement of RA Framework. Start of improvement of Risk Management Framework implementation. Start of Cyber Security Framework implementation. At the end, Third release of E-MAF transmitted to WP2 Tasks, external WPs.

Step #13 (M32)

Collection of results from T2.2, other tasks in WP2, external WPs. End of third iteration.

Step #14-#15 (M33-M39)

Start of fourth iteration. Study of certification and assurance procedure. Finalization of RA Framework. Second improvement of Risk Management Framework implementation. Improvement of Cyber Security Framework implementation. At the end, Fourth release of E-MAF transmitted to WP2 Tasks, external WPs.

Step #16 (M41)

Collection of results from T2.2, other tasks in WP2, external WPs. End of fourth iteration.

Step #17 (M42)

Start of Final ECHO multi-sector cybersecurity framework.

Step #18 (M45)

Release of the final E-MAF CSF.

6. Conclusions

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 (to have a prototype which could be quickly adopted in order to produce results which could support the decision making process) 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 (Section **2.1**) 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), in Section **3**. 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 (Section **4**).

At the end of those two phases, all the necessary information were collected in order to:

- finalize the architectural design described in Section **5**. In this aim, answering to reviewers' comments on the first version of this deliverable (after the first project review) provided a clear added value to the assessment and the architectural design.
- start the implementation of the ECHO Risk Assessment Framework layer from Month 12. Here a risk assessment methodology and operational guidelines involving both traditional cybersecurity factors and financial/economic factors will concretize. As we stated in Section **5.1**, E-MAF is not an update of an already existing Cyber security framework. It takes inspiration from several methods, methodologies and frameworks depicted in this document and defines a new approach based on a multi-sector, transversal reference to cybersecurity Risk Management (and consequently Assessment). At the time of this writing, MEHARI and NIST seems to be the bigger sources for inspiration as well as the approaches put in place CYSM, MEDUSA, and MITIGATE projects. It must not be forgotten that further assessment will be performed on Cyber Security Frameworks in the next weeks towards the prototype release at M19.

Starting from M19 (first iteration), The ECHO RA framework will be applied to D2.1 **[1]** StoryLines Use Cases and will produce important inputs for the Tasks and the WPs listed in Section **5.1**.

In the meanwhile, iteration process will continue towards enhancement and full implementation of E-MAF, starting from the finalization of the comparison of existing Risk Management Frameworks for those aspects we left out in the initial analysis phases (in ISO 27000and NIST SP 800-xx families) as well as the assessment of national frameworks. This will be done in parallel with the ingestion of the outcomes provided by methodologies definition for transversal aspects, technological challenges and opportunities, multi-sector dependencies. With full respect to the project timelines, the next step will then be:

- Development of specific metrics, scoring of risks levels;
- Development of checklists and operational plans;
- Development of recommendations for the risk financing strategies;

- Study of certification and assurance procedure.

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. The final E-MAF together with the finalization of ECHO Taxonomy and Ontology will provide an enormous added value to the work of T2.2. It will be a very amazing activity devoted to follow a sort of yet unexplored path, the team will walk in an enthusiastic manner.

Annexes

Annex 1 – T2.2 Framework and Methodologies Analysis Questionnaires

Annex 1.1 – ISO31000

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
1	**Specific Requirements. Does the Methodology…**			
1.1.1	... enables improvement of multi-sectoral management processes for mitigation of Cyber Security risks?	yes	medium	The ISO 31000 provides the principles, structure and process of risk management. It can be used by any organization, regardless of its size, type of activity or sector. It was developed by a range of stakeholders and is intended for use by anyone who manages risks, not just professional risk managers. Implementing ISO 31000 also helps organizations see both the positive opportunities and negative consequences associated with risk, and allows for more informed, and thus more effective, decision making, namely in the allocation of resources. It can be an active component in improving an organization's governance and, ultimately, its performance. The emphasis is on the continuous improvement of risk management through setting goals for the organization, measuring, reviewing and subsequently modifying processes, systems, resources, capabilities and skills. The ISO 31010 provides guidance on the selection and application of risk assessment methods in a wide range of situations. Methods are used to assist in decision making when uncertainty exists, to provide information on specific risks and as part of the risk management process.
1.1.2	... assesse transversal and inter-sector opportunities and challenges?	yes	medium	The ISO 31000 postulates eleven principles, interpreting risk management as an interdisciplinary task on all levels which has to be transparently integrated in existing organizational structures. It can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment. ISO 31000 was not developed for a particular industry group, management system or subject matter field, but rather to provide best-practice structure and guidance to all operations concerned with risk management.
1.1.3	... enable a transversal vision for security countermeasures?	yes	medium	ISO 31000 takes into account many types of risks. The following factors, and the relationship between these factors, should be considered: tangible and intangible sources of risk; causes and events; threats and opportunities; vulnerabilities and capabilities; changes in the external and internal context; indicators of emerging risks; the nature and value of assets and resources; consequences and their impact on objectives; limitations of knowledge and reliability of information; time-related factors; biases, assumptions and beliefs of those involved.
1.1.4	… use/rely on an EU Methodology?	no	-	-

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
1.1.5	… enable benchmarking initiatives?	yes	medium	Organizations using it can compare their risk management practices with an internationally recognised benchmark, providing sound principles for effective management and corporate governance .The ISO 31000 Guidelines are designed for a wide range of risk management practitioners, experienced or novice, and for those responsible for risk management oversight who are interested in benchmarking their risk management organisation and practices against a recognized international reference.
1.2	Is the Methodology clear and well defined?	yes	medium	ISO 31000: 2018 provides clearer and shorter guidance to help organizations use risk management principles to improve planning and make better decisions.
1.3	Is the Methodology open source?	no	-	You can buy ISO 31000:2018 Risk management — Guidelines at the following link: https://www.iso.org/standard/65694.html, IEC 31010:2019 Risk management — Risk assessment techniques you can buy at the following link: https://www.iso.org/standard/72140.html
1.4	Are the related Taxonomies well defined?	no	-	The standard describes the steps, approaches, methods for identifying and assessing risk, but does not describe the types of risks. In fact, this is a plan-to-do-check, which describes the steps to prevent, prevent, assess and analyze risk. There are no taxonomies in the standard. But there are famous taxonomies of risks for categories: Business processes; Capital infrastructure; Communications; Conflict of interest; Financial management; Governance and strategic direction; Human resources management; Information management; Information technology; Knowledge management; Legal; Organizational transformation and change management; Policy development and implementation; Privacy / Information stewardship; Program design and delivery; Project management; Political; Reputational; Resource management; Stakeholders and partnerships; Values and ethics.
1.5	Are the related Taxonomies expandable?	no	-	-
2	**Economic factors**			
2.1	Does the Methodology include a risk analysis method based on financial factors?	yes	low	1) Examining the organization's external context may include financial factors (5.4.1 Understanding the organization and its context) 2) The nature and value of assets and resources should be considered as a factor for identifying uncertainties that may affect one or more objectives (6.4.2 Risk identification) 3) Cost should be considered as a factor for reporting (6.7)
2.2	Does the Methodology support risk financing strategies for the residual risk?	no	-	-
3	**Innovation**			
3.1	Towards assessment of the suppor to to concept of Technology Roadmap one in ECHO,	-	-	-

