

SECURE DYNAMIC CLOUD FOR INFORMATION, COMMUNICATION AND RESOURCE INTEROPERABILITY BASED ON PAN-EUROPEAN DISASTER INVENTORY

Deliverable 5.3 Validation strategy and first functional evaluation model of communication system concept

Ivan Cucco¹, Simona De Rosa¹, Antonella Passani¹, Alexander Georgiev², Jens Pottebaum³, Christina Schäfer ³, Torben Sauerland³, Katrina Petersen⁴, Ioannis Danilidis ⁵ T6 Ecosystems¹, CloudSigma², University of Paderborn³, Lancaster University⁴, Centre for Security Studies⁵

March 2016

Work Package 5

Project Coordinator

Prof. Dr.-Ing. Rainer Koch (University of Paderborn)

7th Framework Programme for Research and Technological Development COOPERATION

SEC-2012.5.1-1 Analysis and identification of security systems and data set used by first responders and police authorities







		Public				
Due date		28/02/2016				
Sent to coordinator		07/03/2016				
No. of docume	ent	D.5.3				
Name		Validation model of co	Validation strategy and first functional evaluation model of communication system concept			
Туре		Deliverable				
Status & Vers	ion	V2				
No. of pages		193				
Work package	9	5				
Responsible		T6 ECO				
Further contributors		University c (ULANC), C	of Paderborn entre for Sec	(C.I.K.), Lancaster University urity Studies (KEMEA)		
Authors		Ivan Cucco,	T6ECO			
		Simona De Rosa, T6ECO				
		Antonella Passani, T6 ECO				
		Alexander Georgiev, CS				
		Jens Potteb	aum, UPB			
		Christina So	chäfer, UPB			
		Torben Sau	erland, UPB			
		Katrina Pete	ersen, ULAN	C		
		Ioannis Dan	nilidis, KEME	4		
Keywords		Validation, evaluation, common information space demonstrator				
History	Version	Date	Author	Comment		
	V0.1	15/07/2015	T6 ECO	Table of content, first version		
	V0.2	23/11/2015	T6 ECO	Draft for review		
	V0.3	12/02/2016	T6 ECO	Draft for internal review		
	V0.4	15/02/2016	CS	Contribution from CS		
	V0.5	18/02/2016	UPB-BAPCO	Comments from the internal review		
	V0.6	25/02/2016	ULANC	First part of monitoring comments		
	V0.7	26/02/2016	ULANC	Second part of monitoring comments		
	V0.8	26/02/2016	CS	Contents from CS		
	V0.9	28/02/2016	T6 ECO	Draft for final internal review		



D5.3 Validation Strategy, Version 2 (ic) **Public deliverable**



V0.10	29/02/2016	T6 ECO	Review received by partners
V0.11	1/03/2016	T6ECO	Draft sent to the all the consortium for feedback
V1	03/03/2016	T6ECO	First delivery to the coordinator
V2	07/03/2016	T6ECO	Second delivery to the coordinator

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n°607832.





Authors



T6 Ecosystems Via Genova 30 00184 Rome Italy Ivan Cucco Email: i.cucco@t-6.it Simona De Rosa Email: s.derosa@t-6.it Antonella Passani Email: a.passani@t-.6.it



CloudSigma

Alexandre Georgiev Email: alexander.georgiev@cloudsigma.co m



University of Paderborn

Christina Schäfer Email: c.schaefer@cik.upb.de Torben Sauerland Email: sauerland@cik.upb.de Jens Pottebaum Email: pottebaum@cik.upb.de

Email: k.petersen@lancaster.ac.uk

Katrina Petersen



Centre for Mobilities Research Department of Sociology Lancaster University LA1 4YD UK



Center for Security Studies loannis Danilidis (KEMEA) loannis Danilidis i.daniilidis@kemea-research.gr P.Kanellopoulou 4 1101 77 Athens Greece



D5.3 Validation Strategy, Version 2 (ic) **Public deliverable**



Reviewers



University of Paderborn C.I.K Christina Schäfer Email: c.schaefer@cik.upb.de



14 Blandford Square, Newcastle upon Tyne, NE1 4HZ UK Paul Hirst Email: Paul.Hirst@bapco.org.uk





Executive summary

This deliverable provides an overview of the methodology that is used in WP5 to validate and evaluate SecInCoRe's outcomes and impact; the validation and evaluation process is described from a theoretical as well from a practical perspective. The deliverable clarifies how the SecInCoRe Validation and Evaluation Strategy (VES) combines elements of the E-OCVM validation framework with SEQUOIA (a counterfactual evaluation methodology) in a coherent and structured methodological framework that will drive the next steps of validation and evaluation. The E-OCVM aims at answering the validation question "Are we building the right system?"; the SEQUOIA methodology has been selected for evaluation and its aims is to assess the socio-economic impact of the project (the difference that SecInCoRe makes in comparison to current practices).

