Project Title	Wide – Impact cyber Security Risk framework
Project Acronym	WISER
Grant Agreement No	653321
Instrument	Innovation Action
Thematic Priority	Cybersecurity, Privacy & Trust, Risk Management, Assurance Models
Start Date of Project	01.06.2015
Duration of Project	30 Months
Project Website	www.cyberwiser.eu

<D7.4 - MARKET VALIDATION PLAN>

Work Package	WP 7, Market Validation and Roll-Out to Other Verticals
Lead Author (Org)	Timea Biro (TRUST-IT)
Contributing Author(s) (Org)	Paolo Lombardi (TRUST-IT), Niccolò Zazzeri (TRUST-IT), Alberto Biasibetti (AON), Antonio Álvarez (ATOS), Jan Bastiaensens (ENERVALIS), Kari Nieminen (REXEL), Atle Refsdal (SINTEF)
Due Date	30/11/2016
Date	30/11/2016
Version	1.0

Dissemination Level

X	PU: Public
	PP: Restricted to other programme participants (including the Commission)
	RE: Restricted to a group specified by the consortium (including the Commission)
	CO: Confidential, only for members of the consortium (including the Commission)

The work described in this document has been conducted within the project WISER. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 653321. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

Versioning and contribution history

Version	Date	Author	Notes
0.1	01.05.2016	Timea Biro (Trust-IT)	TOC created.
0.2	03.05.2016	Timea Biro, Paolo Lombardi (Trust-IT)	Revised TOC and first assignments on contributions to be provided by the involved Partners. Added proposed delivery schedule
0.3	20.05.2016	Timea Biro, Paolo Lombardi (Trust-IT)	Additions & suggestions following the WP7 call
0.4	10.06.2016	Timea Biro, Niccolo Zazzeri (Trust-IT)	Input section 1
0.5	07.07.2016	Timea Biro, Niccolo Zazzeri (Trust-IT)	Input section 2
0.6	01.09.2016	Timea Biro (Trust-IT)	Input section 1 & 2
0.7	12.10.2016	Jan Bastiaensens (Enervalis)	Input section 5
0.8	13.10.2016	Alberto Biasibetti (AON)	Input section 3
0.9	21.10.2016	Timea Biro (Trust-IT)	Input sections 4, 6, 7
0.10	31.10.2016	Jan Bastiaensens (Enervalis), Antonio Álvarez (ATOS), Atle Refsdal (SINTEF), Timea Biro (Trust-IT)	Contributions to sections 5, 8, 9
0.11	08.11.2016	Alberto Biasibetti (AON), Kari Nieminen (REXEL), Paolo Lombardi, Niccolo Zazzeri, Timea Biro (Trust-IT)	Contributions sections 3, 4, 10 – Minor edits
0.12	11.11.2016	Antonio Álvarez (ATOS)	First document review
0.12b	16.11.2016	Anže Žitnik, Aleš Černivec (XLAB)	1st internal review. Comments and minor changes
0.13	22.11.2016	Paolo Lombardi, Niccolo Zazzeri, Timea Biro (Trust-IT)	Corrections and modifications after internal review
0.14	24.11.2016	Roberto Mannella (REXEL)	Corrections and modifications after internal review
0.15	25.11.2016	Paolo Lombardi, Niccolo Zazzeri, Timea Biro (Trust-IT)	Corrections and modifications after internal review
0.16	28.11.2016	Antonio Álvarez (ATOS)	Second document review
0.17	29.11.2016	Anže Žitnik (XLAB)	Second document review

0.18	29.11.2016	Paolo Lombardi, Niccolo Zazzeri, Timea Biro (Trust-IT)	Corrections and modifications following the second document review
1.0	30.11.2016	Paolo Lombardi, Niccolo Zazzeri, Timea Biro (Trust-IT)	Final version

Disclaimer

Table of Contents

List of Tables

List of Figures

List of Acronyms & Abbreviations

Acronym / Abbreviation	Description
CWE	CyberWISER Essential
CWL	CyberWISER Light
CWP	CyberWISER Plus
FSP	Full Scale Pilots
EAP	Early Assessment Pilots
RAE	Risk Assessment Engine
RPaaS	Risk Management Platform as-a-Service
SME	Small and Medium Enterprises
UAT grids	User Acceptance Test grids
UP	User Panel
WISER	Wide-Impact Cyber Security Risk Framework
WRP	WISER Real-Time Platform

Executive Summary

A fundamental aspect of the development and roll-out of any ICT based system is to check that it actually fulfils its purpose with respect to potential stakeholders. **The aim of the validation effort is to provide objective evidence that the WISER solutions meet the intended use as detailed in the project concept and workplan.**

This document describes the WISER approach to validation. It outlines the validation plan and activities which WISER is undertaking to make sure that all the requirements have been addressed and all the expressed specifications match the user needs.
The role of validation exercise is two-fold, on the one hand it helps determine if the system meets the technical specifications (developer view) and on the other it determines whether the system meets operational business and user needs. Ultimately it supports the continuous frameworks and service improvement and helps build trust.

1 Introduction

1.1 Purpose and Scope

This document presents the WISER plan to validation highlighting the method, components and timeline used to conduct the activities.

As referenced in the WP7 objectives, validation activities should not only focus on the technical aspects but should encompass all stakeholder requirements so as to ensure that the developed system is complete and consistent.

To meet this scope, WISER structures the validation activities based on the View model. This model allows us to divide the complexity of the WISER framework into accessible perspectives, addressing specific aspects from different points of view, and accommodating the difficulties inherent in the validation and verification of complex systems.