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
	does the methodology …			
3.1.1	... enable analysis of a StoryLine or a UseCase from D2.1?	yes	medium	The situation that occurred in the office shows insufficient staff knowledge of security and possible risks, in particular, ISO 31000. If the provisions of paragraphs 6.3, 6.4, 6.5 were met, the consequences of cyber attacks could be avoided and mitigated. When a vulnerability was detected and the first manifestation of an attack, it was necessary to disconnect the router from the power supply, and then take measures to detect malicious actions and eliminate them. Application of the standard would allow creating an action plan in case of various types of attacks, to chose criterias of risks, assess and analyze possible risks.
3.1.2	… support the provisioning of a selection of roadmaps of ways (e.g. Controls) to reduce the risk?	no	-	-
3.1.3	… enable/define linkability to tools/ICT products?	no	-	-
3.2	Does it support the concept of Curricula (like defined in ECHO)?	no	-	-
3.3	Does it support the concept of Certification Scheme (like defined in ECHO)?	no	-	-
3.4	Does the methodology identify transversal, inter-sector and specific skills for Curricula?	no	-	-
3.5	Does the methodology provide a basis for Training Programmes?	yes	medium	ISO 31000 can provide a basis for Training Programmes the Learning Objectives of which are: To understand the concepts, approaches, methods, tools and techniques allowing an effective risk management according to ISO 31000 To understand the relationship between the risk management and the compliance with the requirements of different stakeholders of an organization. To acquire the competence to implement, maintain and manage an ongoing risk management program according to ISO 31000. To acquire the competence to effectively advise organizations on the best practices in risk management
4	**Qualitative Analysis**			

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
4.1	General Comments on investigated RA Framework.	ISO 31000 can help with: Giving you a competitive advantage because ISO is an internationally recognized symbol for quality standards Increasing employee awareness of organizational risks by including them in the management framework and giving them responsibility for the processes they commonly use Reduce the frequency of, and ultimately eliminate risks by educating employees and stakeholders on identified risks Improve trust of stakeholders by maintaining transparency and communicating risks (and demonstrating risk responsibility and mitigation) Foster forward-thinking mentalities by encouraging employees to envision all potential outcomes of a given situation Improve company culture by bringing disparate departments together to exchange fresh perspectives, and consider how they might work together more effectively Improve success rate in all business operations by focusing on the process, thinking preemptively instead of reactively, and giving employees ownership of their work responsibilities		
4.2	Reccommendations, specific aspects to be taken into consideration.	ISO 31000 contains much valuable information and it represents robust, high-level guidelines for the management of risk. However, there is no step-by-step checklist to implementation of the risk management initiative. The challenge for risk professionals is to rearrange the guidance in ISO 31000 to align with their own approach to implementing a risk management initiative. In other words, ISO 31000 clearly states that risk management is an open-ended process designed to be highly customized and tailored to the individual needs and contexts of the organization implementing it.		

Annex 1.2 – TOGAF

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
1	**Specific Requirements.** Does the Methodology…			
1.1.1	... enable improvement of multi-sectoral management processes for mitigation of Cyber Security risks?	yes	low	Chapter 27. An high level description of risk management approach for an architectural point of view.
1.1.2	... assess transversal and inter-sector opportunities and challenges?	yes	low	As per 2.1, only if the sectors architecture are designed with TOGAF principles.
1.1.3	... enable a transversal vision for security countermeasures?	no	-	-
1.1.4	… use/rely on an EU Methodology?	no	-	-
1.1.5	… enable benchmarking initiatives?	yes	high	the Methodology enables the comparison between TOGAF and other frameworks
1.2	Is the Methodology clear and well defined?	yes	medium	TOGAF provide an high level approach to risk management at architecural point of view. For a cyber security risk management refers to other frameworks (eg. ISO, NIST)
1.3	Is the Methodology open source?	yes	high	-
1.4	Are the related Taxonomies well defined?	yes	high	Part V considers taxonomies to categories the outputs of architecture activity in an enterprise
1.5	Are the related Taxonomies expandable?	no	-	-
2	**Economic factors**			
2.1	Does the Methodology include a risk analysis method based on financial factors?	yes	medium	Initial risk assessment include some financial factors
2.2	Does the Methodology support risk financing strategies for the residual risk?	no	-	-
3	**Innovation**			
3.1	Towards assessment of the supporto to concept of Technology Roadmap one in ECHO, does the methodology …	-	-	-
3.1.1	... enable analysis of a StoryLine or a UseCase from D2.1?	no	-	-
3.1.2	… support the provisioning of a selection of roadmaps of ways (e.g. Controls) to reduce the risk?	yes	low	The Risk Mitigation Plan contains activities to mitigate risks. No references to controls in TOGAF.
3.1.3	… enable/define linkability to tools/ICT products?	no	-	-

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
3.2	Does it support the concept of Curricula (like defined in ECHO)?	no	-	-
3.3	Does it support the concept of Certification Scheme (like defined in ECHO)?	yes	low	The TOGAF Standard provides a repository area to hold a set of specifications to which architectures must conform. Only for architectures.
3.4	Does the methodology identify transversal, inter-sector and specific skills for Curricula?	no	-	-
3.5	Does the methodology provide a basis for Training Programmes?	no	-	-
4	**Qualitative Analysis**			
4.1	General Comments on investigated RA Framework.	TOGAF provide a risk management approach at architecural point of view. Does ot give a methodology for anlyze and mitigate a cyber security risk as other framework. In January 2016, the TOGAF Security Guide was published. It addresses security and risk management at a conceptual level, which matches with the way that TOGAF defines architecture. This enables the integration of both processes in the architecture.		
4.2	Reccommendations, specific aspects to be taken into consideration.	Suggest to consider only the eterprise organizational aspect and risk management upon the target architecure (eg. business, data, technology)		