Taken together, these two robust and well-tested methodologies developed within European Union (EU) projects provide the bases for validation and evaluation activities structured around Demonstration Cases. Demonstration Cases are co-designed, organised and run with the involvement external stakeholders. Demonstration Cases follow a multiple-case embedded design in which evidence collected from different Demonstration Cases will be aggregated and compared across relevant dimensions, validation modules and impact areas.

The creation of Demonstration Cases is described within the document in its all major components. The template that will support the creation of Demonstration Cases is given in the Appendix 4: Demonstration Case Template. A timeline and a series of Demonstration Cases has already been identified, and the corresponding Demonstration Case Templates are reported in Chapter 6.

In order to run validation and evaluation activities, SMART indicators are derived from the High-Level Requirements (HLR) stored in the live JIRA database. This on-going effort has allowed linking the work done on WP4 about requirements with the work on validation and evaluation activities undertaken within WP5. Each HLR is related to CIS modules, SecInCoRe expected outcomes and SEQUOIA areas of impact thus providing a description on how will be possible to validate it or evaluate it. These definitions also take into account reflections and suggestions emerged from a first phase of validation with project partners and with the Advisory Board.

Finally, this deliverable provides a concrete description of the Common Information Space Demonstrator, both about concept and architecture. In addition, the document contains the manual for the usage of the main reference implementations of SecInCoRe.





Table of contents

1	Introduction			9
1.1	Purpose of t	his docu	ment	10
1.2	Validity of th	is docun	nent	10
1.3	Relation to c	other doc	uments	11
1.4	Contribution	of this d	ocument	11
1.5	Target audie	ence		11
1.6	Glossary			12
17	List of figure	۹		15
1.7	List of tables	2		16
ייי כ		, validati	on and evaluation strategy	
~		the finel	methodology	
2.1	Overview of		methodology	17
	2.1.1	Describir	ig valuation	18 20
	2.1.2	The relat	ion between evaluation and validation	20
	2.1.4	Usina mi	ultiple Demonstration Cases with embedded Use Cases for vali	dation
		and eval	uation purposes	23
	2.1.5	Validatio	n and evaluation expectations: the project perspective	29
	2.1.6	Indicator	s and metrics for evaluation and validation	30
	2.1.7	Assessin	g project progress through KPI	37
	2.1.8	Outline o	f the remaining Chapters	43
3	Summary of	projec	t stakeholders, their needs and involvemen	t 45
4	Common Inf	ormati	on Space Demonstrator V1	49
4.1	Concept			49
4.2	Reference Ir	nplemen	tations used in Demonstrator implementations	50
	4.2.1	Open Se	mantic Framework	50
		4.2.1.1	Planned future implementations	51
	4.2.2	Open Atr	ium	53
		4.2.2.1	SecInCoRe OpenAtrium platform concepts and features	54
	4.2.3	Semantic	: Media Wiki	56
	4.2.4	Knowled	ge Base	57
	4.2.5	External	Applications	57
	4.2.6	Federate	d Identity Management, AAA and SSO to the CIS	57
		4.2.6.1	NEC AAA Demonstrator	
		4.2.6.2	validation and outcomes from the NEC AAA Demonstrator	





		4.2.6.3	Ongoing research ar	nd implement	ation of the CIS AAA	service63
5	Manual for fi	rst ve	rsion of the Co	ommon Ir	oformation Sp	ace System 66
5.1	Integrated G	UI				
	5.1.1	Search	66			
	5.1.2	Semanti	c Media Wiki			67
	5.1.3	Databas	es			67
	5.1.4	External	applications			67
5.2	Open Atrium					67
6	Validation	and	evaluation	plan:	protocols,	instruments,
	Demonst	ration	Cases and tim	eline		
6.1	Demonstratio	on Case	e Protocol			69
6.2	Draft plan for	r the firs	t round of validation	on and eva	luation	71
6.3	Demonstratio	on Case	e: Lancashire Loca	al Resilienc	e Forum	73
6.4	Demonstratio	on Case	e: Dortmund exerc	ise		
6.5	Demonstratio	on Case	e: refugee crisis			
7	Conclusion.					
8	Literature in	dex				
9	Annexes					100
9.1	Appendix 1:	list of S	equoia indicators .			
9.2	Appendix 2:	JIRA re	quirements and po	ossible indi	cators	
9.3	Appendix 3:	first coll	ection of zero sce	narios		
9.4	Appendix 4:	Demon	stration Case Tem	plate		
9.5	Appendix 5:	SecInC	CoRe OpenAtrium	User Manu	ıal	
9.6	Appendix 6: the Deliverat	questio ble	nnaires and focus	group guid	delines mentione	d in the text of 155