The purpose of this plan is to present the individual validation objectives, user panels and User Acceptance Test (UAT) grids following the view breakdown for the 3 WISER Full Scale Pilots – central to the validation approach.

The validation run at the WISER Full Scale Pilots level will be rounded off with the assessment at service level, based on two types of feedback received at runtime: structured and un-structured.

Ultimately the goal is to check and validate against individual specifications defined in the design phase but also the system as a whole.

1.2 Structure of the document

The document will first give an overview of the WISER objectives related to validation and of the View model together with the rationale behind choosing this reference validation model.

The document is composed of the following sections:

- An introduction describing the context, structure and the objectives of the document
- A section detailing the approach and main components

- Individual sections 3 to 5 dedicated to the Full Scale Pilots – central to the validation approach
- EAPs dedicated section and Other feedback

1.3 Relationship to other project outcomes

The present deliverable 7.4 is produced in the context of the project WP7 - Market Validation and Roll-Out to Other Verticals, Task 7.1 Market conditions, user panels, and validation plan and feeds into the Task 7.2: Validation, carried out over project M12, May 2016, to M30 November 2017. Deliverable 7.5 "Validation Report" to be delivered in M30, November 2017, will detail the validation activities, key outcomes and the lessons learnt.

The validation approach builds on the WP2 efforts and particularly on the requirements assessment detailed in D2.1 "Requirements", D2.2 "Framework design, initial version" that established the key business and technical requirements that have been tested via the Early Assessment Pilots in WP6 and have been consolidated through the iterative process and the WISER Full Scale Pilots instantiations of the CyberWiser-Plus Service. The final version of the Requirements was released as an Annex to D2.2 and was the main outcome of the Task 2.1 Requirements, carried out during project M1 to M6, June-November 2015.

The present plan is closely tied to deliverables 6.3; 6.5; 6.7 – the first set of deliverables concerning the 3 WISER Full Scale Pilots, describing the different services under consideration to validate the WISER Framework and defining the roadmap for the implementation of the 3 FSP. A Continuous exchange is foreseen with the 3 FSP(Tasks 6.2, 6.3 and 6.4) and the validation activity (Task 7.2).

Validation outcomes will impact in Task 7.3, roll-out to other verticals, the stakeholder engagement and community development (Task 8.2), and the exploitation activities (Tasks 8.3 and 8.4)

2 WISER approach to validation

The IEEE Standard Glossary of Software Engineering Terminology (IEEE std 610.12-1990, 1990) defines validation as "The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements".

Validation determines the correctness and completeness of the end product, and ensures that the system will satisfy the actual needs and requirements expressed by the stakeholders.

Validation within WISER will be conducted at two different levels:

- At full-scale pilot level (on the 3 FSPs defined for WISER – each FSP will be a customised instantiation of the CWP service) → here validation will be conducted by the specific User Panels by means of structured UATs, presented in the following sections of the document.
- At service level (CWL, CWE, CWP) → here validation will be carried out by receiving, categorising and possibly implementing end-user feedback
    - Via input provided at runtime in the specific service User Satisfaction questionnaire
    - EAP Interviews, Family & Friends pilots, registered users, synergies from selected organisations such as ENISA
    - via direct feedback, un-structured feedback

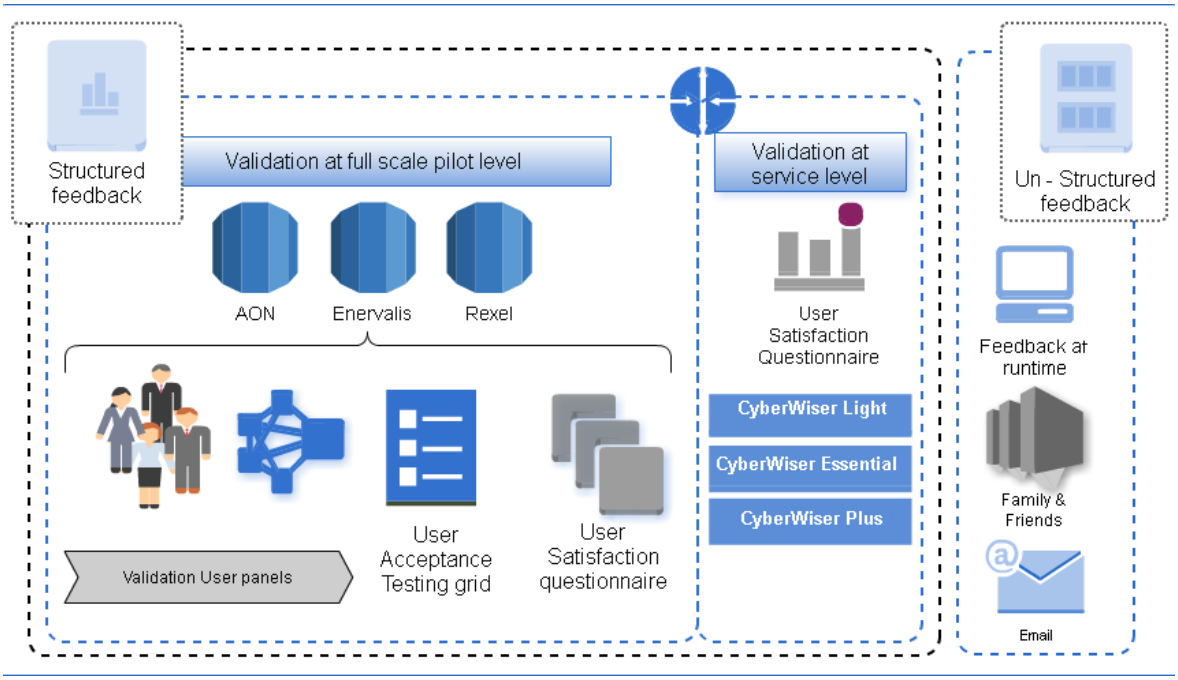

Figure 1 - WISER validation – components & tools

2.1 WISER Approach to Validation - the Methodology

2.1.1 The View model(1)

The purpose of views and viewpoints is to enable the comprehension of very complex systems, to organize the elements of the problem and the solution around domains of expertise *(2)* and to separate concerns.

