Marie Skłodowska-Curie Actions (MSCA)
Research and Innovation Staff Exchange (RISE)
H2020-MSCA-RISE-2016

CYBER Security InSURancE — A Framework for Liability Based Trust[†]

Deliverable D2.2: CyberSure validation framework

Deliverable Release Date	30/06/2018
Authors	NIS, CITY, FORTH, HD, Cablenet, CNR
Responsible Person	Livia Torterolo
Reviewed by	FORTH, CITY, CNR
Approved by	PCC
Version	12
Status	Final
Dissemination level	Public

[†] This project is supported by the European Commission under the Horizon 2020 Program (2014-2020) with Grant agreement no: 734815

Table of Contents

1 Introduction

The aim of the deliverable is to develop a framework to validate CyberSure solution, which is based on the development of several criteria and the methods to validate the solution against these criteria.

Moreover, the deliverable is the output of task 2.4 “Development of validation framework”. The actual implementation and execution of the validation process, based on the outcome of task 2.4, will take place in the end of the project and will involve the CyberSure framework implemented in both E-health and Cloud pilots.

The document is divided in 5 main topics that will guide and describe how the design on the validation framework has been accomplished, from an initial analysis to the definition of validation criteria and methodology:

1. Validation framework principles and criteria
2. Technical criteria
3. Business criteria
4. Legal criteria
5. Application of the Validation Framework on the CyberSure Pilots

The first topic, ‘Validation framework principles and criteria’, is focused on the main principles and criteria we used to design the validation framework. The direction we chose is the result of a process of analysis of the context, hypothesis and considerations done in order to reach a common meaning of validation framework in this project. The outcome of this topic is the definition of a common validation approach that will be followed in the whole validation design and process.

The following topic is the ‘Technical criteria’, where technical criteria have been developed. Technical criteria involve just the platform itself with software components. Since the CyberSure platform is an integration of several tools, we need to validate it, by assessing its outputs and by defining all requirements that the platform needs, in order to pursue the project aims. The outcome of this topic is a punctual list of technical criteria that need to be verified by our solution.

In the ‘Business criteria’ topic, business criteria have been developed. Business criteria involve mainly the environment of the platform and the data and results that come from the platform which are useful to build a sustainable insurance system. The outcome of this topic is a punctual list of business criteria that need to be verified by our solution.

The following topic, ‘Legal criteria’, is about the development of a list of legal criteria that we want to assess in order to ensure that the framework we are developing does not have any legal issues regarding the data treatment, in order to validate the whole framework. The outcome of this topic is a punctual list of legal criteria that need to be verified by our solution.

In the last topic ‘Application of the Validation Framework on the CyberSure Pilots’ we have defined the application of the current validation framework, in the pilots. In particular, starting from the general criteria identified in the previous topics, we have identified a more specific and customized criterion for each pilot.

Moreover, we have defined a list of stakeholders that will contribute to the validation process, in order to make it more accurate and effective.

2 Validation framework principles and criteria

This topic is focused on the main principles and criteria we used to design the validation framework. This topic aims to figure out the context of the validation framework that will focus on the objectives of the related task (T2.4) and to define the approach that will drive the next steps of designing the validation framework for the CyberSure platform.

2.1 Objectives

2.1.1 Concept of validation

Validation is intended to ensure a product, service, or system results (or portion thereof, or set thereof) in a product, service, or system that meets the operational needs of the user. For a new development flow or verification flow, validation procedures may involve modelling either flow and using simulations to predict faults or gaps that might lead to invalid or incomplete verification or development of a product, service, or system.

A set of validation requirements (as defined by the users) and specifications may then be used as a basis for qualifying the developed CyberSure platform and its components. Additional validation procedures include those that are designed specifically to ensure that the qualified development flow or verification flow will have the effect of producing a system which meets the initial design requirements and specifications, as well as specific domain requirements and required by law regulations.

It is a process of establishing evidence that provides a high degree of assurance that a product, service, or system accomplishes its intended requirements.

2.1.2 Task objective within the project

The aim of the task 2.4, is to design the validation process and the validation methodology of the CyberSure framework.

We aim to develop a framework of technical, business and legal criteria to validate the CyberSure solution, as well as the methods to be used in order to validate the CyberSure solution against these criteria.

The development of this validation framework will be driven by the main goal of CyberSure, which is to deliver a market ready solution that can enhance cyber system trust.

The actual implementation and execution of the validation process, based on the outcome of task 2.4, will take place at the end of the project and will involve the CyberSure framework implemented in both E-health and Cloud pilots.

2.2 Initial considerations and context

The CyberSure framework will be validated based on specific principals that are classified in three main categories as:

1. Technical
2. Business
3. And legal

The **technical** criteria will assess the technical compliance of the platform itself, as well as the involved hardware and software components for each pilot. The proper operation of each individual system component is already validated, and in some cases, it is even certified. However, as the platform is composed of several tools (e.g. RIS tool, CUMULUS, NESSOS, Pricing model), we need to validate the correct integration and overall functionalities. The critical goal is to ensure that the CyberSure platform can process input data, captured from the customer infrastructure and organization, and provide the user (insurance player) some accurate and significant outputs, in order to make it able to define the insurance pricing policies. Technical platform requirements mainly deal with the:

- common representation of semantics and communication interfaces
- expected inputs/outputs of each tool
- authorization
- real-time demands
- etc.

Furthermore, we also need to verify that the evaluated pilot systems can interoperate with the proposed CyberSure platform and enable the real-time monitoring of the underlying assets.

Thus, technical concepts raise, including:

- access control and privileges of the involved CyberSure components
- confidentiality, integrity, and availability of data
- anonymization of processed or exchanged personal sensitive information
- ability to install, configure, and operate the monitoring components of the CyberSure platform to the pilot system
- undisrupted functionality of the main pilot hardware and software artifacts and zero side-effects due to CyberSure monitoring
- etc.

The **business** criteria assess the CyberSure's capabilities, in order to provide fruitful results for the business sector. Two main viewpoints are considered for:

1. insurance companies
2. organizations that have to insure their information systems

For the first case, the business requirements examine the provided functionalities of the CyberSure platform for the insurance sector. More specifically, they rate which data and results may be useful towards a sustainable insurance system for the digital assets. For the second case, we have to measure if the market is interested in such solutions in order to forecast the future economic value. The evaluation is based on specific indicators that are detailed in the subsections below.

The **legal** criteria include the strict compliance with the European and national legislations. Specific considerations involve the procedure for gaining the legal permission to collect, process, or store data originated from the pilot systems. The explicit consent of the system owner (and/or the end user) is vital in the era of private data protection and the new

General Data Protection Regulation (GDPR). Moreover, the proposed solution must enforce cyber-security and provide adequate protection of the pilot system assets. The overall setting has to offer activity logging and accountability in order to enhance the legal inspection of the complete operation.

2.2.1 Innovativeness of the project

CyberSure's validation framework is innovative in the sense that it verifies that the various system components can operate with each other without causing any side-effects in the monitored system, while at the same time, the overall setting accomplishes the desirable business goals with respect to the applied legal context. The proposed solution aims to resolve these three issues and give specific insights not only for each one of them, but for the overall setting as well.

The main innovation of the CyberSure framework is in its semiautomatic way of collecting the information about the security risk level of the considered organisation. So far, cyber insurers rely mostly on the results of the questionnaire provided by insureds or historical records. The CyberSure framework integrates a certification checking module (CUMULUS) which is able to validate (at least some of) this information. The quantitative risk assessment helps to quickly process the data and estimate the possible losses for the insurance company. Finally, the insurance component selects the best pricing strategy.