Annex 1.3 – NIST SP800-30

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
1	**Specific Requirements.** Does the Methodology…			
1.1.1	... enable improvement of multi-sectoral management processes for mitigation of Cyber Security risks?	yes	low	The methodology is sector-agnostic and written to be open and applicable to a generic organization and subject to spacification of threats/vulnerability/scale value for each organization
1.1.2	... assess transversal and inter-sector opportunities and challenges?	yes	low	The methodology is sector-agnostic and written to be open and applicable to a generic organization and subject to spacification of threats/vulnerability/scale value for each organization
1.1.3	... enable a transversal vision for security countermeasures?	no	-	The methodology does not provide a taxonomy of security controls, but they can be found in the associated SP 800-53
1.1.4	… use/rely on an EU Methodology?	yes	medium	see point 1.6.16
1.1.5	… enable benchmarking initiatives?	no	-	the scales are provided only as reference and fuly open to customization at organization and also deparment level. It doesn't provide reference levels to be used across different organizations or sectors
1.2	Is the Methodology clear and well defined?	yes	medium	The document desribes all the steps necessary to carry out a risk assessment. The limit of this methodology (as many other) consists in the fact that the risk factors like likelihood and impact (based on Relevance, Likelihood of Attack Initiation, Vulnerabilities and Predisposing Conditions, Severity, Pervasiveness, Likelihood Initiated Attack Succeeds) depends on "organization" and threfore on the "security analyst" designing the process
1.3	Is the Methodology open source?	yes	-	-
1.4	Are the related Taxonomies well defined?	yes	low	The methodology provides categories for threats and vulnerability, criteria for their definition and a list of examples to be used as a basis. The taxonomy can be customised at organization level
1.5	Are the related Taxonomies expandable?	yes	low	The taxonomies are drafted as categories and example, it is necessary to develop them in a structured approach
2	**Economic factors**			
2.1	Does the Methodology include a risk analysis method based on financial factors?	no	-	The financial impact is only mentioned in the impact description, but not quantified or evaluated in any way
2.2	Does the Methodology support risk financing strategies for the residual risk?	no	-	-
3	**Innovation**			
3.1	Towards assessment of the support to concept of Technology Roadmap one in ECHO, does the methodology …	-	-	-
3.1.1	... enable analysis of a StoryLine or a UseCase from D2.1?	yes	medium	The methodology is open enough to be applied to different sectors and allows the customization of threats, vulnerabilites and scales for each sector
3.1.2	… support the provisioning of a selection of roadmaps of	no	-	-

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
	ways (e.g. Controls) to reduce the risk?			
3.1.3	… enable/define linkability to tools/ICT products?	no	-	-
3.2	Does it support the concept of Curricula (like defined in ECHO)?	no	-	-
3.3	Does it support the concept of Certification Scheme (like defined in ECHO)?	no	-	-
3.4	Does the methodology identify transversal, inter-sector and specific skills for Curricula?	no	-	-
3.5	Does the methodology provide a basis for Training Programmes?	no	-	-
4	**Qualitative Analysis**			
4.1	General Comments on investigated RA Framework.	The methodology is well described and detailed steps are provided in order to carry out a risk assessment. The main drawback remains the definition of the risk factors likelihood and impact (based on Relevance, Likelihood of Attack Initiation, Vulnerabilities and Predisposing Conditions, Severity, Pervasiveness, Likelihood Initiated Attack Succeeds) that depends on "organizational and management inputs" and threfore on the "security analyst" designing the process. Also the taxonomies are partially defined, leaving to the analyst their full definition. This approach does not really support the reproducibility and repeatabiloty criteria meant to be pursued by the methodology.		
4.2	Reccommendations, specific aspects to be taken into consideration.	1. Risk assessment must be able to address the 3 tiers (organization level, mission/business process level, and information system level) and it must be able to link risks at information system level to process, mission and organization level risks 2. Reproducibility and repeatability of the methodology and process must be considered 3. Criteria for defining scales for impact and likelihood must be clearly stated in order to provide impartial values to shared across the community and support bechmarking activities.		

Annex 1.4 – MEHARI

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
1	**Specific Requirements.** Does the Methodology…			
1.1.1	... enables improvement of multi-sectoral management processes for mitigation of Cyber Security risks?	yes	high	MEHARI current knowledge base and taxonomy is focused on ICT risks. No specific secto ris targeted: the methodology is widely used to analyse and treat risks on multiple sectors.
1.1.2	... assesse transversal and inter-sector opportunities and challenges?	yes	medium	Available knowledge base of MEHARI does not take into account explicitely of inter-sector opportunities and challenges, but it is quite generic on assessing ICT risks from a multi-sector perspective. MEHARI Knowledge Base, could be expanded/updated in order to identify inter-sector risk scenarios (challenges) which would lead to inter-sector risk treatment (opportunities).
1.1.3	... enable a transversal vision for security countermeasures?	yes	medium	MEHARI does not explicitely take into account inter-sector/transversal security measures, since it relies on a multi-sector horizontal approach. MEHARI knowledge base could be however updated/modified in order to identify inter-sector risk scenarios where transversal security measures can be applied.
1.1.4	… use/rely on an EU Methodology?	yes	high	MEHARI is listed by ENISA as an EU RA methodology. MEHARI is also fully compliant with ISO27001.
1.1.5	… enable benchmarking initiatives?	yes	low	MEHARI offers a systematic method for analysing ICT risks providing standard elements and criteria, that can be used to perform benchmarking activities.
1.2	Is the Methodology clear and well defined?	yes	high	The methodology is extremely clear and well documented. Several manuals and guidelines are available. MEHARI also relies on an excel tool supporting the risk analyst. The tool itself is not of easy use, but it is extremely complete and potentially it could be updated/modified to enrich the list of supported risk scenarios or security controls.
1.3	Is the Methodology open source?	yes	high	The methodology is open source under a License adapted from Creative Commons Attribution-ShareAlike 4.0 International Public License. MEHARI can be freely used also in commercial contexts, but it must be referenced. In case of updates to the methodology or its knowledge base/taxonomies, its governing body (CLUSIF) must be notified.
1.4	Are the related Taxonomies well defined?	yes	high	MEHARI defines Threats, Vulnerabilities, Risk Scenarios and Security Controls complete taxonomies, with a focus on horizontal ICT risks
1.5	Are the related Taxonomies expandable?	yes	high	It is possible to expand all the taxonomies. The activity, however, is not simple, because of the high degree of automation of the methodology: each vulnerability/threat/risk scenario is linked to the other taxonomies via formulas which enable a precise computation of the risk. Adding one or more of these elements requires a precise analysis about how the new element needs to be linked to the other during the risk computation. A new vulnerability space-specific, for example, will need to be linked to one or more specific threats and risk scenarios and the way the vulnerability affects the level of seriousness of the risks will need to be assessed and integrated in the formulas. Aside from what described above, MEHARI can be expanded without losing its precision.
2	**Economic factors**			