Most complex system specifications are so extensive that no single individual can fully comprehend all aspects of the specifications. Furthermore, we all have different interests in a given system and different reasons for examining the system's specifications. A business executive will ask different questions of a system make-up than would a system implementer. The concept of viewpoints framework, therefore, is to provide separate viewpoints into the specification of a given complex system in order to facilitate communication with the stakeholders. Each viewpoint satisfies an audience with interest in a particular set of aspects of the system. Each viewpoint may use a specific viewpoint language that optimizes the vocabulary and presentation for the audience of that viewpoint. (2)

A viewpoint on a system involves a perspective focusing on specific concerns regarding the system, which suppresses details to provide a simplified model having only those elements related to the concerns of the viewpoint. A view (or viewpoint model) of a system is a representation of the system from the perspective of a viewpoint. For example, a security viewpoint focuses on security concerns and a security viewpoint model contains those elements that are related to security from a more general model of a system (3).

The viewpoints address different aspects of the system and enable the ‘separation of concerns’.

The WISER validation views will follow the “separation of concerns” and “requirements categorisation” done in Deliverable 2.1 “Requirements” and further refined in D2.2 & D2.3 “Framework design”, Initial and Final versions. Following the methodology described in D2.1 each requirement has a unique identifier and belongs to a specific category:

- Functional (FUNC): They describe features and functions of the technology, e.g. real time data collecting and processing, email and SMS alerting, ability to read windows event log, etc.
- Technical: they are focused on the following aspects:
    - Security (T-SECU): Requirements related to confidentiality, integrity and availability of functions and data.
    - Usability (T-USAB): Requirements related to the user experience.
    - Platform (T-PLAT): Requirements for the platform supporting the WISER solution, e.g. the IaaS cloud resources or their consumption.
    - Performance (T-PERF): Requirements dealing with the performance of the tool, e.g. the 24x7 availability of the platform.
- Legal – listing the legal requirements to be met

Based on the above mentioned breakdown the following views will be analysed:

1. FUNC: Functional View
2. T-SECU: Application Security View
3. T-USAB: Usability View
4. T-PLAT: Platform View
5. T-PERF: Performance View
6. LEGL: Legal view

The same requirements categorisation and separation of concerns will also provide the basis for the WISER User Panels definition and the **User Acceptance Test grids**, the primary tool used for validation at the level of the 3 WISER Full Scale Pilots.

Some requirements however can only be systematically tested / validated by in depth knowhow of the design and should thus be executed by the design teams. In order to keep the 4 eyes principle a designer cannot check his own development. If needed the different designer teams are invited to use the pilots as a test execution platform, in strict agreement with the pilot owner in order to avoid any adverse effects on the user infrastructure.

2.1.2 Validation of the WISER Full Scale Pilots

The WISER initiative brings forward three compelling, real-life & Full-Scale Pilots (FSPs), which will validate the WISER innovative risk management framework for cyber security.

Sections 3, 4 and 5 of the present document will give an overview of the validation for each individual WISER FSP, but in general a WISER full scale pilot needs to be understood as an instantiation of the WISER framework including sensors and the definition of the business configuration module all adapted to map the different services and needs of the 3 organisation selected for full scale piloting.

All 3 FSP, AON, REXEL and EVERVALIS, are deploying the CyberWISER Plus, the most complex and advanced mode of operation designed for the WISER Platform. As referenced in deliverables D2.4 “Framework Prototype” and D2.5 “WISER Product Strategy, initial version”, CyberWISER-Plus (CWP) is the most complex and advanced service of the WISER Portfolio. It provides evolved features of CyberWISER-Essential offering a higher degree of customization, in terms of integration with the client’s existing systems and tailoring of sensors, as well as support from the WISER

consultants team. Validation of the CyberWiser-Plus mode of operation will reflect in sync on the CyberWiser-Essential mode.

As part of the WISER approach to validation different User Panels and User Acceptance Test grids are defined for each FSP, all set to validate the framework.

2.1.3 Validation User Panels

The WISER validation user panels, one per each WISER FSP, are composed by selected representatives from the FSP supported where necessary by WISER partners.

The Validation User panel members need to be identified before starting the validation activities as the validation results depend on the composition and maximum relevance of the panel membership.

The identification of the best candidates and clear establishment of the User Panels is essential thus to facilitate the selection and enrolment of the members, specific profiles or validator categories have been identified and viewpoints as well as areas of validation defined as illustrated in the example below:

Validator category/ Profile	WISER viewpoint	Areas of validation
Service representative	Top executive/ decision maker	Functional, T-USAB: Usability view
Financial officer	Business impact	Functional, T-USAB: Usability view
CISO	CISO	T-SECU: Application Security, T-USAB: Usability
IT Architect	ICT manager	T-PLAT: Platform, T-PERF: Performance, T-USAB: Usability view
Risk Manager	Risk Manager	Functional, T-USAB: Usability view, T-SECU: Application Security view
Legal representative	Legal Officer	LEGL view
WISER Pioneer	Pioneer	Functional, T-USAB: Usability view, T-SECU: Application Security view

Table 1 – User Panels – validator categories and validation areas

The key suggested validation viewpoints are:

Top Executive/decision maker – responsible for making an informed decision based on the input provided by the Risk Manager, Legal office, and the technical team. Based on its specific profile it can cover the Functional and Usability areas / views.