1 Introduction

SecInCoRe envisages a Common Information Space (CIS) for cooperation and collaboration among all relevant stakeholders in all phases of crisis management based on an intense interoperability analysis focusing on first responder organisations and Police authorities. In line with this a methodology of validation and evaluation tailored on project's specification has been developed. This deliverable contains all references needed to understand the adopted strategy for validation and evaluation.

Indeed, this deliverable provides an overview of the strategy that is used to validate and evaluate the activities¹, outputs², outcomes³ and impacts⁴ of the SecInCoRe project. Starting from the proposed validation and evaluation strategies, the Deliverable derives the plans for the first round of validation and evaluation activities based on Demonstration Cases. In addition, it details the stakeholders, and the different elements that will be involved in the execution of the validation and evaluation strategy: the Pan European Inventory, the Common Information Space Demonstrator (CISD), the manual for the first version of the Common Information Space (CIS) and the documentation of Demonstration Cases.

Chapter 2 introduces the final SecInCoRe validation and evaluation strategy, noting that the strategy will be further adapted as the concepts develop, mature and proceed along the project life-cycle. Building upon work done in D5.2, Chapter 2 clarifies how elements derived from the two validation and evaluation models that have been selected as reference points for SecInCoRe (namely E-OCVM and SEQUOIA) are combined in the final SecInCoRe validation and evaluation strategy. It will then explain the key role that Demonstration Cases play in the validation and evaluation strategy. Finally, a preliminary and on-going list of indicators related to the two performance frameworks selected for the validation and evaluation strategy (the E-OCVM-based Key Performance Areas (KPA)/Key Performance Indicators (KPI) framework for the monitoring and validation of project objectives, and the multi-dimensional SEQUOIA framework for the evaluation of expected socio-economic impacts) will be provided. The Deliverable outlines the approach that will be used to relate individual indicators, KPAs and SEQUOIA-based impact areas to the Common Information Space and Common Emergency Information Space (CEIS) components identified in D4.2 as well as to project requirements listed in the live JIRA system.

Chapters 3 to 5 introduce and document the current state of analysis or development concerning three key elements involved in the preparation and execution of Demonstration Cases: stakeholders, the CIS Demonstrator and the Manual for the Common Information Space System.

Chapter 6 introduces the demonstration-based validation and evaluation activities envisaged for the next months. The tools and procedures that will be used to prepare, coordinate, monitor and run Demonstration Cases will be presented, together with a first description of the associated data collection and reporting instruments. The

¹ The specific programs or actions that the project undertakes.

² Tangible and intangible products and services that are the result of the project activities.

 ³ Specific changes in behaviors and affected by the delivery of the services and products created by the project.
 ⁴ Benefits to the communities and society as a whole as a result of the project outcomes. Impacts are the net

difference made by an activity after the outputs interact with society and the economy.





Chapter includes a number of Demonstration Case Templates for the preparatory phase of different Demonstration Cases that have been identified as possible candidates for runs of validation and evaluation in the following months. This validation is based on several rounds of iterative formative evaluation through questionnaires, focus groups, co-design workshops and Ethical and Privacy Impact Assessments.

Finally, Chapter 7 derives conclusions and briefly discusses the next steps.

1.1 *Purpose of this document*

This deliverable documents the strategy for the validation and evaluation of SecInCoRe's results (according to the DoW, T5.2).



Figure 1. SecInCoRe Overview (See D4.1 for a description)

1.2 Validity of this document

This deliverable reflects the current state of the work on validation and evaluation; it is based on literature review (documented with references) and experience gathered in previous European research projects. The literature reviewed includes European Commission (EC) reports and academic sources. The methodology has been developed following two well-established approaches: E-OCVM methodology⁵ and the SEQUOIA⁶ methodology for the impact assessment. Through the support of

⁵ Available at: https://www.eurocontrol.int/sites/default/files/publication/files/e-ocvm3-vol-1-022010.pdf

⁶ Available at: http://www.lse.ac.uk/media@lse/research/SEQUOIA/SEQUOIA_D2.2b_final.pdf





referenced documents, the strategy that will be used to validate and evaluate outputs, outcomes and impacts of the SecInCoRe project will be built. The planning of the SecInCoRe validation and evaluation activities which are part of this report is based on the state of the art of SecInCoRe development at the time of writing this report and may need to be updated in the next months in order to maintain the alignment with other WP developments.