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
2.1	Does the Methodology include a risk analysis method based on financial factors?	yes	medium	MEHARI defines the impact component of the risk as dependant on Malfunctios related to business processes. Each Malfunction carries a score, defining the impact over the business process in case the Malfunction is actually triggered. The Impact metrics can be defined as the risk analyst prefers and must be consistent during the whole risk assessment iteration. MEHARI guidelines suggests to define the impact on the business processes as a financial impact, but this decision is completely up to the risk analyst: it is also possible to define more than one metric for the impact definition (could be financial and operational impact, for example). What the methodology DOES NOT offer is a direct and guided support on financial factors.
2.2	Does the Methodology support risk financing strategies for the residual risk?	yes	medium	Once the residual risk is computed (in form of treated risk scenarios) it is possible to define how the residual risk will be handled (transferred, ignored, accepted). MEHARI could hence be used in order to support insurance-based schemas to cover the residual risk.
3	**Innovation**			
3.1	Towards assessment of the supporto to concept of Technology Roadmap one in ECHO, does the methodology …	yes	low	Potentially, MEHARI could fit within the process of elicitation of the technology roadmaps, since its knowledge base is designed to be expanded and the methodology could be used to perform risk analysis over complex uses cases such as the ones elicited within Task 2.1.
3.1.1	... enable analysis of a StoryLine or a UseCase from D2.1?	yes	medium	MEHARI could be used to analyse the Use Cases of T2.1. It may be needed, however, to expand its knowledge base in order to cover more risk scenarios and potentially, more threats, vulnerabilities and security controls. Additional data would be needed from the Storylines in order to better define the business context.
3.1.2	… support the provisioning of a selection of roadmaps of ways (e.g. Controls) to reduce the risk?	yes	high	MEHARI risk treatment fits this role.
3.1.3	… enable/define linkability to tools/ICT products?	yes	Medium	MEHARI comes with an excel tool providing support for the risk analyst. RHEA developed two tools fully supporting MEHARI: an Open Source tool built for the European Space Agency, and a commercial version.
3.2	Does it support the concept of Curricula (like defined in ECHO)?	no	low	MEHARI do not define neither training programs nor capabilities
3.3	Does it support the concept of Certification Scheme (like defined in ECHO)?	no	low	MEHARI is a methodology for risk analysis and detection. The possible certification is conditioned to the necessary changes to carry out in the noncompliance of risks detected under the methodology. At the academic level, there is no explicit possibility of MEHARI certification.
3.4	Does the methodology identify transversal, inter-sector and specific skills for Curricula?	no	low	The skills a person must have to use the methodology are not made explicit. In itself, the methodology is defined so that anyone can execute it.
3.5	Does the methodology provide a basis for Training Programmes?	no	low	Training programs are not defined
4	**Qualitative Analysis**			

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
4.1	General Comments on investigated RA Framework.	MEHARI could fit as the basic methodology for the ECHO Multi-sector Assessment Framework. I tis a complete, European, detailed methodology It is expandible and provides results, while not quantitative, certainly much less prone to human errors than most fo RA methodology, thanks to the whole set of formulas linking assets types, vulnerabilities, threats and risk scenarios. MEHARI, however, is not a simple methodology and risk assessment iterations using it may require longer effort than with other, higher level, methodologies.		
4.2	Reccommendations, specific aspects to be taken into consideration.	MEHARI could fit as the basic methodology for the ECHO Multi-sector Assessment Framework. I tis a complete, European, detailed methodology It is expandible and provides results, while not quantitative, certainly much less prone to human errors than most of RA methodology, thanks to the whole set of formulas linking assets types, vulnerabilities, threats and risk scenarios. MEHARI, however, is not a simple methodology and risk assessment iterations using it may require longer effort than with other, higher level, methodologies. as a summary, MEHARI could fit the role as a starting point for the ECHO MAF. Any update to the methodology, however, must be notified to its governing body (CLUSIF). This could slow down its usage on ECHO.		

Annex 1.5 – MAGERIT

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
1	**Specific Requirements.** Does the Methodology…			
1.1.1	... enable improvement of multi-sectoral management processes for mitigation of Cyber Security risks?	no	-	-
1.1.2	... assess transversal and inter-sector opportunities and challenges?	yes	low	Available the Guide of Techniques – Compilation of different kinds of techniques that could be useful to apply the method. This book provides additional information and guides on some techniques often used when carrying out risk analysis and management projects: Techniques specific to risk analysis: ● Analysis using tables; ● Algorithmic analysis; ● Attack trees. General techniques: ● Graphical techniques; ● Work sessions: interviews, meetings and presentations; ● Delphi evaluation. ● Available a separate book proposes a catalogue - open to additions - that provides guidelines for: ● Types of assets. ● Dimensions for evaluating assets. ● Criteria for evaluating assets. ● Typical threats to information systems. ● Safeguards to be considered for protecting information systems
1.1.3	... enable a transversal vision for security countermeasures?	yes	high	Magerit is specialized in ICT risks. MAGERIT implements the Risk Management Process within a working framework for governing bodies to make decisions taking into account the risks derived from the use of information technologies. The ultimate aim of using Magerit is to make a methodical approach that leaves no room for improvisation, and not to depend on the analyst's whim.
1.1.4	… use/rely on an EU Methodology?	yes	high	OCTAVE
1.1.5	… enable benchmarking initiatives?	yes	medium	MAGERIT offers a systematic method for analysing ICT risks providing standard elements and criteria, that can be used to perform benchmarking activities. Chapter 8 anticipates some problems recurrently coming up when analysing risks.
1.2	Is the Methodology clear and well defined?	yes	high	Use of separate book to deepen topics. Version 3 of Magerit has been structured into two books and a technical guide: • Book I – The method

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
				• Book II – Catalogue of elements • Guide of Techniques – Compilation of different kinds of techniques that could be useful to apply the method. The first describes the methodology, providing core steps and basic tasks to carry out Risk Analysis and Management. The second book is the catalogue of elements, providing asset classes, valuation dimensions, valuation criteria, etc. The third book describes the practical techniques to be used in risk analysis and management projects.
1.3	Is the Methodology open source?	yes	-	The methodology is Open Source and it is available in English and Spanish at http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en
1.4	Are the related Taxonomies well defined?	yes	medium	According to ISO 31000 terminology, Magerit responds to what is called “Risk Management Process”, section 4.4 (“Implementing Risk Management”) within the “Framework for Risk Management”. In other words, MAGERIT implements the Risk Management Process within a working framework for governing bodies to make decisions taking into account the risks derived from the use of information technologies. Vocabulary from: [CNSS 4009:2010] Committee on National Security Systems. CNSS Instruction No. 4009. National Information Assurance (IA) Glossary [ISO/IEC 7498-2:1989] Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture [ISO/IEC 19790:2012] Information technology -- Security techniques -- Security requirements for cryptographic modules [ISO/IEC 21827:2008] Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®) [ISO/IEC 27000:2014] Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary [ISO/IEC 27031:2011] Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity [ISO/IEC Guide 2:2004] Standardization and related activities -- General vocabulary [ISO/IEC Guide 73:2002] Risk management -- Vocabulary

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
1.5	Are the related Taxonomies expandable?	yes	high	There are rules on which taxonomy has been built and rules about how to use it; there are guidelines how to expand it. A separate book proposes a catalogue of elelemts. Each section includes XML notation to be used for regularly publishing the elements in a standard format that can be processed automatically by analysis and management tools. If the reader uses a risk analysis and management tool; this catalogue will form part of it. If the analysis is carried out manually; this catalogue provides a wide starting base for quick progress without distractions or oversights. All the techniques in the Guide of Techniques can be used without automated aids; however, for repeated or com-plex use, it is recommended to use tools as widely and frequently as possible. It is important to point out that the notation proposed for applying the technique is in no case com-pulsory. Each organization may adapt to the available tools or sector specific notations.
2	**Economic factors**			
2.1	Does the Methodology include a risk analysis method based on financial factors?	yes	high	Once it has been determined which security dimensions are of interest in an asset, it must be valued. The valuation is the determination of the loss of value caused by an incident. There are many factors to be considered: • Replacement cost: acquisition and installation. • Labour cost invested in recovering (the value of) the asset. • Loss of income. • Loss of capacity to operate: lack of confidence of users and suppliers resulting in a loss of activity, or in worse economic conditions • Penalties due to non-compliance with the law or with contractual obligations. • Damage to other assets, internal or external. • Injury to persons. • Environmental damage. If the valuation is monetary, financial studies can also be made comparing what is at risk with what the solution costs by answering the questions: • Is it worth investing so much money in this safeguard?