2.2.1.1 Quantitative risk

The cyber risk analysis of CyberSure is quantitative and provides the insurance module the estimated loss from potential threats to be covered. Many cyber risk assessment methods are qualitative, e.g. they provide only a relative evaluation of risk (i.e., the one which helps only to prioritise the risks) without the possibility to estimate expected losses. Apart from providing a more useful value than a relative score, the quantitative CyberSure risk assessment module will help to identify the ways for risk mitigation and reduce cost of insurance. This approach should help both insured and insurer. The former will receive a professional advice to improve its security, reducing any residual costs and reducing the premium to pay. The insurer will face less risk and will get more convenient way to profile the insureds.

2.2.1.2 Certification

The quantitative way of risk computation relies a lot on the correctness of the input values. The values provided by the insured could be imprecise or (deliberately) wrong. Therefore, CyberSure include a certification module, which aims to guarantee that the provided risk parameters are sufficient and correct. The module will provide this information during the initial risk assessment analysis, as well as dynamically, verifying that the parameters stay as the insurance contract requires. In this way, cyber insurer gets a mechanism to reduces the information asymmetry (and, up to some point, eliminate the moral hazard problem).

The certification module will also monitor the insured network in order to detect any violation that might occur, at runtime. The insured may try to hide the occurrence of an event (e.g., if uncovered reputational costs exceed the promised coverage), or simply fail to detect it. In this way, the insurer will get the real data for further analysis, as well as the assurance that the predictions were made correctly or incorrectly.

2.2.1.3 Risk analysis and insurance: an integrated process

Based on the initial risk assessment, pricing for the cyber insurance policies is determined. As the risk is evaluated dynamically, certain stipulations in the contract may enforce that the risk score stays above a certain threshold to ensure the same premiums and deductibles. Events or omissions from the insured party that may compromise the cyber risk score should also be taken into account in pricing, either in the form of increased deductibles, or increased prices for the duration that the cyber risk score is below the threshold. The quantitative nature of the cyber risk score is ideal for the dynamic determination of pricing and adjustments and will be taken into account in the development of the pricing models.

2.2.2 Issues on validation

2.2.2.1 Quantitative risk

- **Precision**

Risk assessment is not an easily verifiable process. Therefore, we are going to work with the pilot domain experts to check if the results of the risks assessment are reasonable. The analysis is quantitative, which means that the CyberSure platform will manage numbers, making possible a good level of precision and the opportunity to compare results in different scenarios and environments.

- **Simplicity**

Risk assessment requires a lot of effort and it is a time consuming process. We will test our risk assessment model to evaluate whether the CyberSure risk assessment module makes the process simpler.

- **Improvement specification**

The insurance company may suggest installation of additional countermeasures in exchange to insurance price (premium) reduction. We will test if our risk assessment module may help in this task.

2.2.2.2 Certification

- **Static verification of cyber insurance contract**

The certification module is intended to detect whether security features are actually in place and operate as defined. Also, the certification module has to detect changes in the work of security features during the contract period and notify about any changes detected.

- **Event occurrence collection**

The certification modules are going to collect the information about cyber security events and provide it to the interested party. We will test how much useful information could be provided to the insurer and how it may help in analysis of the further claims.

- **Required resources and trust**

Security monitoring often relies on many assumptions and requires additional investments. In the validation we will check the easiness of certification module deployment and maintenance and the amount of trust (e.g., to insured) required to ensure reliable results provided by the module.

2.2.2.3 Risk analysis and insurance: an integrate process

Having access to the quantitative risk assessment and the certification that checks whether security features are in place, it enables the insurer to estimate more accurately the cyber risk for each insured party and price their policies accordingly. In addition, by suggesting or encouraging the use of certain security features, it provides an added benefit both in reducing premiums for the insured and in increasing the overall cyber security of the portfolio. With these mechanisms in place, both the insurer and the insured can continuously assess their cyber risk and take the necessary actions to reduce the risk, a net positive for all parties.

2.3 Hypothesis on validation

In the design of the validation process, we have taken into account three validation approach alternatives, which are: (i) the mathematical demonstration; (ii) the experimental demonstration; and (iii) the comparison with other models.

After a first evaluation, considering the peculiarities of the project and the level of innovativeness, we have concluded that it is not possible to run just one of these 3 approaches, in their whole, to carry on the validation of CyberSure. In particular:

- The comparison with other models approach is discarded, due to the fact that there is no any other similar model to compare our approach with.
- The mathematical approach presents some limitations because it is possible to test and verify a single algorithm (i.e. the mathematic function that receives in input some parameters and provide a risk value as an output) but it may be a limiting approach if we are managing risk: it is necessary to validate the methodology, besides the strictly mathematical function. Indeed, the mathematical verification is only a part of the framework validation: it is necessary to validate that a specific outcome corresponds to a reliable, realistic risk.
- An experimental approach itself is not enough to validate a complex project like this one.

So, by discarding the more traditional approaches, we decided to design a customised validation approach based on the project peculiarities and needs, which takes into account the cybersecurity context and the related issues figured out in the previous paragraphs.

2.4 Validation approach

The validation approach designed, consists of combining different verification approaches that are detailed as followed:

- **Mathematical demonstration**

  The mathematical validation of the components has been performed internally and will be reported again in deliverable D3.1. The mathematical validation of the integrated CyberSure platform will be performed in the same deliverable as well. In particular, we are going to show how the results produced by one module are served as a valid input for another one and discuss limitations of the approach.

  Moreover, we are going to apply the four core components (CUMULUS, NESSOS, RIS and Pricing module) to the two pilot case studies to demonstrate how they operate separately and together in the specific context. This demonstration is primarily

focussed on the core features of the components (and the platform in general) and ensures that the results are correct and useful.

- **Experimental approach**

  We will also validate the CyberSure framework by applying it in the Healthcare and Cloud case studies. This deliverable defines the goals and means of such validation. The results will be reported in Deliverables D2.4 and D2.5. The experimental validation will help us to analyse the operational issues (such as simplicity of the method, required time and effort, the amount of human involvement, etc.).

- **Comparison with other models**

  CyberSure is an innovative project and aims to provide a new approach for cyber insurance, therefore, there are no other models available to compare our platform with. Even though cyber insurers use their own models to assess clients and set up premiums, these models are private and with inadequate data available for the analysis, the models are considered as intellectual properties and are not available for analysis.

  On the other hand, the comparison of the four separate modules (CUMULUS, NESSOS, RIS and Pricing module) with state of the art models, will be performed in the D3.1 deliverable.

  The main objective of the validation is to assess whether or not the whole platform is able to carry on with its main functions, in order to address successfully the technical and business aims related to the CyberSure framework, and to guarantee the compliant with current laws and regulations.

For this reason, the validation process is divided into 3 steps: technical validation, business validation and legal validation.

In the validation process we will carry on firstly the technical validation, then the business validation and finally the legal validation.

For the technical validation, since the single tools CUMULUS, NESSOS, RIS and Pricing module) are already validated, the validation approach should focus on assessing their integration, and that the CyberSure platform as a whole works effectively, from a technical point of view.

For the business validation, the validation approach aims to evaluate the business idea of the project. Given that the CyberSure platform works well and is able to provide an accurate risk score, we have to assess the profitability and sustainability of the business model, in relation to the market and the customer attractiveness. In fact, the objective of the project is to develop a market-ready solution, thus we will verify all the related aspects.

For the legal validation, the validation approach aims to verify the platform's compliant with all European and national laws and regulations, including GDPR.