1.3 Relation to other documents

This deliverable relates to the following foreground documents in the project:

- [1] Grant Agreement (no. 607832) and Annex 1. Description of Work
- [2] Consortium Agreement
- [3] D2.1 (WP-2) 'Overview of disaster events, crisis management models and stakeholders'
- [4] D3.1 (WP-3) 'Setup Inventory Framework and specification of Research Requirements'
- [5] D4.1 (WP-4) 'Requirements Report'
- [6] D4.2 (WP4)- Concept of Operation
- [7] D5.2 (WP5)- Validation

Outputs:

- [8] D.5.4 (WP-5) 'Validation Report and Final Evaluation Model of Communication System Concept' [in the form of T5.1/T5.2 input to T5.5
- [9] D.5.5 (WP-5) 'Evaluation and Validation report for SecInCoRe stakeholders' [in the form of T5.5 input to T6.3]
- [10] D6.3 (WP-6) 'Report and Evaluation on new Business Models' [in the form of T3.4/T3.3 input to T6.4]

1.4 Contribution of this document

The SecInCoRe 'Common Information Space' concept is based on a 'Pan-European inventory'. This deliverable contributes a description of the strategy that is adopted for the validation and evaluation of project achievements and expected impacts. In line with this, this deliverable is linked transversally to all the Work Packages.

1.5 Target audience

D5.3 is public and it has three main target audiences. First of all, the SecInCoRe project consortium. Since all project partners will be engaged in validation and evaluation activities, it important for them to be aware of the requirements, processes and objectives of the validation and evaluation strategy and to consider the indications provided in this deliverable when planning future development activities. Secondly, another target is the EC, which needs to understand how the SecInCoRe project assures the constant evaluation of its activities and pays attention to monitoring the continuing alignment of project activities with the DoW as well as with stakeholder requirements. Finally, external parties such as other projects which need to understand the methodological approach implemented and used by SecInCoRe.





1.6 Glossary

Abbreviation	Expression	Explanation
AAA	Authentication, Authorization and Accounting	Abbreviation is used as a description of a concept component and linked to security issues
AB	Advisory Board	Advisory Board defined within the consortium
CEIS	Cloud Emergency Information System	Emergency information system which can be accessed via internet.
CIS	Common Information Space	Service-oriented software framework facilitating complex systems
CISD	Common Information Space Demonstrator	Demonstrator to make visible the CIS to users
CISS	Common Information Space System	Concept to make visible the CIS to users
CLM	Concept Lifecycle Module	Lifecycle concept described in E-OCVM methodology
ConOps	Concept of Operation	Abbreviation is used as a description of a concept component
DCP	Demonstrator Case Protocol	Protocol for deriving demonstration cases
DF	Dortmund Fire	Fire brigades based in Dortmund
DoW	Description of Work	The description of SecInCoRe project as it has been approved by the EC.
E-OCVM	EuropeanOperationalControlValidationMethodology	Methodology provided by an European project for validation activities
EASO	European Asylum Support Office	European Union agency that plays a key role in the implementation of the Common European Asylum System
EC	European Commission	European body
ELSI	Ethical legal social issues	Ethical and social challenges and opportunities that arise in emergency situations, especially with a view to the use of ICT. Legal issues arising, particularly around data protection, liability, and responder safety
EU	European Union	Supranational Institution
EURODAC	European Dactyloscopie	European Database for fingerprints



D5.3 Validation Strategy, Version 2 (ic) **Public deliverable**



FR	First Responder	A first responder is an employee of an emergency service who is likely to be among the first people to arrive at and assist at the scene of an emergency, such as an accident, natural disaster, or terrorist attack. First responders typically include police officers, firefighters, paramedics, and emergency medical technicians.
FRONTEX	European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the	European Union Agency
FRS	European Onion First Responder Service	Emergency services
GP	General Practitioners	Figure of emergency service
GUI	Graphical User Interface	GUI is a type of interface that allows users to interact with electronic devices through graphical icons and visual indicators such as secondary notation, as opposed to text-based interfaces, typed command labels or text navigation.
HPC	Humanitarian Process Cycle	Process of emergency
IAIA	International Association for Impact Assessment	Association specialised in the study of Impact Assessment
IDM	Identity Management	Identity management (IdM) describes the management of individual principals, their authentication, authorization, and privileges within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime and repetitive tasks
IS	Information sharing	A computer Information System (IS) is a system composed of people and computers that processes or interprets information.
КВ	Knowledge Base	A knowledge base (KB) is a technology used to store complex structured and