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
				• Which group of safeguards optimises the investment? • Over what period of time is the investment recovered? • What is the reasonable cost of an insurance policy? The “Guide of techniques” gives an analysis model based on quantitative valuations.
2.2	Does the Methodology support risk financing strategies for the residual risk?	yes	medium	The “Guide of techniques” gives an analysis model based on qualitative and quantitative valuations, taking into consideration also the concept of residual risk.
3	**Innovation**			
3.1	Towards assessment of the supporto to concept of Technology Roadmap one in ECHO, does the methodology …	-	-	-
3.1.1	... enable analysis of a StoryLine or a UseCase from D2.1?	yes	high	We can use the methodology for a RA of the use cases: detailed reasoning is in D2.2. In Catalogue of Elements book, there are a lot of specific assets divided in common types of asset; there is a wide description of possible impacts wrt a scale from 0 to 10; there is a comprehensive set of threats; Safeguards are .... Mapping specific assets, vulnerabilities and impacts of the Storyline and use cases we can proceede with the following steps of RA in Magerit: Key assets have been identified: information to be dealt with and services provided Needs or levels of security have been assessed that are required for each key asset in each security dimension Other system assets have been identified It has been established the value (or the required security level) of the other assets depending on their relation with other essential assets (for example, through the identification of the premises) Possible threats on the assets have been identified

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
				The consequences have been estimated, if those threats actually occurred The likelihood that those threats actually occurred has been estimated Potential impacts and risks - inherent to the system - have been estimated The applicable safeguards have been identified to tackle potential impacts and risks The implementation of the identified safeguards has been assessed The values of residual impact and risks have been estimated, which correspond to the level of impact and risk that the system, after the implementation of the safeguards, continues to support
3.1.2	… support the provisioning of a selection of roadmaps of ways (e.g. Controls) to reduce the risk?	yes	high	Not all the assets are of the same type. The threats and safeguards are different according to the type of assets. Chapter 2 of the “Elements catalogue” gives a list of types of assets. A detailed table is intended as a guide for users uniformly valuing assets whose value is important for different reasons after taking account of: • The security of persons. • Personal information • Obligations arising from the law, from the regulatory framework, from contracts, etc. • Capacity for following up offences. • Commercial and financial interests • Financial losses. • Interruption of the service. • Public order. • Corporate policy. • Other intangible values

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
				Chapter 6 of the “Elements catalogue” gives a list of suitable safeguards for each type of asset. Safeguard types and level of effectiveness are defined with respect to specific threats divided into the following main categories: [N] Natural disasters [I] Of industrial origin [E] Errors and unintentional failures [A] Wilful attacks
3.1.3	… enable/define linkability to tools/ICT products?	yes	high	PILAR: PILAR, the Spanish acronym for “Logical Computer Procedure for Risk Analysis”, is a tool developed to the specifications of the National Security Agency to support risk analysis in information systems using the Magerit methodology. the tool calculates security ratings according to the usual de iure or de facto standards, including: • Spanish National Security Framework • ISO/IEC 27002 Security management systems • Spanish RD 1720:2007 Personal data protection In Annex, The features required from present or future tools for supporting the risk analysis and management process. All the techniques in the Guide of Techniques can be used without automated aids; however, for repeated or complex use, it is recommended to use tools as widely and frequently as possible. It is important to point out that the notation proposed for applying the technique is in no case compulsory. Each organization may adapt to the available tools or sector specific notations.
3.2	Does it support the concept of Curricula (like defined in ECHO)?	yes	low	The best security plan would be seriously undermined without the active collaboration of the persons involved in the information system, especially if the attitude is negative, and contrary or one of “fighting against the security measures”. This requires the creation of a “security culture” which, coming from top management, encourages the awareness of all those involved of its need and relevance. There are three basic pillars for creating this culture: • A corporate security policy which is understood (written so as to be understood by those who are not experts in the matter) which is published and kept updated. • Security policies that, in specific areas of activity, clarify the stance of the Organisation; i.e., defining the correct use and what non-compliance means. • Continuous training at all levels, with reminders of routine precautions and specialised activities, depending on the responsibility assigned to each job

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
3.3	Does it support the concept of Certification Scheme (like defined in ECHO)?	yes	low	Indirect objectives of Magerit is to prepare the organisation for the processes of evaluating, auditing, certifying or accrediting, as relevant in each case. Paragraph 1.8. Evaluation, certification, auditing and accrediting: This section provides a conceptual presentation of these activities. The reader will find a specific discussion of the standards relating to management systems and security products in Appendix 4.
3.4	Does the methodology identify transversal, inter-sector and specific skills for Curricula?	no	-	-
3.5	Does the methodology provide a basis for Training Programmes?	no	-	-
4	**Qualitative Analysis**			
4.1	General Comments on investigated RA Framework.	References to octave for vocabulary, asset definition, impacts: C. Alberts and A. Dorofee, “Managing information Security Risks. The OCTAVE Approach”, Addison Wesley, 2003. http://www.cert.org/octave/		
4.2	Reccommendations, specific aspects to be taken into consideration.	-		

Annex 1.6 – OCTAVE

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
1	**Specific Requirements.** Does the Methodology…			
1.1.1	... enable improvement of multi-sectoral management processes for mitigation of Cyber Security risks?	yes	medium	The OCTAVE methodology is self-directed, requiring an organization to manage its evaluation process and make information-protection decisions. An interdisciplinary team, called the analysis team, leads the evaluation. The team is composed by people from both the business units and the IT department, because both points of view are important to characterize the global, organizational view of information security risk. The analysis teams have to : • identify information-related assets (i.e. information and systems) that are critical to the organization • focus risk analysis activities on those assets deemed to be most critical to the organization • consider the relationships among critical assets, the threats to those assets, and vulnerabilities (both organizational and technological) that may expose assets to threats • evaluate risks in an operational context - how they are used to conduct an organization's business and how those assets are at risk due to security threats • create a practice-based protection strategy for organizational improvement as well as risk mitigation plans to reduce the risk to the organization's critical assets.
1.1.2	... assess transversal and inter-sector opportunities and challenges?	no	-	-
1.1.3	... enable a transversal vision for security countermeasures?	no	-	-
1.1.4	… use/rely on an EU Methodology?	no	-	-
1.1.5	… enable benchmarking initiatives?	no	low	No specific references to benchmarking activities can be found in the OCTAVE Allegro method. However the flexibility of the approach, requiring the organization to manage its evaluation process and make information-protection decisions, can be surely adapted , if of interst, to benchmark its risk management organisation and practices against a recognized international reference.