Risk Manager – responsible for tailoring and implementing a specialised risk model for the organisation; the risk manager is responsible for making clear cost versus benefit analysis and advising on the security mechanisms to be implemented. The profile is associated with a complex background that would allow the validator to cover most of the areas of validation: Functional, Usability, Application Security, Platform etc.

IT Manager – is responsible for IT operations, of maintaining the integrity and availability of all Information services offered by the organisation, and thus responsible of the technical side of the

cyber risk management of the organisation. From this viewpoint the IT manager can validate critical views such as Application Security, Platform, and Performance, but not limited to this.

Legal Officer – responsible for advising on legal matters such as contracts, privacy, intellectual property, regulatory compliance; under the validation activities would cover the legal requirements/view

WISER Pioneer – is a member of the organisation that has been extensively involved in the WISER project and can perform a complete validation covering all views associated to framework

Considering the specific product/service chain of the WISER Full Scale Pilots specific validator categories are defined for each FSP as well as tailored UAT grids to ensure maximum relevance. The individual FSP sections of this deliverable detail both components, the UAT grid and validation panel membership, in relation to their organisation and specific product/service chain.

2.1.4 User Acceptance Tests (UATs)

Considered the final step before the framework is released, User Acceptance Testing (UAT), is commonly referred to as the testing methodology where the clients/end users are involved in testing the product to validate against the specifications identified the Requirements Analysis phase.

In the case of WISER in the requirements analysis phase, the first step in the verification process, the specifications were collected and defined by analyzing different categories of needs expressed across a wide range of users (referenced in in Deliverable 2.1 “Requirements” and further refined in D2.2 & D2.3 “Framework design”, Initial and Final versions).

User acceptance testing is conducted to evaluate (confirm or not) if the identified set of requirements are met. A specific user acceptance test grid will be distributed to the members of the User Panels in order to collect ratings as well as general feedback, opinions and facts concerning the WISER framework and services. Specific UAT grids are defined for each FSP User Panel validating the specific sets of concerns that are relevant for the instantiation of that particular FSP referenced in:

Appendix II: UAT Grid FSP 1- AON

Appendix III: UAT Grid FSP 2 - REXEL

Appendix IV: UAT Grid FSP 3 - ENERVALIS

The FSP UAT grids cover:

- FSP execution plan - includes references to the individual FSP validation activities
- Validation area- provides references for the category of requirements validated
- Requirement ID- references to the requirement ID as assigned in the Requirements Analysis phase
- Requirement overview – description of the requirement
- Validator details – for tracking and operational purposes
- Validator assessment marked per requirement: OK/KO | Comment for KO | Satisfaction rate – the rating provided by the validator (ok for validation; KO for non-conformity, addition comments for the KO; satisfaction rate expressed in a 3 level scale Low/Medium/High)

2.1.5 Key Performance Indicators (KPIs)

The KPIs foreseen for the project validation activities referenced in the project workplan are

- KPI7.2: Validation rate – expressed as a percentage: number of UAT requirements validated as OK / Total number of UAT requirements evaluated. KPI achieved if securing a threshold of over 90%
- KPI7.3: End-user satisfaction rate – expressed as the combined percentage of Medium and High (in a 3 levels scale: Low, Medium, High) qualitative attributes expressed by a single validators for each evaluated UAT requirement. KPI achieved if the sum of Medium and High ratings exceed a threshold of 75%

Other KPIs to be considered for reporting regard:

% of validation action executed (strictly operational) – expressed as a percentage for number of UAT requirements evaluated / Total number of UAT requirements foreseen for validation. For monitoring purposes, an intermediate milestone has been introduced in the overall validation timeline (Section 10) for May 2017 with an intermediate threshold of 70%

% of resolved remarks- expressed as the percentage of remarks (requirements initially marked as KO) resolved

2.1.6 User Satisfaction questionnaires

User Satisfaction questionnaires have been envisioned in order to gather structured feedback specific to each of the WISER Services. The user questionnaires will be run via the cyberwiser.eu web platform.

2.1.7 Validation Documentation

Documentation that refers to validation activities will be generated and stored in appropriate folder on the project repository.
The validation documentation includes:

- FSP UAT grids, with versioning and timestamp
- User Satisfaction questionnaire answers for all 3 services with versioning and timestamp
- Records of unstructured feedback received via email, direct interviews etc
- Feedback received via the ticketing system
- Intermediate analysis and checkpoint reports
- Any other documentation that needs to be referenced in the final validation plan.

3 Validation of Full-Scale Pilot 1 (AON)

3.1 Full-Scale Pilot 1 Validation Overview

3.1.1 Introduction to AON FSP

AON is the leading global provider of risk management, insurance and reinsurance brokerage, and human resources solutions and outsourcing services. It is present in over 120 countries and provides innovative and effective risk and people solutions, industry-leading global resources and technical expertise. AON has been named repeatedly as the world's best broker, best insurance intermediary, reinsurance intermediary, captives manager and best employee benefits consulting firm by multiple

industry sources.