D5.3 Validation Strategy, Version 2 (ic) **Public deliverable**



		unstructured information used by a
		computer system. In the SecInCoRe
		context the knowledge Base is the
		technical representation of the inventory
KPA	Key Performance Area	Areas in which need to be evaluated,
		measured the success of an organization
KPI	Key Performance	Indicators to measure the success of an
	Indicator	organization
LEA	Law enforcement agents	A law enforcement agency (LEA) is any
		agency which enforces the law.
LLRF	Lancashire Local	Multi-agency partnerships made up of
	Resilience Forum	representatives from local public services
		that aim to plan and prepare for localised
		incidents and catastrophic emergencies
MCA	Multi-criteria analysis	Quanti-qualitative method to derive
	,	analysis
MoU	Memorandum of	Main document
	Understanding	
NEC	Network enable	Abbreviation is used as a description of a
	communication	concept component and contains
		everything dealing with communication
		infrastructure and technical solutions in
		this field
NGO	Non-governmental	Organisation that is neither part of
	Organisation	a government nor a conventional for-profit
		business
OA	Open Atrium	Platform for enhancing sharing and
		collaboration
OSF	Open Semantic	Integrated software stack using semantic
	Framework	technologies for knowledge management
PD	Past disaster	Gathering of past disaster information
PD-DB	Past Disaster Database	Database containing information about
		Past Disaster events
PPDR	Public Protection and	This expression compromises the domain
	Disaster Relief	of all
		first responder and police authorities and
		is used in literature
RD	Resilience Direct	Secure web-based platform for the
		resilience community to share information
		among stakeholders
SEQUOIA	Socio-Economic Impact	Methodology for impact assessment
	Assessment for Research	provided by the Sequoia European





	Projects	project
SIS	Schengen Information System	Large-scale information system that supports external border control and law enforcement cooperation in the Schengen States
SMART	Specific, Measurable, Achievable, Relevant and Time-bound	Defined categories to measure items.
SME	Small / Medium Enterprises	Businesses sized according to staff head- count and financial turnover (EU definition)
SMW	Semantic Media Wiki	Open-source extension of Media Wiki that lets store and query data
UNHCR	Office of the United Nations High Commissioner for Refugees	UN Agency for refugees
VES	Validation and evaluation strategy	Abbreviation to indicate the strategy for both validation and evaluation
VIS	Visa Information System	System that allows Schengen States to exchange visa data
WP	Work Package	Work packages are defined steps in the DoW (see above) in order to achieve the project objectives

1.7 List of figures

Figure 1. SecInCoRe Overview (See D4.1 for a description)1	0
Figure 2. CIS Specification Modules (from D4.2)2	0
igure 3. The Impact Value Chain, demonstration cases and validation / evaluatio	n
strategy2	3
igure 4. Relation between Demonstration Cases and Demonstrator Implementation	S
	5
igure 5. The multiple-case embedded design2	8
Figure 6. Reference Implementations5	0
igure 7 SecInCoRe OSF GUI5	1
igure 8 Search results5	2
Figure 9 Hierarchy view	3
igure 10 CIS Concept [D4.2]5	4
igure 11 OpenAtrium Spaces and Sections conceptual model	5
igure 12 Open Atrium Members, Groups and Teams Access Control principles5	6
igure 13. WIFI access point configuration5	8
igure 14. RADIUS Server network access5	9
-igure 15. RADIUS Server settings5	9
-igure 15. RADIUS Server settings5	9





Figure 16. RADIUS Server Authentication different devices	60
Figure 17. RADIUS Server audit log showing multiple access attempts	61
Figure 18. Eduroam: Ubiquitous Network Access	62
Figure 19. Map of countries participating in Eduroam	63
Figure 20. Trust between federated domain controllers	65
Figure 21. Search function	66
Figure 22. Demonstration Cases covering different scenarios	72
Figure 23. Screenshot of SecInCoRe OpenAtrium home page	145
Figure 24. Screenshot of SecInCoRe OpenAtrium login page	146
Figure 25. Screenshot showing SecInCoRe OpenAtrium navigation	146
Figure 26. Screenshot showing SecInCoRe OpenAtrium sitemap	147
Figure 27. Screenshot showing how to go back to the SecInCoRe OpenAtrium s	itemap
	147
Figure 28. Screenshot showing how to join a SecInCoRe OpenAtrium Space	148
Figure 29. Screenshot showing SecInCoRe OpenAtrium Section navigation	149
Figure 30. Screenshot showing how to add content to SecInCoRe OpenAtrium	149
Figure 31. Screenshot showing the add Document screen	150
Figure 32. Screenshot showing the various options on the 'add document' screen	n151
Figure 33. Screenshot showing the 'Text' feature of the 'paragraph' module	within
OpenAtrium. Note the Layout option	152
Figure 34. Screenshot showing how the 'paragraph' module formats the 'Text	ť type,
according to the 3 column layout	152