In order to develop the validation criteria, we will start by defining the main technical, business and legal key (success) factors involved in the CyberSure platform. Subsequently, we will exploit all related issues in the validation and measurement of these factors.

This process will lead to the development of a punctual list of technical, business and legal criteria, involved in the actual validation.

3 Technical criteria

This section aims at defining a set of technical criteria that we want to verify in order to ensure the project outcomes and in order to validate the whole framework. The technical criteria refer to the individual modules as well as to the platform as a whole.

The main objective of technical criteria for validation is to assess whether the platform is able to process and produce reasonable results.

3.1 Objectives

3.1.1 Objectives on technical validation

From the technical point of view, the CyberSure platform has to be validated in terms of:

- Methodology and functionalities
- Software components
- Infrastructure
- Integration and communication

Any elements of the previous list must be individually considered and analysed to obtain a successful validation of the whole framework.

3.2 Development of technical criteria

The validation of the platform has to be considered as an integration of the validation process of the tools.

This means that every single tool, which has a specific function within the framework, must be able to interface effectively with others and at the same time be able to pursue the defined goals.

3.2.1 Key technical factors

The main modules involved in the platform, which need to be validated are:

- CUMULUS
- RIS
- NESSOS
- Pricing module

We need to analyse which are the main key technical factors critical to make the whole CyberSure framework properly work.

3.2.1.1 CUMULUS

CUMULUS is a tool that is used to monitor security controls of IT infrastructures. The Monitor component of CUMULUS communicates with the client infrastructure through a VPN connection. VPN will offer a confidential network channel, for data exchange with external parties. PI will capture the evidence required by the monitor, by using an event captor, encrypt it and send it to the CUMULUS Monitor through the Event Bus. The Event Bus will enable the communication of events to CUMULUS and will forward them to appropriate monitors depending on event subscriptions.

Thus, we need to verify that the evaluated pilot systems can interact with the proposed CyberSure platform and enable the real-time monitoring of the underlying assets. As a result, the technical key factors to be evaluated include:

- Ability to install, configure, and operate the event captors to the pilot system.
- The minimum disruption of the functionality of the main pilot hardware and software by the CyberSure monitor.
- Ability to create a secure environment that will include authorization and authentication of different event captors before transmitting events to CUMULUS. This will prevent CUMULUS from receiving and analysing events which were not transmitted from one of the Pilots.

3.2.1.2 RIS

The RIS service is a web application which relies on a database, hosted on the same server.

Methodology

RIS methodology has been developed for assessment and certification of IT systems with respect to data protection and ISO 27001 standard. This methodology has been validated through its adoption in different real environments in the context of data protection and ISO27001 certification process.

Software

The RIS service relies on an Oracle Database and Oracle Application Express technology. Some specific factors must be considered in the validation of the process of risk assessment:

- Authentication and authorization mechanisms
- Validation (reliability) of input parameters
- Risk outcomes coherence: the risks highlighted by the tool must adhere to the real risks which stand on the scope of analysis
- Security in SDLC (i.e. OWASP rules)

All these aspects have been already treated during the development of the tool and the following testing phases, and will be further addressed and evaluated inside the CyberSure platform

Infrastructure

All the servers are on a virtual infrastructure that must be analysed and evaluated

- Server hardening: it is necessary to analyse the server from the point of view of OS and the main configurations.

Delivery

The RIS service must be provided in SaaS and the availability of the service must be analysed and validated.

3.2.1.3 NESSOS

The NESSOS tool is a web-based application which has the goal to evaluate risks of an organisation.

Methodology

The methodology used by NESSOS has been developed for assessment of IT systems with respect to ISO 27001 standard, but other standards could also be used as a basis for the evaluation. The methodology is based on various risk assessment standards and has been set up using statistical data from available cyber security surveys.

Software

The following factors has to be considered for the validation of the NESSOS tool:

- Authentication and authorization, to ensure that only the data owner and assigned data processor are able to see and modify the input and output data.
- Validation (reliability) of input parameters, to ensure that the tool makes it reasoning on valid data.
- Risk outcomes coherence, to ensure that the output of the risk assessment are valid approximation of real risks.
- Security in SDLC (i.e. OWASP rules), to ensure that the tool is robust and secure enough to process sensitive data.

These factors will be enforced be the NESSOS tool itself and the platform as a whole.

Infrastructure

For a reliable and secure execution of the NESSOS tool, we must also ensure that the infrastructure it is running on is reliable and secure as well.

- Server hardening, to ensure that the OS, the virtualization, and the server software are robust.

Delivery

The NESSOS tool must be integrated with other modules of the platform, thus, we need to validate its:

- Availability
- Correct interaction with other tools of the CyberSure platform.

3.2.1.4 Pricing module

The pricing module is developed to estimate the price for various cyber insurance products, based on the input provided by other components of the CyberSure platform, the prices on similar products in the market and any additional factors that may be taken into account.

Software

For the software validation some factors must be considered:

- Authentication and authorization mechanisms
- Validation (reliability) of input parameters from other CyberSure components
- Validation (reliability) of products and prices of similar cyber insurance products from competitors' intelligence
- Policy outcomes coherence: the designed cyber insurance products adhere to the real situation, the technical configuration of the customer organization, allow to

define the level of security in the customer's services, and accordingly the product and pricing

- Security in SDLC (i.e. OWASP rules)

All these aspects will be further addressed and evaluated inside the CyberSure platform.

Infrastructure

All the servers are on a virtual infrastructure that must be analysed and evaluated

- Server hardening: it is necessary to analyse the server from the point of view of OS and the main configurations.

Delivery

The Pricing module must be integrated with other modules to receive inputs from the baseline and the comprehensive risk assessment, receive competitors' product and pricing intelligence from the market and must provide proper and adequate policies to the insurance company.

3.2.1.5 The platform - Integration and communication

A very crucial element to be considered is the way different components are going to interact and communicate to validate the CyberSure platform as a whole: being elements born in different contexts and not designed to collaborate, the effort to make them interacting within a single platform must aim to preserve the validation levels obtained by each component separately. Integration might, potentially, introduce issues in the technical reliability of the whole solution.

From an integration point of view, it is critical to guarantee a safe and efficient communication between the components of the platform.

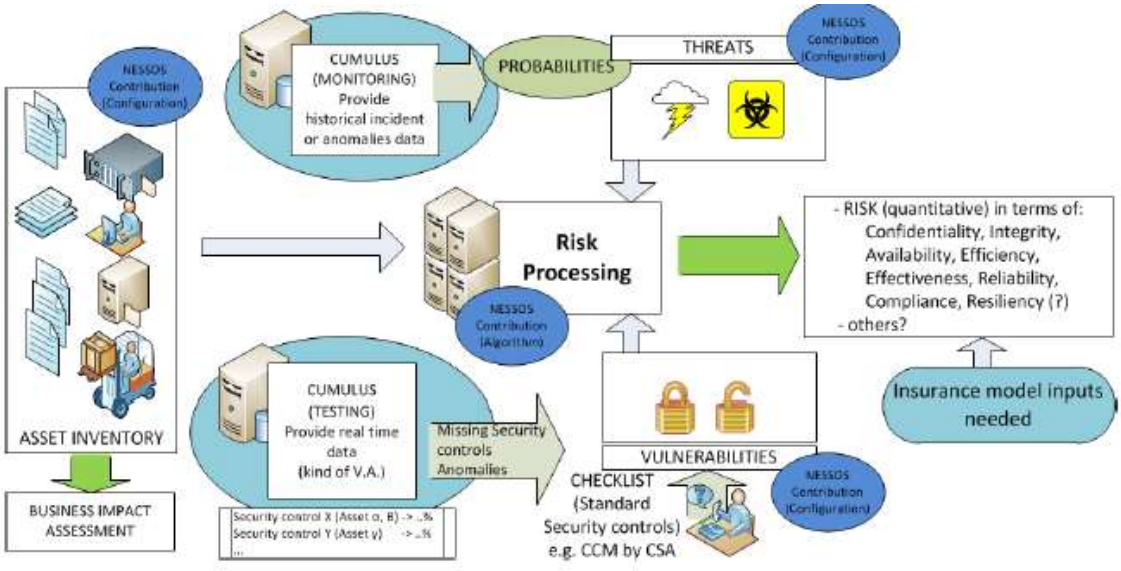

Figure 1 Comprehensive Risk Analysis

Indeed, the communication environment between CUMULUS and the RIS Tool, in order to: (a) receive the risk models developed in Baseline Risk Analysis and (b) send the certificates and/or the operational evidence generated by Certification, must take into account several security requirements including:

- A confidential network channel must be established in order to exchange data from CUMULUS to RIS tool and vice versa.
- A well-defined access controls, privileges and roles for the communication between the platform modules must be specified. This will help us identify which are the users that can use these tools and what privileges they have.
- Authorization and Authentication mechanisms for the communication between RIS tool and the CUMULUS platform. This will prevent non-authorized end-users from both sides to use features of the system that should not be available to them

3.2.2 Issues on key technical factors validation

For each key technical factor defined, which are the criticisms in assessing that factor? From a platform point of view, the following table shows the main criteria that will need to be verified during the validation process.

Criteria	Criticality
Authentication and authorization of the access to the platform	Involve a substantial group of users
Input parameters	Reliability of input parameters (human contributes)
Event captors	Obtain an access to a real environment with meaningful data
Modules connectivity and interactions	Different technologies and interfaces
Communications channels (intra)	Communications between modules involves definition of proper interfaces
Communications channels (extra)	Communications over the internet involves security issues
Security in SDLC	Make the development team aware and trained enough
Certification outcome coherence	Time. Obtain real and reliable series of historical data
Risk outcome coherence	Time. Obtain real and reliable series of historical data

3.3 Evaluations and assumptions

We assume that the single modules have been already validated, at least as standalone solutions. Moreover, the integration of them inside the CyberSure platform triggers new, possible, breach from the technical point of view: it will be necessary to evaluate the CyberSure framework as a whole and this involves a new application of some of the validation criteria used for CUMULUS, RIS, NESSOS and the Pricing module.

3.4 Technical validation criteria

Main validation criteria emerging from the analysis of the key technical factors are:

ID	Criteria	Action	Expected results
Tech-01	Authentication and authorization of the access to the platform	Verify accessibility to the system and profiles behaviours inside the functionalities of the platform	The users that have access to the CyberSure system must be properly authenticated and authorized to perform specific actions
Tech-02	Input parameters	Verify reliability of input provided to the platform (asset lists, control application levels, probability of events, etc.)	Reliability of the input parameters
Tech-03	Event captors	Verify the ability of the agent to capture all significant events on the pilot system (i.e. role-based access control policy)	The local monitoring tools at the two pilot system ends must be able to monitor the role-based access control policy for access the database of each organization (hospital and cloud provider)
Tech-04	Modules connectivity and interactions	Verify the proper implementation of interfaces	Communication interfaces make the data flows from source to destination in proper and secure ways
Tech-05	Communications channels (intra)	Verify the security of communication channels between modules	The transmitted data between the various systems must be securely encrypted via related communication protocols, like SSL/TLS
Tech-06	Communications channels (extra)	Access to the platform through secure protocols	The access to the platform will be enabled via an HTTPS connection to the platform's web interface
Tech-07	Security in SDLC	Use of security techniques during development lifecycle	The properties of the produced code should be validated by code analysis (e.g. [7])
Tech-08	Certification outcome coherence	Verify the reliability of the certificate delivery/revoke, even when CUMULUS is integrated in the CyberSure	Certification results maintain the same level of reliability of the CUMULUS tool standalone (already

		platform	validated)
Tech-09	Risk outcome coherence	Risk values are meaningful and reflect the expected behaviour of the system, even when CUMULUS is integrated in the CyberSure platform	Risk results maintain the same level of reliability of the RIS service standalone (already validated)
Tech-10	PII management	Anonymization of all the Personal Identifiable Information (PII) that may be monitored by or disclosed to the CyberSure platform	The PII must be anonymized at pilot system end (i.e. pseudonymized) before being processed by the CyberSure's components
Tech-11	Access control	Verify security measures on the interacting system points (e.g. access control and usage rights)	The platform must enforce a specific access policy (e.g. policy- or role-based) and informs the user in case of violation (e.g. [8])
Tech-12	Components	Verify that the overall overhead of the CyberSure monitoring components that are installed in the pilot system don't cause no serious performance degradation of the main pilot systems' functionality	The user of the two pilot systems (ICS-M and CABLENET's cloud) must not realize any deviation in the response time during the normal operation
Tech-13	Usability	Verify the usability of the interface and its functionalities	User-friendly interface

4 Business criteria

This topic is about the development of a list of business criteria that we want to assess in order to ensure the project results in a business point of view and in order to validate the whole framework.

The main objective of the business criteria for our validation is to measure if the market is interested in such kind of services and insurances in order to forecast the future market performances of the platform, from the insurance point of view, based on specific indicators.

4.1 Objectives

The main objective of business criteria for validation is to assess the appeal of cyber insurance products and associated services in the market, as well as to define the value proposition of the platform that would allow us to capture enough market share to make the project financially viable.

In addition, a very important goal is to be able to forecast the future market performance of the platform from the insurance point of view, and how the platform can be used to estimate the risk for cyber threats and, hence, adjust the pricing of insurance policies.

4.2 Development of business criteria

4.2.1 Key business factors

The key business factors for success of the cyber insurance business include:

a) the profitability of the underwriting models,

b) the customer attractiveness of the cyber insurance products,

c) and the cyber risk score.

The insurance needs consist of the method to estimate the cyber risk of the customers, both in terms of the magnitude of the expected economic effect and of the expected frequency of each event. Utilizing the output from the CyberSure platform, and taking into account the cyber insurance market prices and the desire and prospect for growth of the company portfolio, the insurance company will price each prospective customer accordingly.

4.2.1.1 Profitability

The profitability of the underwriting models is defined as the total amount of insurance premiums collected from insured, subtracting the amounts claimed by the insured due to events that have affected the insured business as prescribed in the insurance agreement. As long as this amount is positive, this line of insurance is deemed profitable. If it is negative, then this line of insurance is a loss-making part of the business, and premiums or policies should be adjusted accordingly. The loss ratio, defined as the percentage of claims amounts over the premiums collected, is the metric commonly used in insurance business to describe the profitability. Common values for the loss ratio vary across the insurance industry and across countries. Indicative values for loss ratio in the car insurance industry in Greece vary from 60-80%, whereas in the property insurance industry in Greece and Cyprus, loss ratio varies from 10-20%. For cyber insurance, such numbers are not as readily available, due to the relatively recent and low market penetration (and need for certain insurance). Premiums are calculated with the need to balance high-frequency, low-value events, such as small car

crashes, with rare, high-value events, such as death accidents. The cyber insurance industry is peculiar in the sense that it focuses on rare, high-value events, since security breaches or information technology down-time has the ability to perturb the whole business of the customer, causing typically high economic losses, in the rare event that they do occur. The CyberSure platform aims to offer a procedure with which to estimate the cyber risks and the economic value of said events.