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
1.2	Is the Methodology clear and well defined?	yes	medium	There are three distinctive OCTAVE methodologies available for public use: the OCTAVE method, OCTAVE-S, and OCTAVE Allegro. OCTAVE-S approach is specifically designed for organizations of about 100 people or less. OCTAVE Allegro is the next generation of the OCTAVE methodology. Its approach differs from previous OCTAVE approaches by focusing primarily on information assets in the context of how they are used, where they are stored, transported, and processed, and how they are exposed to threats, vulnerabilities, and disruptions as a result. It is a methodology for streamlining and optimizing the information security risk assessment process; an organization can then achieve sufficient results with a limited investment of time, people and other limited resources. Allegro enables the organization to consider people, technology and facilities in the context of their relationship to the information and business processes and services they underpin. Like previous methods, OCTAVE Allegro can be performed in a workshop-style, collaborative setting and is supported with guidance, worksheets, and questionnaires. However, it is also well suited for use by individuals who want to perform risk assessment without extensive organizational involvement, expertise, or input.
1.3	Is the Methodology open source?	yes	medium	Altrough being open source it is available a commercial product, a so called "OCTAVE automated Tool" as mentioned at the ENISA page https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_octave.html. However, the links to the developers, the Advanced Technology Institute (ATI), currently (2019) do not provide information on the tool. Courses on the OCTAVE Allegro methodology can be found at the following link: https://www.sei.cmu.edu/education-outreach/courses/course.cfm?coursecode=P10B A book named "Managing Information Security Risks: The OCTAVE Approach" can be bought at the following link: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=30678
1.4	Are the related Taxonomies well defined?	no	-	Although an official taxonomy is not defined within the OCTAVE, a paper (James J. Cebula, Mary Popeck, Lisa R. Young, "A Taxonomy of Operational Cyber Security Risks Version 2", Software Engineering Institute, 2014 - https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=13473) presents a taxonomy of operational cyber security risks and studies , among the others, its harmonization with the OCTAVE method. Specifically, the paper declares that the threat categories from OCTAVE can be aligned with the classes in the proposed risk taxonomy
1.5	Are the related Taxonomies expandable?	no	-	-
2	**Economic factors**			

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
2.1	Does the Methodology include a risk analysis method based on financial factors?	no	-	-
2.2	Does the Methodology support risk financing strategies for the residual risk?	no	-	-
3	**Innovation**			
3.1	Towards assessment of the supporto to concept of Technology Roadmap one in ECHO, does the methodology …	-	-	-
3.1.1	... enable analysis of a StoryLine or a UseCase from D2.1?	yes	medium	The existing OCTAVE methods use threat trees as a guide for identifying threats. While threat trees provide a structured means for identifying and considering various threat scenarios, they can sometimes be confusing to use, especially for users with limited risk management experience. For example, each path in an OCTAVE threat tree is a generic articulation of a threat; to make effective use of these trees, participants in an OCTAVE assessment must become adept at translating these generic paths to real-world scenarios. When users fail to make this translation, it significantly affects the robustness of the identification of threats and risks. In order to overcome to this difficulties, the OCTAVE Allegro approach consists of eight steps that are organized into four phases: • Phase 1 - Establish drivers, where the organization develops risk measurement criteria that are consistent with organizational drivers. • Phase 2 - Profile assets, where the information assets that are the focus of the risk assessment are identified and profiled and the assets' containers (i.e a person, an object like a piece of paper, a techology) are identified. • Phase 3 - Identify threats, where threats to the assets - in the context of the locations where the assets are stored, transported, or processed - are identified and documented through a structured process, that begins with the analysis of the possible situations that can threaten an organization's information asset. • Phase 4 - Identify and mitigate risks, where risks to information assets are identified and analyzed based on threat information, and mitigation strategies are developed to face the risks. The OCTAVE Allegro phases enable the analysis of an EHO storyline or use case.

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
3.1.2	… support the provisioning of a selection of roadmaps of ways (e.g. Controls) to reduce the risk?	yes	medium	Since a protection strategy provides organizational direction with respect to information security activities, it is structured according to security practice areas. OCTAVE illustrate the security practise areas but it does not provide specific safeguards correlated to threats and assets. In order to overcome to this difficulties, the OCTAVE Allegro approach consists of eight steps that are organized into four phases (see above).
3.1.3	… enable/define linkability to tools/ICT products?	yes	(very) low	As reported above , ENISA speaks about the so called "OCTAVE automated Tool" (https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_octave.html) . However, the link to the developers (http://oattool.aticorp.org/Tool_Info.html) , the Advanced Technology Institute (ATI) , currently (2019) does not provide information on the tool. Any other reference to specific ICT technologies which can enable an even partial automation of the risk assessment workflow process has not be found, even if, in principle, the existence of the Tool orients us in this direction.
3.2	Does it support the concept of Curricula (like defined in ECHO)?	no	-	Although conditions are set at the level of use (i.e. the profiles of the organization personnel composing the analysis team) , there is no envisaged definition of a set of skills, curricula , training programs to raise the level of widespread Cyber Security Level.
3.3	Does it support the concept of Certification Scheme (like defined in ECHO)?	no	-	See above
3.4	Does the methodology identify transversal, inter-sector and specific skills for Curricula?	no	-	See above
3.5	Does the methodology provide a basis for Training Programmes?	no	-	See above
4	**Qualitative Analysis**			
4.1	General Comments on investigated RA Framework.	-		
4.2	Reccommendations, specific aspects to be taken into consideration.	OCTAVE is a methodology for streamlining and optimizing the information security risk assessment process; an organization can then achieve sufficient results with a limited investment of time, people and other limited resources. OCTAVE does not define a set of requirements, it does not offer /rely on a certified (EU) methodology.		

Annex 1.7 – HITRUST

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
1	**Specific Requirements.** Does the Methodology…			
1.1.1	... enables improvement of multi-sectoral management processes for mitigation of Cyber Security risks?	no	-	The HITRUST CSF **is applicable to healthcare organizations** of varying size and complexity due to incorporation of all major healthcare information security-related requirements and practices.
1.1.2	... assesse transversal and inter-sector opportunities and challenges?	no	-	The HITRUST CSF **is applicable to healthcare organizations** of varying size and complexity due to incorporation of all major healthcare information security-related requirements and practices.
1.1.3	... enable a transversal vision for security countermeasures?	no	-	Despite being a framework very targeted to the healthcare organization and not directly transversal to other sector, it is mapped and relies to some of the main framework and standards like NIST, COBIS and ISO2700 that are suitable to every organization
1.1.4	… use/rely on an EU Methodology?	no	-	The framework is mapped upon NIST, COBIS, ISO 27000 and other American standards. The GDPR is the EU Regulation upon which are mapped some Controls.
1.1.5	… enable benchmarking initiatives?	no	-	-
1.2	Is the Methodology clear and well defined?	yes	high	The HITRUST CSF is organized by 14 Control Categories, which contain 49 Control Objectives and 156 Control Specifications based on ISO/IEC 27001:2005 and 27002:2005. Each Control Specification consists of as many as three implementation levels applied to healthcare organizations according to specific organizational, system and regulatory factors. Each Control Category contains the following: • Control Reference: Control number and title. • Control Objective: A statement of the desired result or purpose to be achieved by one or more controls within a HITRUST CSF Control Category. Each control contains the following: • Control Specification: The policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature, to meet the control objective. • Risk Factor: Listing of organizational, system, and regulatory factors that drive requirements for a higher level of control. • Implementation Requirement: Detailed information to support the implementation of the control and meeting the control objective. Up to three levels of requirements are defined based on the relevant organizational or system applicability factors. Level 1 provides the minimum baseline control requirements as determined by the industry. Each additional level encompasses the lower levels and includes additional requirements commensurate with increasing levels of risk.