1.8 List of tables

Table 1. Requirements for validation and evaluation activities	22
Table 2. Overview of Economic impact	31
Table 3. Overview of Social Impact	31
Table 4. Expected outcomes, objectives and SEQUOIA impact areas	34
Table 5. JIRA requirement and possible indicators. Example 1	35
Table 6. JIRA requirement and possible indicators. Example 2	36
Table 7. JIRA requirement and possible indicators. Example 3	37
Table 8. Measurement to validate the achievement of the project	43
Table 9. Direct and indirect users involved in the validation / evaluation activities	47
Table 10. Direct users main categories involved in the preparedness phase	48
Table 11. Possible implementation	64





2 SecInCoRe validation and evaluation strategy

2.1 Overview of the final methodology

The SecInCoRe Validation and Evaluation Strategy (VES) combines elements of the E-OCVM validation framework with SEQUOIA, an evaluation-oriented methodology (D5.2, pp. 21). The SEQUOIA methodology⁷ (Passani et al., 2014) has been selected for the evaluation phase, since it provides a flexible multi-criteria approach to the evaluation of quantifiable and non-quantifiable socio-economic impacts along the impact value chain through counter-factual assessments methods (D5.2, pp.22).

In line with this, SecInCoRe VES is based on the triangulation of evidence concerning project impacts and outcomes concurrently generated by two robust and well-tested methodologies developed within European Union (EU) projects. The aim of this Deliverable is to combine the two approaches into a coherent, valid and consistent validation and evaluation strategy. The relatively advanced stage of maturity already attained by most SecInCoRe concepts offers the opportunity (and at the same time presents us with the challenge) to tailor the application of both methodologies to the requirements of SecInCoRe's validation and evaluation objectives. First attempts in this direction have however revealed a considerable degree of overlap between the two methodologies in terms of their selection of indicators and definition of impact areas, thus requiring a further clarification of the respective scope of application within the overall evaluation and validation strategy.

The nature of SecInCoRe as an emergent socio-technical system calls for an emphasis on user-based validation and evaluation activities, an approach that is fully compatible with both E-OCVM and SEQUOIA. Since the expected outcomes and impacts of SecInCoRe are not separable from the end-users' own interpretation and creative adaptation of the possibilities implied in projects outputs, the boundary between validation and evaluation activities (the former being address through an adaptation of E-OCVM, the latter through an adaptation of SEQUOIA) is in this case bound to change as the SecInCoRe concept moves further along its lifecycle. As will be further discussed in subsequent sections, elements of both methodologies merge in the design, execution and analysis of Demonstration Cases. In order to ensure the validity of conclusions derived from Demonstration Cases, it is therefore particularly important to clarify at this stage the respective contributions and objectives of the two approaches and combine them under a unified validation and evaluation design.

Consistently with the view expressed in the E-OCVM manual (EUROCONTROL, 2010, pp.23), we accept that "the overall purpose of a validation strategy is to ensure that a validation programme or project fulfils its functions. It does this by ensuring that there is a common understanding of the set of shared principles and practices, which are to be used to structure and organise activities throughout concept development and validation to progress the maturity of the concept through to implementation [...]. These must be shared or applied by all validation activities covered by the validation strategy to produce the coherent and consistent results needed if an adequate

⁷ Passani, A., Monacciani, F., Van Der Graaf, S., Spagnoli, F., Bellini, F., Debicki, M., & Dini, P. (2014). SEQUOIA: A methodology for the socio-economic impact assessment of Software-as-a-Service and Internet of Services research projects. *Research Evaluation*, *23*(2), 133-149.





validation of the target concept is to be achieved". One of the main aims of this Validation and Evaluation Strategy document is therefore to establish and maintain a shared understanding of how principles, practices and approaches derived from E-OCVM and SEQUOIA will interact and will be adapted to the specific needs of SecInCoRe.

Finally, and again consistently with the E-OCVM approach, the validation and evaluation strategy document will be maintained and updated throughout the project as a living document. As more evidence is gathered and concepts reach higher degrees of stability and maturation, the validation and evaluation strategy will be revisited and updated. This reflects the iterative and incremental nature of both the E-OCVM and SEQUOIA methodologies. A constantly updated version of the Validation and Evaluation Strategy (VES) will be made available to all project partners and stored in Open Atrium (OA) in order to be always visible to all and updated.