4.2.1.2 Customer attractiveness

The customer attractiveness of the cyber insurance products is based on a variety of factors, the main of which are the price, relatively to the competition and the insured value (sum assured), and the coverage of the insurance (i.e. under which events/circumstances would the cyber insurance reimburse the insured for their losses). Additional factors that contribute to the customer attractiveness is the ease of policy acquisition, the ease of the claims procedure and the availability and type of customer service (phone, chat, email, on-site, technical, 24-hour). The CyberSure platform aims to aid the customer attractiveness process by estimating more accurately than the competition, and in a more robust and automated way, the cyber risks and expected economic value of the insured events, hence allowing the insurer to lower the insurance premiums. In addition, through the CyberSure platform, the customer can continuously evaluate their cyber insurance risk score, and be informed of ways to further decrease this score, hence lowering the premiums and the probability for a cyber-claim, a win-win situation for both the insurer and the insured.

4.2.1.3 Risk score

The cyber risk score, the main output of the CyberSure platform, will be calculated using semi-automated tools, developed by the CyberSure collaboration, and can be monitored by both the insurer and the insured continuously. Risks are taken into account depending on their economic value and their probability of occurrence, and are frequently re-evaluated to include new cyber risks or attacks that become possible as technology progresses. The insurance business needs both factors, in order to estimate the premiums to charge, in order to be both competitive in the market, and covered in the case of an unpredictable cyber risk event.

4.2.2 Issues on key business factors validation

Criticisms in assessing each of the key business factors defined in the previous subsection are described in this paragraph.

4.2.2.1 Profitability

The profitability of the underwriting factors greatly depends on assessing the cyber risk as accurately as possible, and on the diversification of the insured portfolio. The occurrence of most risks may be random, but in certain cases, such as physical risks like the elimination of the electricity grid in an area will affect at the same time multiple insured customers, with negative consequences for the total claims cost and the ability of the insurer to reimburse simultaneously large amounts.

4.2.2.2 Customer attractiveness

The competition for customer attractiveness may result in the insurance premium prices to lean cheaper, in order to capture a higher proportion of the market. Often, this race to lower prices has problematic implications, since the premiums may end up to be insufficient to

cover the reimbursements in the case of a claim. Caution should be taken to avoid this kind of competition and keep the prices at a reasonable level.

4.2.2.3 Risk score

The cyber risk score takes into account known risks. With technology rapidly evolving by creating new inventive ways to affect the cyber risk, it is not always possible to know accurately the actual cyber risk of a customer. As a result, the cyber risk score may appear out of date, until new risk factors are taken into account.

4.3 Evaluations and assumptions

The evaluation of the key business criteria will be determined by two main factors: the market penetration and the profitability of the business. The market share of the cyber insurance products should be respectable, in order to have the cyber insurance line deemed successful. In addition, the brand awareness of the cyber insurance line should be such that potential that customers would consider this opportunity, even if they will not purchase in the end. The profitability of the business will be shown in the medium term, after cyber insurance claims have been filed and the cyber insurance line is profitable, after accounting for the claims, and the operating expenses as well.

The main assumption behind the business criteria is that the cyber risk score will capture the majority of the risk factors associated with each potential policyholder. Additional assumptions include that the regulatory climate with respect to cyber insurance will not change. Changes in regulation may force businesses to obtain cyber insurance, increasing demand.

4.4 Business validation criteria

The validation criteria to be used consist of various simulated stress tests on the portfolio for specific cyber threats. Each possible cyber threat is assumed to carry a probability of occurrence. Taking into account the probabilities for each event for each customer in the portfolio of insured policyholders, different scenarios can be simulated varying the portfolio and the perceived probabilities to ascertain the expected cost of claims over a period of time. Taking the range of this expected loss ratio can give a measure of validation of the cyber risk models and the pricing of the insurance premiums. The business criteria will be considered validated if for 95% of the scenarios the loss ratio is less than one (premiums collected are greater than incurred claims).

ID	Criteria	Action	Expected results
Busi-01	Profitability	Find price for premiums to be higher than potential claims, at an acceptable level for the expected profitability of this insurance line	Profitable loss ratio
Busi-02	Customer attractiveness	Find price for premiums to be lower than competition or improve products to be better value for money for the customer	Increase customer conversions and customer retention

Busi-03	Risk score	Estimate cyber risk score using CyberSure tools, enabling customers to take actions to improve their scores and lower their premiums	Cyber score available online for customers and premiums adjusted accordingly

5 Legal criteria

The main objective of legal criteria for validation is to verify that the platform CyberSure is compliant with all European and national laws and regulations, including the new GDPR for privacy.

5.1 Objectives

The aim is to develop a list of criteria that will guide the design and development of the platform and then that will assess the legal compliance of the platform.

The main requirements are related to the processing of data which fall under Article 4(2) of the GDPR which define processing as “any operation performed upon data”, and it comprises the many possible actions in the data lifecycle.

5.2 Development of legal criteria

5.2.1 The analysis of legal landscape relevant for CyberSure

5.2.1.1 Provider (insurance) and Customer

There is an existing market for cyber insurance with leading insurance and re-insurance players active in the space. The legal framework is not dissimilar to other insurance sectors such as life or health. The most important aspects of the legal framework is a clear distinction between what is and is not covered in each policy, exclusions, limits and sub-limits of cover and deductibles. Also very important is making explicit what kind of risks can be covered, for example currently no single insurer is willing to cover electricity providers (these kind of insurance contracts are created under special treaties with a consortium of insurance and re-insurance providers). The only new regulation that is still not clear how it will be addressed is GDPR which relates to personal data.

According to the General Data Protection Regulation (GDPR, https://www.eugdpr.org) any data collected about customers can only be collected, used and kept for the intended use it is collected for, with the explicit opt-in consent of the customer. For example, marketing follow-up of customers who inquired for a price quotation will no longer be permitted, unless explicitly chosen by the customer. This has potential implications in the ability of the insurer to effectively market itself to potential customers. Data collected for the purpose of estimating the risk score will be governed by the same rules.

Following the directive on security of network and information systems (NIS directive, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive) ensures that the main principles of cybersecurity as outlined by the EU legislation are complied with. In addition, in the field of cybercrime, the following laws are complied with (taken verbatim from https://cyberwiser.eu/cyprus-cy):

1. The Law ratifying the Convention on Cybercrime (Budapest Convention), L.22(III)/2004. This legislation covers hacking, child pornography and fraud committed via electronic communication and the Internet.
2. The Law that revises the legal framework on the prevention and combating the sexual abuse and sexual exploitation of children and child pornography, L 91(I)/2014. This legislation ratifies the EU Directive 2011/93/EE and covers child pornography, grooming and notice and takedown.

3. The Law ratifying the Additional Protocol to the Convention on Cybercrime, concerning the Criminalization of Racist and Xenophobic acts, L.26(III)/2004. This legislation covers racism and xenophobia via computer systems and the Internet.
4. The Law on the Processing of Personal Data, L.138(I)/2001.
5. Law 112(I)/2004 Regulating Electronic Communication and Postal Services.
6. Law implementing Directive 2013/40/EU on attacks against information system, 147(i)/2015.

The aforementioned laws govern cybercrime in specific illegal actions, as well as providing the legal framework for processes against attacks, hackers, fraud, racism, and child pornography. Moreover, they cover electronic communications and personal data, relevant issues for the CyberSure consortium and the cyber insurance line of business.

For legal criteria is also important to consider the customer or end user legal requirements that the platform has to be compliant with.