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
				• Control Assessment Guidance: Guidance in performing an assessment is included in the online version of the HITRUST CSF, available as Illustrative Procedures in MyCSF, to provide clarity to both assessor organizations and those adopting the HITRUST CSF (e.g., by compliance or internal audit) when validating the security controls implemented by the organization against the requirements of the HITRUST CSF. This guidance includes examination of documentation, interviewing of personnel, and testing of technical implementation. Although illustrative, these procedures should be the starting point when performing an assessment and developing a test plan. • Standard Mapping: The cross-reference between each Implementation Requirement Level and the requirements and controls of other common standards and regulations. While the document version of the HITRUST CSF release continues to consolidate mappings to its authoritative sources at the implementation level, mappings are now also provided for each industry segment. Mappings between individual HITRUST CSF implementation requirements and the HITRUST CSF authoritative sources are available in MyCSF.
1.3	Is the Methodology open source?	no	-	The framework defined by a privately held company and it isn't open source. The framework defines three level of certification. It is possible to obtain a free version of the CSF framework, you cannot determine which implementation level is required for each of the requirements unless you purchase access to the myCSF tool. This is part of HITRUST's proprietary information that you must pay to get access to. As you create an assessment object within the tool and answer the scoping factors, the tool will determine the implementation level for each requirement. If the assessment is performed by en external company, the total cost of the HITRUST Assessment is appraised $100,000 - $160,000 and assessor firms must pay an annual fee to HITRUST each year to maintain their assessor status. HITRUST Validated Assessment fees range from $40,000/yr to $250,000/yr depending on the factors associated with the assessment
1.4	Are the related Taxonomies well defined?	no	-	Althrough there isn't an official taxonomy, the framwork defines fourteen Control Categories allowing a classification of the Risks
1.5	Are the related Taxonomies expandable?	no	-	-
2	**Economic factors**			
2.1	Does the Methodology include a risk analysis method based on financial factors?	no	-	-
2.2	Does the Methodology support risk financing strategies for the residual risk?	no	-	-
3	**Innovation**			

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
3.1	Towards assessment of the supporto to concept of Technology Roadmap one in ECHO, does the methodology …	-	-	-
3.1.1	... enable analysis of a StoryLine or a UseCase from D2.1?	yes	low	The HITRUST CSF is extensively tailored for the healthcare, so the natural application of the framework is to assest the healthcare StoryLines and Use cases
3.1.2	… support the provisioning of a selection of roadmaps of ways (e.g. Controls) to reduce the risk?	yes	low	HITRST CSF defines a set of 14 security Control Categories comprised of 49 Control Objectives and 156 Control Specifications, including to provide comprehensive and prescriptive coverage over a thirty-eight (38) major information security related standards, regulations and frameworks, included as the major supporting references, but does not define a roadmap
3.1.3	… enable/define linkability to tools/ICT products?	no	-	-
3.2	Does it support the concept of Curricula (like defined in ECHO)?	no	-	-
3.3	Does it support the concept of Certification Scheme (like defined in ECHO)?	yes	high	The ECHO Certification Scheme will be based on the ENISA Certification scheme and influenced by the approach of the NIST. HITRUST CSF, being mapped upon the NIST, share the same Certification Scheme based on methods to describe organisational security functional and assurance requirements, methods to describe product security functional and assurance compliance to requirementsand methods to describe the test and evaluation procedures to validate whether or not a product meets the organisational security functional and assurance requirements.
3.4	Does the methodology identify transversal, inter-sector and specific skills for Curricula?	no	-	-
3.5	Does the methodology provide a basis for Training Programmes?	no	-	The HITRUST CSF does not define a Training Program, but there is available an HITRUST Training program designed to educate security professionals about information protection and the utilization of the HITRUST CSF® to manage risk.
4	**Qualitative Analysis**			
4.1	General Comments on investigated RA Framework.	-		
4.2	Reccommendations, specific aspects to be taken into consideration.	-		

Annex 1.8 – CYSM

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
1	**Specific Requirements.** Does the Methodology…			
1.1.1	... enables improvement of multi-sectoral management processes for mitigation of Cyber Security risks?	no	-	CYSM methodology **is specifically foreseen for ports risk management**. However, approach based on multi-scope risk analysis can be easily mutuated for different sector. Multi-sectoral risk management requires however a change in the general PoV by enabling and highlithing of multi-sector and inter-sector issues. CYSM analyses sectoral, interconnected and interdependent threats and this could be a starting point for a further extension.
1.1.2	... assesse transversal and inter-sector opportunities and challenges?	no	-	See above.
1.1.3	... enable a transversal vision for security countermeasures?	no	-	In addition to the lack of multi-sectoral approach, there is also neither identification nor isolation of transversal issues in the speficific domain, the process of asset, threat, and vulnerability can be conducted putting under evidence the transversal aspects among the several departments. The countermeasures will be quite automatically mapped in a similar transversal manner. This option could be taken into consideration when mutuating some interesting concepts.
1.1.4	… use/rely on an EU Methodology?	yes	-	CYSM announces compatibility with standards (e.g. ISO27001, ISPS code);
1.1.5	… enable benchmarking initiatives?	no	-	-
1.2	Is the Methodology clear and well defined?	yes	high	The six phases are clearly documented. The list of inputs and outputs for each phase is defined. Also the impact of personal evaluation processes is considered.
1.3	Is the Methodology open source?	yes	-	It is the outcome of an EU funded project.
1.4	Are the related Taxonomies well defined?	yes	medium	The CYSM Semantic Modeling component integrates semantic structure like ontologies and taxonomies. The safety posture of ports, the behavior of staff members with respective roles and resposabilities as well as their existing security awareness, cyber issues and tools, etc.
1.5	Are the related Taxonomies expandable?	yes	medium	Semantic content categories are defined by someone having administrative access to the content in the form of tree-like structures, even they're never created by end users.
2	**Economic factors**			
2.1	Does the Methodology include a risk analysis method based on financial factors?	yes	High	Assets are evaluated according to seven impact criteria keeping into consideration: Financial Losses (direct, indirect and long-term financial consequences), Legal Consequences (privacy issues, sensitive and personal data, commercial data, competition-related issues, private and non-disclosure agreements issues, IPR and copyright issues, etc), reputation consequences like confidentiality issues regarding organizations, their suppliers or shareholders
2.2	Does the Methodology support risk financing strategies for the residual risk?	no	-	-
3	**Innovation**			
3.1	Towards assessment of the support to concept of Technology Roadmap	-	-	-