2.1.1 Describing validation

According to the E-OCVM manual (EUROCONTROL, 2010, p.58), whereas verification deals with answering the question "Are we building the system right?", validation is defined as the range of activities that answer the question "Are we building the right system?" In other words, validation is concerned with assessing the concept's fitness for purpose.

The strategy established by T6 ECO to validate the main outcomes of the project is modelled upon key elements of the E-OCVM framework (the Structured Planning Framework and the Case-Based Approach) and entails two concurrent methods:

- a regular and ongoing internal validation process with project partners and Advisory Board members through consultations and seminars;
- external validation with selected end-users through Demonstration Cases in which specific parts of the SecInCoRe concept are exposed to end-users for shorter or longer periods of time. In collaboration with these users, the SecInCoRe team will formulate Scenarios and Use Cases that identify a range of challenges related to realistic work practices of multi-agency and cross border collaboration'. The SecInCoRe team will then prepare Demonstrator Implementations that will allow users to try and address the scenario-related challenges using the opportunities offered by SecInCoRe. Quantitative and qualitative data will be collected from end-users before, during and after each Demonstration Case to assess SecInCoRe's fitness for purpose.

Although this Deliverable presents the results of previous rounds of internal validation, it specifically focuses on the definition of a general strategy for designing, organizing, running and analyzing Demonstration Cases. With relation to the EOCVM Structured Planning Framework (SPF), identified in the DoW as "*the most relevant perspective for validation in SecInCoRe*", the work reported in this Deliverable covers the following step:

• Step 1: Set Validation Strategy. This step identifies stakeholders, issues, aims, objectives, indicators, cost-benefit mechanisms and expected outputs of the validation process.





An updated identification of *stakeholders* is reported in Chapter 3. A first detailed identification of *issues, objectives and expected outputs* for validation is generated using a "top-down approach" starting from the modules of the CIS Specification as detailed in the *CIS Concept Documentation presented* in D4.2 (Figure 2). The validation objectives and a first list of quantitative and qualitative indicators for each module are further defined on the basis of the list of requirements reported in the JIRA system (D4.2, pp.34) (hereafter JIRA requirements), that are being reviewed from a validation perspective in order to derive associated SMART indicators (D4.2, pp. 21 and pp. 38) and at the same time are being aligned to the updated definition of CIS Specification modules. Validation objectives derived from the CIS Specification modules and from JIRA requirements are compared to (and where necessary supplemented by) the list of validation objectives generated through previous consultations with project partners and Advisory Board members.

In terms of *indicators and cost-benefit indicators*, validation will be based primarily on data and evidence collected during Demonstration Cases. As indicated in the E-OCVM approach, the SecInCoRe concept will be assessed with reference to an updated *performance framework* that, although building upon the KPAs originally identified in the DoW (Operational procedures, Efficiency, Capacity, Economic Considerations), more accurately reflects the current definition of SecInCoRe's high-level objectives.

The allocation of issues, objectives and expected outputs to CIS Specification Modules (Figure 2) and the necessity to further break down JIRA requirements in sub-tasks associated to SMART indicators for validation purposes will be discussed with project partners. A first example of the work being undertaken is provided in Section 2.1.7.

In this Deliverable, we also start to collect and organise evidence, plans and guidelines for the following step of the SPF:

• Step 2: Determine the Activity Needs. This step plans a validation activity defined in the validation work plan and captures all the detailed exercise needs.

With regard to Step 2, Chapter 6 presents the tools developed to date to ensure that validation activities are consistent with the overall validation and evaluation strategy, and details the status of preparatory activities for a first validation activity based on Demonstration Cases.







Figure 2. CIS Specification Modules (from D4.2)

2.1.2 Describing evaluation

According to the definition provided by the International Association for Impact Assessment (IAIA), impact is "the difference between what would happen with the action and what would happen without it^{8} ". The evaluation strategy proposed for SecInCoRe (D5.2, pp. 25) intends to estimate the socio-economic impact of the project responding to questions such as:

- What is the difference SecInCoRe project makes?
- Why is SecInCoRe relevant and for whom?
- How much difference does SecInCoRe make?