The first of the 3 WISER FSPs, AON, focuses on Cyber Secure assessment for financial institutions, and deploys a fully customized version of CyberWISER Plus, the most advanced type of service WISER provides, for 5 different AON online services, each one characterized by the different type of data handled and processed, the number of customers served, and the uptime of the service.
For further reference, the AON Full Scale Pilot set up is detailed in deliverable D 6.3 “FSP1 - Cyber Secure Assessment Process of financial institutions, preliminary version”, released in month M12 of the project, with a final version of the report (D6.4) foreseen for M26, June 2017. .

3.1.2 Methodology – aspects particular to the AON FSP

A key objective behind the AON FSP is to validate the WISER methodological approach in a real case scenario and ensure adherence of the WISER cyber risk assessment strategy to the goals of the AON corporate business in reducing the exposure of their services to potential cyber risks and assess their potential impact.
The FSP1 takes advantage of AON’s methodology and tools for risk analysis and assessment to validate the WISER methodology, the risk modelling language, the taxonomies of risks, threats and vulnerabilities and the supporting tools in the specific contexts of AONs customers.
In addition to serving as the test environment for WISER, AON also introduces its experience in insurance models to the WISER solution and thus helps evaluate the WISER risk assessment approach, the cost-benefit analysis techniques and the impact assessment coverage to support new models of cyber risk insurance.

3.2 Full-Scale Pilot 1 User Panel

The AON FSP User Panel includes diverse profiles, Product/Service Managers, CIO, IT manager, WISER pioneers and Legal & Compliance director, covering the full array of requirements. The initial suggested structure is detailed below, referencing names, validator categories and the validation areas covered :

1. Giancarlo Baglioni, CIO – covering the T-SECU: Application Security view, T-USAB: Usability view
2. Diego Tommasi IT Manager/Architect - covering the T-PLAT: Platform view, T-PERF: Performance, T-USAB: Usability
3. Giorgio Aprile WISER Pioneer - covering the Functional view, T-USAB: Usability view, T-SECU: Application Security view
4. Alberto Biasibetti WISER Pioneer - covering the Functional view, T-USAB: Usability view, T-SECU: Application Security view
5. Romina Colciago WISER Pioneer - covering the Functional view, T-USAB: Usability view, T-SECU: Application Security view
6. Carlo Bosisio Product/Service manager – covering the Functional view, T-USAB: Usability view
7. Valeria Cecili Product/Service manager - covering the Functional view, T-USAB: Usability view
8. Conny Mastroieni Legal & Compliance Director - covering the LEGL: Legal view

3.3 Full-Scale Pilot 1 UAT grid

AON validation effort will cover all views associated to the WISER Framework and will reference in its assessment the full list of Requirements v1.3 defined under WP2.

The AON UAT grid, listing the requirements to be validated, will be annexed to this deliverable, final version dated 22.11.2016. Particular effort will be dedicated to the Functional; Platform and Usability requirements. Furthermore considering the resources AON is allocating to the validation effort, more detailed analysis on how the Legal requirements will be included in the final Validation report to be delivered as the outcome of the validation exercise.

4 Validation of Full-Scale Pilot 2 (REXEL)

4.1 Full-Scale Pilot 2 Validation Overview

4.1.1 Introduction to REXEL FSP

Founded in 1967, REXEL is a worldwide leading distributor of electrical supplies. Through its distribution networks for professional customers in the industrial, residential, and commercial sectors, REXEL provides innovative electrical solutions and equipment to improve comfort, performance, and energy efficiency.

The REXEL Pilot focuses on testing the effectiveness of the WISER approach when applied to the procurement of energy products. The testing focuses on risks deriving from a global supply network configuration.

As a distributor of electrical products and services, REXEL has procurement processes in two primary facets: REXEL procures products from suppliers and it has procurements processes for products and services with its customers.

As such, REXEL has identified five critical applications, that are used across the entire process chain to deliver products and services to its customers, that will be assessed using the WISER framework and methodology. Deliverable 6 “FSP2 - Global energy solutions procurement, preliminary version”, details the implementation of the REXEL services under evaluation and identifies what are the WISER sensors and agents that will be installed on the REXEL infrastructure. Furthermore it defines the roadmap to implement the Full Scale Pilot and identify the intermediate steps to provide an intermediate evaluation of the WISER components and functionalities. Feedback from these intermediate stages will be streamlined as well into the Deliverable 7.5 “Validation Report”.

4.1.2 Methodology – aspects particular to the REXEL FSP

REXEL will be implementing and validating the full set of tools developed within the WISER framework. The methodology to perform the validation is to provide data from all aspects of the REXEL’s environment (DNS, network, honeypot and application sensors) so that potential threats and vulnerabilities can be identified across the entire pilot scope.

This is critical to REXEL for various reasons. For example, REXEL needs to be able to not only identify potential vulnerabilities in its environment but also to quantify the potential risk that is posed. Once this risk level is identified, then REXEL can make an informed decision with respect to the urgency of remediation as well as determining the necessary resources (personnel, technology and budget) to allocate to the remediation effort.

4.2 Full-Scale Pilot 2 User Panel

A complete REXEL User Panel carrying out the validation for the FSP2 is being defined and will cover as many validation areas as possible.

1. Rolf Rönnblad, CFO / Financial officer - covering the Functional, T-USAB: Usability view
2. Roberto Mannella CISO T-SECU: Application Security viewpoint, T-USAB: Usability view

3. Kari Nieminen System Manager/IT Manager/Architect – covering the T-PLAT: Platform view, T-PERF: Performance, T-USAB: Usability view

4.3 Full-Scale Pilot 2 UAT grid

The REXEL User Panel will focus on assessing a selection of the requirements of specific importance to the REXEL FSP. The list of requirements to be validated as part of the REXEL UAT grid will be annexed to this deliverable, final version dated 22.11.2016.