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
	one in ECHO, does the methodology …			
3.1.1	... enable analysis of a StoryLine or a UseCase from D2.1?	yes	low	The CYSM methodology is dedicated to port management. It could be mutuated with limited effort. Unfortunately there is no chance to identify and isolate multi- and inter- sector issues from StoryLines and Use cases in lack of a considerable investment of time and people, at the current status.
3.1.2	… support the provisioning of a selection of roadmaps of ways (e.g. Controls) to reduce the risk?	yes	high	Controls and list of countermeasures are the expected outputs of the methodology.
3.1.3	… enable/define linkability to tools/ICT products?	yes	low	The CYSM system Web Interative Component, where all needed applications can run in a consistently and systematic integrated way, allows the user to inspect and retrieve information and content related to Risk Assessment (e.g. requirement, ruls, recommendation, etc.); external applications can be integrated as information sources through RSS feed or subset of functionality.
3.2	Does it support the concept of Curricula (like defined in ECHO)?	no	-	-
3.3	Does it support the concept of Certification Scheme (like defined in ECHO)?	no	-	-
3.4	Does the methodology identify transversal, inter-sector and specific skills for Curricula?	no	-	-
3.5	Does the methodology provide a basis for Training Programmes?	no	-	-
4	**Qualitative Analysis**			
4.1	General Comments on investigated RA Framework.	CYSM methodology is oriented to address the security and safety requirements of the commercial ports' Critical Information Infrastructures CII with a very effective quantitative approach.		
4.2	Reccommendations, specific aspects to be taken into consideration.	CYSM aims to introduce a valuable integrated security management system for port operators enabling asset modelling, risk analysis, anticipation/management of attacks, as well as stakeholders' collaboration. The system helps to identify, assess and treat ports' security and safety problems with a harmonized and unified approach.		

Annex 1.9 – COMPACT

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
1	**Specific Requirements.** Does the Methodology…			
1.1.1	... enables improvement of multi-sectoral management processes for mitigation of Cyber Security risks?	no	-	-
1.1.2	... assesse transversal and inter-sector opportunities and challenges?	no	-	-
1.1.3	... enable a transversal vision for security countermeasures?	no	-	-
1.1.4	… use/rely on an EU Methodology?	yes	-	COMPACT respect compatibility with EN ISO/IEC 27001 and BS ISO/IEC 27005
1.1.5	… enable benchmarking initiatives?	no	-	-
1.2	Is the Methodology clear and well defined?	yes	medium	Not every tool is defined at the present state. It will be updated in the future.
1.3	Is the Methodology open source?	yes	-	It is the outcome of an EU funded project.
1.4	Are the related Taxonomies well defined?	no	-	-
1.5	Are the related Taxonomies expandable?	no	-	-
2	**Economic factors**			
2.1	Does the Methodology include a risk analysis method based on financial factors?	no	-	-
2.2	Does the Methodology support risk financing strategies for the residual risk?	no	-	-
3	**Innovation**			
3.1	Towards assessment of the support to concept of Technology Roadmap one in ECHO, does the methodology …	-	-	-
3.1.1	... enable analysis of a StoryLine or a UseCase from D2.1?	yes	low	The COMPACT RA tools have a list of possible threats that can be updated by the users.
3.1.2	… support the provisioning of a selection of roadmaps of ways (e.g. Controls) to reduce the risk?	yes	medium	The tools themselves have a list of countermeasures for a list of cyber threats.
3.1.3	… enable/define linkability to tools/ICT products?	yes	low	COMPACT uses ICT product and adapt them for LPAs.
3.2	Does it support the concept of Curricula (like defined in ECHO)?	no	-	-

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
3.3	Does it support the concept of Certification Scheme (like defined in ECHO)?	no	-	-
3.4	Does the methodology identify transversal, inter-sector and specific skills for Curricula?	no	-	-
3.5	Does the methodology provide a basis for Training Programmes?	no	-	-
4	**Qualitative Analysis**			
4.1	General Comments on investigated RA Framework.	COMPACT aims to increase the security and safety of LPAs using existing tools adapted for Public Administration.		
4.2	Reccommendations, specific aspects to be taken into consideration.	-		

Annex 1.10 – PROTECTIVE

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
1	**Specific Requirements.** Does the Methodology…			
1.1.1	... enables improvement of multi-sectoral management processes for mitigation of Cyber Security risks?	no	-	PROTECTIVE's aim is to raise Cyber Security awareness though the improvement of security alert correlation and prioritization by a computing platform. Threat Awareness, Mission Awareness, Constituency Awareness, and Context Awareness are the fundamental keys on which the project is based.
1.1.2	... assess transversal and inter-sector opportunities and challenges?	yes	medium	PROTECTIVE system is based on the assessment of threats from different sectors, including the context of the organisations.
1.1.3	... enable a transversal vision for security countermeasures?	no	-	-
1.1.4	… use/rely on an EU Methodology?	yes	-	PROTECTIVE quotes the coherence with ENISA (European Union Agency for Network and Information Security).
1.1.5	… enable benchmarking initiatives?	yes	medium	PROTECTIVE system cross-checks through the information passed to it by its subsystems.
1.2	Is the Methodology clear and well defined?	yes	high	
1.3	Is the Methodology open source?	yes	-	It is the outcome of an EU funded project.
1.4	Are the related Taxonomies well defined?	yes	medium	The system is very well described in the deliverables.
1.5	Are the related Taxonomies expandable?	no	-	-
2	**Economic factors**			
2.1	Does the Methodology include a risk analysis method based on financial factors?	yes	medium	It uses Multicriteria Decidion Aiding which research is extended to various disciplines, including economic.
2.2	Does the Methodology support risk financing strategies for the residual risk?	no	-	-
3	**Innovation**			
3.1	Towards assessment of the support to concept of Technology Roadmap one in ECHO, does the methodology …	-	-	-
3.1.1	... enable analysis of a StoryLine or a UseCase from D2.1?	yes	high	The PROTECTIVE system is set to constantly receive information about threats and it ranks them in priority lists, sharing them within a trustable community.
3.1.2	… support the provisioning of a selection of roadmaps of ways (e.g. Controls) to reduce the risk?	yes	medium	The system is designed to evaluate the risks and report meta-alerts to reduce and constrast them.
3.1.3	… enable/define linkability to tools/ICT products?	no	-	

	CRITERIA	ADOPTED	LEVEL OF ADOPTION	SPECIFICATIONs
3.2	Does it support the concept of Curricula (like defined in ECHO)?	no	-	-
3.3	Does it support the concept of Certification Scheme (like defined in ECHO)?	no	-	-
3.4	Does the methodology identify transversal, inter-sector and specific skills for Curricula?	no	-	-
3.5	Does the methodology provide a basis for Training Programmes?	no	-	-
4	**Qualitative Analysis**			
4.1	General Comments on investigated RA Framework.	PROTECTIVE creates a system for Cyber Security awareness, whose purpose is to increase awareness by evaluating threats and risks from different sources.		
4.2	Reccommendations, specific aspects to be taken into consideration.	-		