The general aim is to ensure the Confidentiality. Integrity, Availability and Resilience of personal data of the customer and this topic is developed more in details in the paragraph 6.2 for the E-Health pilot and in the paragraph 6.3 for the Cloud pilot.

5.2.2 Data involved

CyberSure platform will collect data about clients, which could be seen as sensitive and require special treatment according to legal requirements.

First, the platform will require data which describe an insured, including identifiable information. This information is required for the cyber insurance module to issue an insurance contract. Some financial information may be required as well. We would like to note, that for the core part of the project, i.e., specification of the premium and coverage, as well as further monitoring, this data is not necessary and we will not use them (real ones) in scope of the project. On the other hand, when the platform will be ready for use, this information will be necessary for contract underwriting.

The CyberSure platform will required data about the insurer's risks, collected in different ways. First, this is data about assets of the client and security controls applied. This information is sensitive for organisation, as it may help malicious entities to understand better the security posture of the organisation and launch more specified attack. The data we collect will come as from the insured itself, as well as from the verification engine (CUMULUS) and in both cases must be protected from possible abuse. With the latter, we acknowledge that operational data, e.g., logs or internal measurements, are also of sensitive nature for the potential client. Furthermore, the results of the verification, risk reports and even insurance proposal could be seen as sensitive information as well. They must be shared with the client only and protected as the law requires.

5.2.3 Principles and measures

During the course of our activities we will collect, store and otherwise process personal information about a variety of individuals with whom we have contact. The following principals will apply:

Data quality: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date'.

Purpose specification: 'The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose'.

Use limitation: 'Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the purpose specification principle] except:

a) with the consent of the data subject; or

b) by the authority of law'.

Security safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data'.

Please note that CyberSure will develop and maintain security policies and procedures for the platform based on ISO 27001.

Openness: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller'.

Individual participation: 'An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended'.

Accountability: 'A data controller should be accountable for complying with measures which give effect to the principles stated above'.

All the principles just described, will be implemented in CyberSure through the following measures:

Basis of the CyberSure Data Protection Policy

Based on the General Data Protection Regulation effective as of 25th May 2018.

Scope: The CyberSure Data Protection Policy sets out the requirements regarding data protection and the legal conditions which must be satisfied in relation to the processing of

personal data, where processing includes obtaining, recording, holding, altering, disclosing, transferring, destroying or otherwise using personal data.

The types of information that we may be required to handle include details of current, past and prospective employees, and their family members, service providers, suppliers, customers and any others with whom we communicate. This information may be held on paper or on a computer or other media and is subject to certain legal safeguards specified in GDPR and other regulations. The GDPR sets out how that information should be handled and imposes restrictions on how we may use it.

The Data Protection Policy and relevant documents are living documents which will be monitored, reviewed, updated, and audited by the Cablenet Data Protection Officer to ensure compliance.

Policy Statement

CyberSure takes its responsibilities under the GDPR and the requirement to treat personal information in an appropriate and lawful manner very seriously and as such, complies with the data protection principles.

In General terms it is CyberSure's Policy to:

- Process personal information fairly and in accordance with applicable laws
- Inform (either directly or in our policies) about how we will use the subject's personal information;
- Only collect personal information from when we need it for legitimate purposes, or legal reasons;
- Ensure that all personal information is adequate, relevant and not excessive for the purpose for which we collect it;
- Not keep personal information for longer than we need to;
- Keep personal information secure, and limit the people who can access it;
- Ensure that the subject knows how to access their personal information and exercise their rights in relation to it, including being able to keep it accurate and up-to-date; and
- Ensure that any third parties we share personal information with take appropriate steps to protect it.

Requirement: Cablenet will supply the Data Protection Officer for this project. Once the Platform has been developed and the activities are clear within the platform, Cablenet will develop the Data Protection Procedures required to comply with GDPR by performing Data Protection Impact Assessments (DPIA's) for all activities concerning data subjects and their rights.

5.3 Legal validation criteria

Main validation criteria emerging from the analysis of the key legal factors are:

ID	Criteria	Action	Expected results
Lega-01	GDPR	- Update communication policy according to GDPR guidelines, acquiring explicit consent from customers to receive promotional emails - Assign data protection Officer duties to Marios Panayiotou from Cable. Implement GDPR framework. Deliver GDPR training, Information and awareness to consortium to ensure compliance at all levels	Compliance with GDPR, keep customers who wish to receive promotional emails
Lega-02	NIS directive	Adhere to the main principles of cybersecurity	Compliance with NIS, secure against cases of cybercrime
Lega-03	L.22(III)/2004	Set protections against hacking and fraud via electronic communications	Compliance with law
Lega-04	L 91(I)/2014,	Set protections for preventing and combating sexual abuse, exploitation and pornography	Compliance with law
Lega-05	L.26(III)/2004	Set protections for preventing and combating racism and xenophobia	Compliance with law
Lega-06	L.138(I)/2001	Ensure respect for personal data, largely superseded by GDPR	Compliance with law
Lega-07	L.112(I)/2004	Adhere to regulations for electronic communications and postal services	Compliance with law
Lega-08	Directive 2013/40/EU	Set protections for attacks against information systems	Compliance with law
Lega-09	Data management	Specific description of which data will be accessed and for what purpose, and obtain the explicit consent of the client organization.	The procedures for accessing data from the pilot systems must be compliant with the GDPR
Lega -10	Data access	Access on the minimum set of personal data that is required for the specified service and processing terms and must not have access to confidential	CyberSure must access and process only the minimum required set of personal data from the pilot systems, as derived by the GDPR's

		information	rules

Since GDPR is a new and complex regulation, we have detailed the criteria 'Lega-01', related to GDPR, with those articles of the Regulation that are involved in CyberSure platform so in this sense, they become requirements for the platform that we have to take into account.

GDPR Reference	Requirement
Article 7	Legal Consent (opt-in)
Article 12	Transparent information, communication and modalities for the exercise of the rights of the data subject
Article 15	Right of access by the data subject
Article 16	Right to rectification
Article 17	Right to erasure (right to be forgotten)
Article 18	Right to restriction of processing
Article 20	Right to data portability
Article 22	Right to object to automated individual decision making including profiling
Article 25	Data Protection by design
Article 32	Security of processing-Use of suitable technical and organisational measures to secure personal data (Encryption)
Article 37	Designation of Data protection Officer
Article 44-55	Transfers of personal data to third countries or international organisations

In particular, a GDPR Policy document has been developed and procedures put in place to meet the following requirements under GDPR.

6 Application of the Validation Framework on the CyberSure Pilots

6.1 Objectives

This topic is about the development of the application methodology that will define the practical measures and specification of the validation criteria figured out in the previous topics that we will use for the validation process of the framework in pilots.

In particular, we have identified some general technical, business and legal validation criteria in the previous topics, thus, in this paragraph we will identify those technical, business and legal criteria that involves specifically CyberSure pilots.

Moreover, we identified almost 50 stakeholders that will contribute actively during the application of the CyberSure validation process.

6.2 Pilot 1: E-health

For the e-health pilot validation, CyberSure will evaluate the Integrated Care Solutions – Medical (ICS-M) software suite. In brief, the software suite is implemented by the Center for eHealth Applications & Services (CeHA), which operates in the context of FORTH. The software is based upon an open, evolvable, and scalable architecture with a modular and robust infrastructure, comprising a series of IT services and applications. It constitutes an innovative service platform providing e-health functionality across heterogeneous networks, focusing on a patient-centred, clinically-driven, healthcare delivery system. High quality international trends are applied for the structure of the Electronic Health Record (EHR), as well as for the integration with third party systems by utilizing internationally acclaimed standards and protocols (like e.g. HL7, DICOM etc.). Through its various applications and tools, ICS contributes to the treatment planning and the clinical decision support for disease management. The ICS suite is installed in 20 health service providers in Greece, including regional health authorities, hospitals, and primary care centres. The pilot system is detailed in the deliverable D2.1.