5 Validation of Full-Scale Pilot 3 (ENERVALIS)

5.1 Full-Scale Pilot 3 Validation Overview

5.1.1 Introduction to Enervalis FSP

It should be understood that Enervalis is a small company which started up 3 years ago. As such there is no separate IT department and the manpower devoted to cyber security is very limited. Nevertheless, Enervalis has recognised that cybersecurity is very relevant to their market segment of cloud based energy management systems which is sensitive to security and privacy risks. As such several initiatives are running to better understand the risks, their potential impact to the business and of course take preventive actions to remediate. Participating in the WISER project is one of these actions.

For all the reasons above Enervalis will also be an excellent test case in the WISER market segment of SME's as a typical example of such company seeking for rational security improvements. As such Enervalis would certainly be a potential buyer of the WISER services.

In the course of the pilot execution, Enervalis will deploy the WISER agent and several of the WISER security sensors to monitor their Smart Power Suite® and their energy gateway which is typically deployed on the customer's premises.

For a description of the Enervalis FSP specifics please refer to WISER deliverable D6.7

5.1.2 Validation methodology aspects particular to the Enervalis FSP

Enervalis will validate the WISER platform out of the point of view of the typical SME user. In this sense it should be possible to setup and use the WISER infrastructure with the limited security knowhow which is present in an SME. The system should be easy to configure and provide relevant and easy to understand information. The overhead and configuration effort should be limited.

Rather than complete information about every possible aspect, it would be important for an SME to be easily guided to the most important security risks and mitigation actions.

Suggested mitigation actions should also be tailored to the typical SME, meaning that they should fit into the size of an organisation of 10 to 20 persons or less.

The main contribution of Enervalis in the validation process will be that we will simply implement and use the platform in the course of our FSP and formulate unstructured remarks.

Enervalis will not test all of the functional requirements systematically though. The reason for this is that either in our small organisation the knowhow to competently validate the requirement is not there

or that systematic testing of the requirement would take white or grey box knowhow on the design of the system which is simply not available to Enervalis.

Many of these requirements will however be touched during the platform usage and should any issues pop up we will use the UAT grid to report those issues.

The absence of a remark on a specific functional requirement should not be regarded as a positive validation however. The presence of a remark could be regarded as negative validation provided we believe that for our type of business the lack of functionality is critical in this case we will give a KO or not OK as validation.

In the UAT grid Enervalis took a subset of test which we think would be particularly interesting for a typical SME in our type of business. The consortium should regard these tests as our input for a simplified acceptance of the product.
We also added some tests around the bandwidth requirements of WISER sensors over a 3G network.

And we are a candidate to test some of the sensors in a controlled hack on our infrastructure and see how they would behave in real life.

5.2 Full-Scale Pilot 3 User Panel

As stated before, Enervalis is really a small company, total personnel is only 11 people. This means inherently that a full-scale user panel is difficult to assemble. A lot of central services, like the financial services, are outsourced to service providers having little understanding of what is happening inside the company. They are not dedicated personnel, but rather people who work one or two days a week for this company. They are not the people to address in order to assess a company policy around security or even understand the possible impact of cyber security on the company results.

A lot of roles existing in a big company, like the CFO, CTO are rather distributed tasks assigned partly to outside advisors and partly to the most knowledgeable persons on the subject inside the company. We also don't have a formal and dedicated CIO, nor a CISO, this task is rather performed by the most knowledgeable system architect.

What we propose to do is assemble the following user panel, for the maximum value towards the WISER project.

1. Stefan Lodeweyckx: CEO also incorporates informally the CFO functionality, will assess the wiser framework mainly on usability for his business and for the SME market in general.

   Validation category : Financial officer

2. Jan Bastiaensens: project and service manager for Enervalis will assess on usability and selected functional requirements

   Validation category : Product Service manager / WISER pioneer

3. Filip Aben: IT System architect will assess on usability, selected functional requirements and performance and also give unstructured feedback on the overall system.

   Validation category : IT manager / architect

4. Anneleen Scholts: IT System architect and specialist on front-end development will have a specific look at the user panels and will give unstructured feedback on usability

   Validation category : IT manager / architect

5.3 Full-Scale Pilot 3 UAT grid

In the UAT grid, Enervalis selected requirements which are most important to their business. Those are mainly centred on functionalities which would be naturally encountered during the normal use of the system like an SME who is **not specialised in security** would do it.

In other words, like a potential customer in this category.

What would be very important:

- Ease of use
- Ease of set-up by a non-specialist
- Easy interpretation of the results, available
- The suggestion of remedies which are very practical and ranked according to priority
- The actual prove that it does what it claims to do, namely detect an intrusion.

We are suggesting two validation tests to be performed on FSP3, but where we require the help of the partners to perform them

1. We added a requirement around data usage by the sensors. As the remote energy management business often uses 3G networks for the collection of data out of the remote meters and control devices the used bandwidth is an important factor in the business case. Therefore, the data bandwidth corresponding with the remote probes should be small with respect to the payload. We would need help from the partners to measure and assess this data usage and, if needed, suggest mitigating measures

   This would be a GO/NO GO criterion for our business

2. We propose to perform a simulated hack on our system in order to assess if the system really does what it claims to do. Namely detect an intrusion and propose effective countermeasures.

   We would need dedicated help from the partners to jointly:

   - Define the conditions so that the experiment remains under control and we don't risk a service interruption
   - Propose a method of attack
   - Execute the hack under controlled conditions
   - Monitor what is happening in the system
   - Assess the results and proposed counter measures
   - Write the report

Note that the latter material would also be an excellent marketing tool if exploited well.