6.2.1 Technical criteria for E-health pilot

In 2011, ICS-M was certified with the **EuroRec Seal of Quality EHR Level 2** by the European Institute for Health Records EuroRec (www.eurorec.org). The Seal encompasses 50 functional quality criteria, addressing various essential functions of the EHR:

- access and security management of the system
- basic functional requirements on medication
- clinical data management
- and the generic statements focusing on trustworthiness of the clinical data

The nursing and medical applications of ICS-M have been designed for health care professionals who require the use of software within a medical context.

The integration of with the CyberSure platform should not violate the provided protection mechanisms. The key security, privacy, and dependability requirements for e-health pilot include:

1. the preservation of privacy, confidentiality and integrity of medical records in-transit and at-storage
2. the preservation of privacy, confidentiality and integrity of prescription and financial data in-transit and at-storage
3. and the preservation of a high degree of the e-health platform availability

Thus, the integration of ICS-M and CyberSure's platform must comply with the technical criteria defined in the paragraph 3.4, and the specific ones described in the following table:

ID	Criteria	Action	Expected results
EH-Tech-01	Health record access	The CyberSure platform must not have access to confidential information and EHR data	The monitoring components at the pilot end must not collect information regarding the patients' PII data and being compliant with the GDPR

6.2.2 Business criteria for E-health pilot

The CyberSure platform will provide new business services and opportunities of innovation, both for the insurance companies and the organizations that are involved in healthcare services.

One main procedure is the collection of statistical data regarding cyber-threats for the e-health domain. Currently, the healthcare sector is not a popular target for hackers. Thus, some cyber-security events (e.g. Denial-of-Service or ransomware attacks) are not frequent. It would be preferable for an insurance company if it could utilize the collected statistical information from the currently evaluated hospitals in order to update its own database and take more robust decisions regarding its insurance models and policies.

The insured organizations are also benefited under this setting. They are provided with accurate and more complete information regarding the real cyber security state, with suitable and effective suggestions for updating the current systems. The overall risk from disruptive and malicious events is reduced and the business operation is safeguarded against significant economic losses.

Thus, the integration of ICS-M and CyberSure's platform must comply with the business criteria defined in the paragraph 4.4, and the specific ones described in the following table:

ID	Criteria	Action	Expected results
EH-Busi-01	Collection of statistical data for the healthcare sector	The insurance company have to be able to collect statistical data	The insurance company could gather statistical data about various incidents that have

		regarding the frequency of real events in the evaluated healthcare organization with the additional capability to integrate this knowledge in its database and decision support systems	occurred in the healthcare domain, based on the risk assessment procedures and the interviews of the accountable personnel that have taken place prior the certification process. Then, the company can update the information in its own databases that are also considered as a main business asset
EH-Busi-02	Feasible economic risk	The overall analysis and evaluation procedures of the examined healthcare system must provide adequate information and assist the insurance company in order to establish a proper contract with low economic risk	The analysis must take into consideration the fine that is determined by the GDPR (20 million euros or the 4% of the organization's budget). For the insurance company there have to be a decent profit for certifying a hospital while the economic risk should also be low.
EH-Busi-03	Early warnings of potential certification violation by the CyberSure platform	Where possible, the insured organization must have provident warnings towards an upcoming violation of the certificate before the relevant event occurs	In case where the contract insures the availability of the main hospital's server during the working hours for the public, the CyberSure platform should inform the hospital about the potential violation of the contract before event really occurs (the server has not been maintained for some period and the possibility of malfunctioning during the next few days is high).

EH-Busi-04	Avoidance of cyber-threats	The insured organization should be provided with timely and adequate information in order to take precautionary measures and avoid cyber-threats	The monitoring controls on the pilot system should capture the personnel's login behaviour and inform the organization if the compliance with the security policy is not adhered (i.e. the password strength is not sufficient, the passwords are not changed regularly, there many failed login connections, etc.)
EH-Busi-05	Timely compensation of the insured organization	When an incident occurs that is covered by a valid contract, the insurance company must estimate the loss and pay the agreed amount of money to the involved parties in a short period of time	In case of a cyber-security incident, as the CyberSure platform monitors the runtime operation of the pilot system, it should be able to verify in short time if the agreed policies were followed or violated by the insured organization and facilitate the compensation procedure accordingly.

6.2.3 Legal criteria for E-health pilot

For the e-health pilot system, legal compliance must be assured by the following procedures:

- informed consent and voluntary participation
- confidentiality
- anonymity and privacy
- data usage/control/destruction
- minimal risk
- transfer of data to third parties
- feedback

Moreover, two main points we have identified requiring special attention and focus from an ethical point of view:

- Ensure personal data protection and anonymity for ICS-M pilot planned to take place in Greece
- Ensure compliance with legislation and directives as described in deliverable D1.2 on both the European but also the national levels of Greece where the pilot will take place

These actions include a special effort to conform to the new European data protection legislation, labelled as General Data Protection Regulation (GDPR), which will be enforceable in May 2018.

Thus, the integration of ICS-M and CyberSure's platform must comply with the legal criteria defined in the paragraph 5.3, and the specific ones described in the following table:

ID	Criteria	Action	Expected results
EH-Lega-01	Monitoring controls	Compliance with the national legislations and regulatory context (e.g. the Greek law 2472/97 regarding the processing of personal data, law 2774/99 regarding the protection of personal data in telecommunications, and article 371 of the Penal Code and the medical ethics regulation, as well as law Ε.Σ.Υ.2071/92 for the confidentiality of medical records)	All collected data from the pilot system must be anonymized in order to avoid any law violation
EH-Lega-02	Integration of the CyberSure platform and the ICS-M	The integration of the two systems must comply with the European laws and the legal directives (i.e. GDPR)	The ICS-M owner must grant its permission regarding the integration of the monitoring mechanisms with the CyberSure platform. If it is required, the healthcare organization must be also informed for the process

6.3 Pilot 2: Cloud

With regards to the cloud pilot validation, CyberSure will assess the Cablenet Cloud Services Platform, and more specifically the operation of Hosted Exchange Email service on the cyber security perspective.

The Cloud Services platform is hosted on Cablenet infrastructure exclusively in Cyprus and results in a wide range of commercial and technical benefits for the business of its customers. Cablenet local data hosting is in line with the European Union's reform regarding data confidentiality, allowing businesses to know at all times where their crucial business information is stored.

Cloud platform is deployed utilizing Cablenet's Data Centre Virtual Infrastructure (DVI). DVI is physically protected by a number of protection measures focusing on controlling physical access, mitigating power-related risks, providing air conditioning and fire suppression. One of the major roles on the provision of DVI is the heavy-duty support by the IP/Network infrastructure, which is the backbone towards providing high quality connectivity and resiliency for the DVI cloud services. Backbone/Core network operates based on multi-10G self-healing and fully meshed setup and provide connectivity over IP MPLS/VPN throughout all points of Cablenet presence and beyond. Data access is provided via multi-10G redundant connections towards the cloud blade centre depending on the data exchange traffic and needs, as well as in similar manner storage is directly connected on the cloud blade chassis for the storage/inventory.

Most specifically, Hosted Exchange Email offers custom email address & resource mailboxes, anywhere Mobile Access with Active Sync, Outlook Web App (OWA) & Outlook Client License, Secure Encryption (SSL), Active Directory and Shared Contacts, Calendar & Distribution Lists.