As stated above, Enervalis has selected those functional requirements in the UAT grid which are most relevant to our business and which would be encountered naturally while using the system like a typical customer in a category would. The reference UTA grid, dated 22.11.2016, is annexed to this deliverable.

6 Ulterior Structured feedback from end-users received at runtime via user satisfaction questionnaires

User satisfaction questionnaires usually fall under the realm of the structured, quantitative feedback. Three different questionnaires are foreseen to collect feedback form users at runtime, one for every CyberWiser service made available.

Although they contain both open-ended as well as closed options questions the surveys run are designed to collect accurate data, that require less time and effort for interpretation and analysis.

An initial basic User Satisfaction Questionnaire was released following the launch of the CyberWiser-Light service. Users are prompted to fill in the questionnaire upon completing the CWL assessment.

The questionnaire contains 2 open-ended and 3 pre-defined options questions and is focused on gathering information about the user needs, the service usability and the user experience.

Initial version of the User Satisfaction for the CyberWiser-Light service is documented in the Appendix I. The questionnaire was published in June 2016. Users are prompted to provide feedback after using the CyberWiser-Light service.

The questionnaire is also available at https://www.cyberwiser.eu/content/feedback-cyberwiser-light

More specific and extended user satisfaction questionnaires with be associated to the more advanced CyberWiser services, CyberWiser-Essential and CyberWiser-Plus.

The answers will be coded based on a common data analysis plan. The questionnaires will be are run via the cyberwiser.eu web platform that will also provide an automatic analysis on the data.

7 Involvement of the EAPs in the validation process

In the context of Task 6.1, the Early Assessment Pilots kindly put their knowledge and experience at the disposal of the WISER Consortium, in order to steer the elicitation of requirements and the design of the WISER Framework and align them with real world needs. This interaction with remarkable advisors outside the Consortium was such a success, and their good advice was very helpful for the Consortium to envision, design and finally implement the WISER Framework (by the time this deliverable is published, the implementation is going through its final stage and the Framework prototype is actually delivered in parallel and documented in Deliverable D2.4).

Also in the context of Task 6.1, the Early Assessment Pilots were presented CyberWISER-Light, the first service of the WISER Portfolio, and they had the opportunity to interact with the tool, which was made available through cyberwiser.eu. Their feedback was positive and, again, they gave very valuable advice to refine and strengthen the tool. This is extensively documented in Deliverables D6.1 and D6.2.

Despite Task 6.1 having finished, the WISER Consortium would like to invite the External Partners to participate in the validation process of WISER Framework and Services at a more advanced piloting stage, EAPs will be contacted and invited to test the services on a training infrastructure providing in return feedback in an unstructured manner.

The validation exercise involving the EAP will not only bring valuable input for the WISER final Validation Report but it will also be seen as an engagement effort targeting potential customers that have already a consolidated knowledge of the WISER framework and should be keep informed on the project developments and the benefits they can take advantage given their role.

The EAPs play a key role in validating the WISER framework but consensus needs to be reached inside the WISER consortium on regarding the amount of effort to be dedicated and the ownership of this activity. It also needs to be noted that the EAPs have no effort assigned under the validation effort and their approval and participation to the activities will be done on voluntary basis. A specific yet simple plan on their involvement will be defined and outcomes will be included in the WISER Validation report. As foreseen at the moment an agreement will be signed between WISER and the interested EAPs, covering the offer and expected return. A training infrastructure will be provided and initial support and guidelines for usage; feedback will be collected and further actions can be carried out under WP8 with the EAPs for the service uptake.

By the end of the project, the final WISER workshop will take place. This workshop will gather relevant people from industry, academia and public institutions. The results of the project will be presented, including live demos of the WISER Services. This will take place collocated with a major event and the Early Assessment Pilots will be invited to attend.

8 Un-structured feedback from end-users received at runtime

We foresee unstructured feedback to be collected in different forms: feedback provided to partners via email, web Contact form, social media or direct exchange with users and other stakeholders.

This type of feedback is just as valuable as the structured feedback received via the questionnaires especially since it is commonly associated with a “qualitative assessment” and provide detailed insight that a closed options survey doesn’t.

The challenges for this type of feedback lie in: a) collecting the data, b) cleaning & harmonising it and c) offering an interpretation to align the feedback with the other components of the validation plan.

4 Milestones set for the collection of the unstructured feedback:

1. Initial launch of CWL - Family & Friends (March 2016)
2. Global launch of CWL (May 2016)
3. Launch of CWE (December 2016)
4. Launch of CWP (December 2016)

Both structured as well as un-structured feedback will be mapped against the View model perspectives for a consistent approach and reporting.

9 Validation of threat model algorithms

WISER will also dedicate effort to validating the cyber risk assessment algorithms developed for the risk patterns identified for the project. Each pattern captures a common type of cyber- attack and the corresponding risks. Each pattern also identifies the indicators that will provide the dynamic inputs to the assessment algorithms. The outputs from the algorithms are risk level assessments that take into account the expected frequency and impact of each unwanted incident identified in the risk pattern.

For each pattern, two different algorithms are defined: one quantitative and one qualitative. Quantitative algorithms are expressed using **R**, while qualitative algorithms are expressed using DEXi.

The definitions of the assessment algorithms are to a very large degree based on subjective judgment. There are two main reasons for this. First, we are not able to obtain the statistical data needed to establish the relation between sets of indicator values and corresponding risk levels. In fact, it is doubtful whether such data even exist. Second, even if such data were available, they would of course represent the past, and would not necessarily provide a correct representation of the future.

This does not imply that no historical data are available and useful; it simply means that we must do our best and use our judgment to define the algorithms based on whatever relevant data we are able to obtain. To allow stakeholders to determine to what degree they put confidence in the assessment algorithms, it is therefore important to be open and clear about the approach taken to arrive at these algorithms.

A reference document covering the Algorithm validation is currently being drafted; this will be followed by separate forms for each risk pattern (4). The validation of the quantitative and qualitative algorithm for each specific pattern will follow a set template and contain the following information:

- A brief description of the pattern, with reference to its full description in D3.1
- A list of the validation team members who took part in the validation, as well as the date.
- A list of the historical data sources that were taken into account when defining the algorithm.
- A presentation of the reasoning behind the algorithm, including interpretation and use of the available data and the consistency between the quantitative and qualitative versions.

A specific procedure is being defined in order to arrive at the validated algorithms. A carefully selected validation team will be involved in the process and clear steps based on the continuous exchange with the validation team will be followed. The work is performed under the WP3, WISER modelling and an account of the activities and outcomes will be included in the WISER Validation report, deliverable 7.5 scheduled for project month 30.

10 Overall validation timeline

The main pillars and foreseen timeline for the validation activities are illustrated in the figure below:

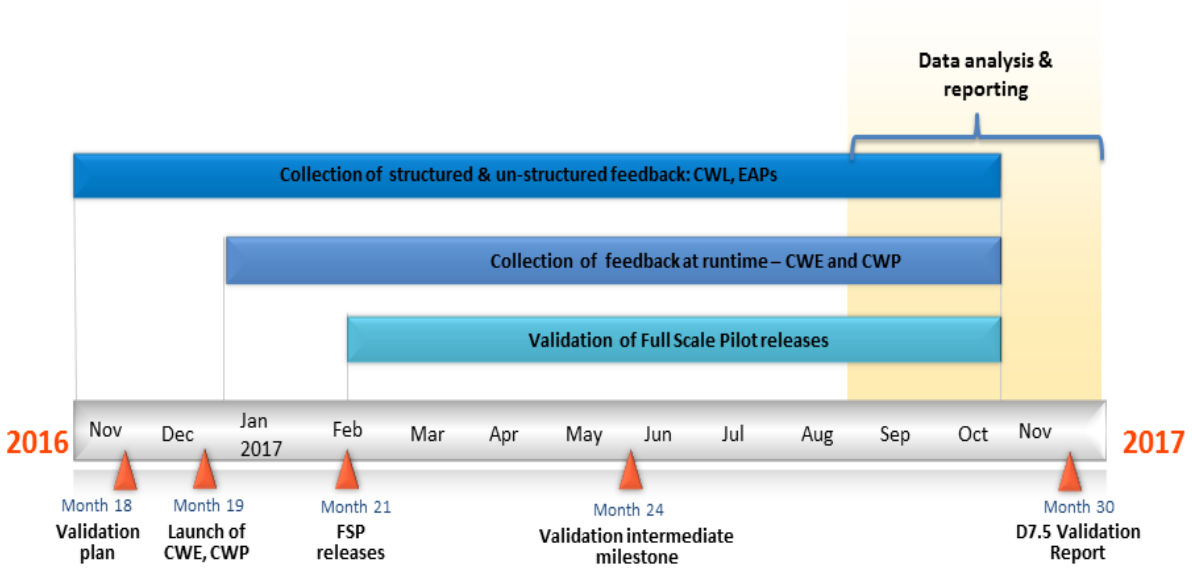

Figure 2 – WISER Validation timeline

11 References

1. **View Model**. *Wikipedia: the Free Encyclopedia.* [Online] [Cited: 1 May 2016.] https://en.wikipedia.org/wiki/View_model.
2. **Barkmeyer, Edward J. Concepts for Automating Systems Integration NIST**. *NIST: National Institute of Standards and Technology.* [Online] 2003. [Cited: 12 September 2016.] http://www.mel.nist.gov/msidlibrary/doc/AMIS-Concepts.pdf.
3. **Sinan, Alhir Si. Understanding the Model Driven Architecture (MDA).** *Methods & tools - Software Development Magazine.* [Online] Fall 2003. [Cited: 20 September 2016.] http://www.methodsandtools.com/archive/archive.php?id=5.
4. ***WISER_algorithm_validation_v01**, November2016.*

Appendix I *CyberWiser-Light User Satisfaction questionnaire*

1. What were the needs related to cybersecurity your organisation expected CyberWiser-Light to answer? *

2. Rate the CyberWiser-Light ease of use.
   Please rate on a scale of 1 to 5 where 1 is very easy and 5 is very difficult. *

3. How would you rate the usefulness of the information provided by CyberWiser-Light?
   Please rate on a scale of 1 to 5 where 1 is very useful and 5 is not useful at all. *

4. Would you recommend CyberWiser-Light to a colleague or a collaborator? *
   Yes / No / Not sure

5. How would you improve CyberWiser-Light? We would appreciate your questions and suggestions. *

Appendix II *UAT Grid FSP 1- AON*

Ref. WISER_validation_UAT_grid_FSP1_AON_v22112016

Appendix III *UAT Grid FSP 2 - REXEL*

Ref. WISER_validation_UAT_grid_FSP2_REXEL_v22112016

Appendix IV *UAT Grid FSP 3 - ENERVALIS*

Ref. WISER_validation_UAT_grid_FSP3_ENERVALIS_v22112016