The pilot is described in more detail in the deliverable D2.1.

6.3.1 Technical criteria

Cloud platform and all underlying applications and stored/exchanged data, along with the integration with CyberSure functionalities, shall strictly be obeying to the following rules for every aspect:

- Data (e.g., data transferred via emails, shared contacts and calendars, other user files) must be encrypted to remain confidential both in transit and at-storage
- Data integrity (e.g., no unauthorized modification) and privacy (e.g., non-easily traceable ownership) are also mandatory. Application integrity and availability must be ensured
- Mechanisms should be in place, monitoring and reporting any abnormalities and breaches in the cloud services. Notifications of security breaches to system administrators and potentially the users (to comply with forthcoming regulations) should also be supported

Additionally, according to the European Network and Information Security Agency (ENISA) 2009 risk assessment [9], which was compiled to present the detail on benefits, risks and recommendations for information security in Cloud Computing and is widely used within and out of the EU, there is a shortlist of key recommendations and liabilities concerning both

customers and providers depending on the deployment, which must be respected by CyberSure platform.

More specifically, the below table enumerates all factors under consideration:

ID	Criteria	Action	Expected results
CL-Tech-01	Email record/content access	Verify platform does not have access to confidential information and Cloud Hosted Exchange data	The monitoring components at the pilot must not collect information regarding the customers' email content and being compliant with the GDPR
CL-Tech-02	Management of identity system and authentication platform	Verify platform supports authentication, authorization and accounting (SSL)	Pilot system shall confirm read/write permissions securely without intervening with the system as such
CL-Tech-03	Physical infrastructure security and availability	Verify power, cooling, storage, bandwidth, security appliances and other network components composing the infrastructure are healthy	Pilot should confirm availability and uptime constraints (%) securely by logger retrievals
CL-Tech-04	OS patch management and hardening procedures	Verify Operating Systems, firmware and software are up to date	Monitoring components shall compare with online/offline benchmarks after secure retrieval
CL-Tech-05	Log collection and security monitoring	Verify all system components and applications are monitored, logging events and are raising alarms for incidents	The monitoring components on the pilot shall export events for importing in parser, composing XML and ready for exporting on CUMULUS

6.3.2 Business and legal criteria

In this pilot, business and legal specific criteria are not applicable so for these kinds of criteria we can focus on the general criteria defined in the topic 4 and 5 of this document.

6.4 Stakeholders for validation

The validation process will involve real end users of the relevant systems and services and other stakeholders involved in their provision, including service providers, insurers, certifiers and regulators.

Almost 50 stakeholders will be involved in the validation of services in each of the two pilots: all the effort collected by the selected stakeholders is a really important component in the design and application of the validation framework of CyberSure.

Each type of stakeholder taken into account has a specific role in the validation process and it could be a more theoretical one or a more experimental and practical one.

As a consortium, it has been decided to consider both internal and external stakeholders that will take part of the validation participating to three different committees:

- Technical validation team
- Business validation team
- Legal validation team

Regarding the internal stakeholders, an internal technical committee, composed by project resources, will highly contribute on the technical validation of the platform.

Regarding the external stakeholders, we have considered different clusters of stakeholders that will contribute to the validation framework for business and legal aspects. For each stakeholder type, we have indicated the specific resource name or the group of people or area involved, the modality of involvement and the contribution we expect to receive for the validation framework and the impact that the stakeholder aid will have on each the validation criteria.

Table 1: list of stakeholders involved in validation

Partner	Stakeholder	Role	Number of stakeholders	Involvement	Validation criteria type
NIS	Senior IT consultant	Solution Architect	2	Evaluation of CyberSure platform - software integration architecture	Technical
CNR	Senior IT consultant	Solution Architect	3	Evaluation of CyberSure platform - software integration architecture	Technical
CITY	Senior IT consultant	Solution Architect	3	Evaluation of CyberSure platform - software integration	Technical

				architecture	
FORTH	Center for eHealth Applications and Services	Stakeholders from E-Health pilot	10	Development and installation of the integration care solution (ICS) suite	Technical
CABLENET	Cloud IT managers	Stakeholders from Cloud pilot	5	Development and installation of the platform for the cloud solution	Technical
HD	2 Hospitals (a small size and a large one)	Stakeholders from E-Health pilot	30/300	Evaluation of platform outcomes	Business
	HD customers		15	Survey to customers about their potential interest in the CyberSure platform	Business
FORTH	2 Hospitals (a small size and a large one)	Stakeholders from E-Health pilot	30/300	Evaluation of the ICS suite	Business
NIS	EBIT S.r.L - Esaote Group	Stakeholders from software company in e-heath sector	3	Evaluation of software integration architecture	Business
CABLENET	Senior security manager	Stakeholders from Cloud pilot	5	Evaluation of platform outcomes	Business
CABLENET	Senior security manager	DPO	1	Evaluation of GDPR-related legal criteria	Legal
NIS	Third party Legal Office	Law Firm	3	Evaluation of legal criteria	Legal
	External	DPO	1	Evaluation of GDPR	Legal

	Senior security consultant advisor			compliance aspects	
HD	Senior security manager	DPO	1	Evaluation of legal criteria	Legal

7 Conclusions

The present document is the design of CyberSure Platform validation, based on the current state of the pilot implementation and deployment.

This validation will serve as the basis for the Initial and Final Validation of CyberSure Solution and final validation of the CyberSure platform that will take place subsequently and will be documented in the deliverables D2.4 “Initial Validation of CyberSure Solution” [month 30] and D2.5 “Final Validation of CyberSure Solution” [month 44].

Any changes of the validation framework that might occur during the validation process will be documented in the relevant deliverables.

8 References

[1] GDPR Portal, 2018, https://www.eugdpr.org/ .

[2] M. Krotsiani, C. Kloukinas, and G. Spanoudakis, "Cloud certification process validation using formal methods," 15th International Conference on Service Oriented Computing (ICSOC), Malaga, Spain, 13-16 November, 2017, pp. 65-79.

[3] Consortium, "CyberSure Description of Action," 2017.

[4] F. Innerhofer-Oberperfler, R. Breu, "Potential rating indicators for Cyberinsurance: an exploratory qualitative study".

[5] A.Marotta, F.Martinelli, S.Nanni, A.Orlando, A.Yautsiukhin, "Cyber-insurance survey," Computer Science Review, vol. 24, May 2017, pp. 35-61.

[6] S.A. Butler, "Security attribute evaluation method: a cost-benefit approach," 24th International Conference on Software Engineering, (ICSE'02), ACM Press, 2002, pp. 232-240.

[7] G. Hatzivasilis, I. Papaefstathiou, C. Manifavas, "Software Security, Privacy and Dependability: Metrics and Measurement," IEEE Software, IEEE, vol. 33, issue 4, 2016, pp. 46-54.

[8] G. Hatzivasilis,I. Papaefstathiou, D. Plexousakis, C. Manifavas, N. Papadakis, "AmbISPDM: Managing Embedded Systems in Ambient Environment and Disaster Mitigation Planning," Applied Intelligence, Springer, vol. 48, issue 6, 2017, pp. 1623-1643.

[9] ENISA, "Incentives and barriers of the cyber insurance market in Europe," available via http://goo.gl/BtNyj4 on 03/01/2017, June 2012.

[10] R. Anderson, R. Böhme, R. Claytin, T. Moore, "Security economics and the internal market," available via https://www.enisa.europa.eu/publications/archive/economics-sec/at_download/fullReport on 03/01/2017, January 2008.