Given that the actual impact of the project is only to a very limited extent directly observable in the course of the project lifecycle, and at the same time only to a partial extent quantifiable in terms of purely economic indicators, any attempt at answering these questions requires a focus on *expected impacts assessed on multiple dimensions*. The SEQUOIA methodology (Passani et al., 2014) assesses the impact of a project through the adoption of counterfactual methods based on the comparison of so-called *zero scenarios* (the current practice) with a future scenario in which

⁸ Available at http://www.iaia.org/uploads/pdf/What_is_IA_web.pdf





SecInCoRe has been adopted, and estimates the expected project impacts by combining multiple quantifiable and non-quantifiable dimensions.

The use of the term scenario in both the Demonstration Case approach and in the SEQUOIA counterfactual methodology may generate some confusion. It is important to keep in mind that, in the context of the Demonstration Case approach, the term scenario refers to a narrative co-generated with end-users aimed at identifying a hypothetical operational situation that provides the background for the challenges endusers involved in a Demonstration Case have to face. In the context of the counterfactual SEQUOIA approach, zero-scenario refers instead to the status quo: how would end-users respond to a challenge in the current situation? The zeroscenario is used as a baseline against which to calculate or assess the improvement that SecInCoRe is expected to make. In order to avoid confusion, in the remainder of the Deliverable we will use the term *Demonstration Scenario* to refer to the scenarios collaboratively developed with end-users for validation and evaluation activities; Zero Scenarios to refer to the baseline scenario used in SEQUOIA evaluation (based on current practices); and Evaluation Scenario to refer to a future situation in which the SecInCoRe concept has been fully developed and integrated into crisis management practices (the situation whose impact SEQUOIA evaluation activities intend to asses).

The main steps envisaged in the SEQUOIA process are:

- mapping the area of the impact;
- describing the current situation (without the adoption of SecInCoRe);
- describing the counterfactual scenario with the introduction of SecInCoRe;
- exercising final assessment analysis though a multi-criteria and multidimensional description of SecInCoRe impacts.

The first step for the application of the methodology is the identification of relevant stakeholders. From a methodological perspective, the term *stakeholder* refers to the group of people or organisations directly impacted by the introduction of the innovation. Once the main stakeholders are identified, the main areas of impact are then defined. Then, the methodology envisages the description of the zero scenario, in other words, of the situation prior to SecInCoRe's implementation.

When the project has produced relevant outputs, it is possible to describe how the situation changes with the implementation of the SecInCoRe concept. In this phase, qualitative evaluation is augmented by indicators and variables that help in quantifying benefits and changes where this is meaningful; a description of the indicators derived from the SEQUOIA methodology for the SecInCoRe concept is provided in Appendix 1.

Finally, though a multi-criteria analysis, qualitative and quantitative data are discussed and analysed to estimate the impact that SecInCoRe has produced. Results from the evaluation activity will contribute to the learning of partners.

The validation and evaluation strategy will fulfil the requirements set in the DoW for validation and evaluation activities, as reported in Table 1. Progress towards the listed objectives will be assessed at each validation and evaluation activity.





Objective	Measurement
Performance of at least one validation run	Number of validation activities
One finalised validation process minimum of the integration framework	Indicators described by the verification
Iterative validation process (minimum two cycles) concerning the development of the inventory	Numbers of cycle of validation process on inventory development
Performance of a validation activity including the application of the pilot cloud service	Number of activities utilising pilot cloud
More than 10 different external test-users accessing the inventory as well as the common information space	Number of test-users accessing the inventory and the CIS
At least one Advisory Board meeting targeting validation aspects only	Number of AB meting on validation
All Advisory Board workshops with more than 10 different end- users (more than five from First Responder organisations, more than four from Police authorities) from at least more than two countries	Number of different stakeholders' roles involved during AB workshop
Evaluation with more than 10 different end-users and one workshops dedicated especially for this topic	Number of evaluation activities organised and number of people involve. Number of workshop dedicated to evaluation

2.1.3 The relation between evaluation and validation

While validation activities monitor the development of project outputs, their alignment to project objectives and to stakeholders' requirements and their capacity to generate the expected outcomes (i.e., their capacity to enable changes in stakeholders' practices and routines in the intended direction), evaluation activities analyse and assess the expected socio-economic impacts of SecInCoRe outputs on stakeholders and on society as a whole. As explained in D5.2, in terms of the impact value chain





(Ebrahim and Rangan, 2010) (Figure 3), it can be said that the validation activity covers the assessment of expected outcomes; the evaluation activity is instead mainly concerned with impacts.

In both cases, the assessment of outcomes and impacts requires an analysis of the interaction between project outputs (for example, project concepts as captured in Reference Implementations) and end-users' practices (stakeholders). This interaction takes place in Demonstration Cases (through the creation of Demonstrator Implementations and the involvement of end-users), and both validation and evaluation are based on the analysis of end-users' activities in the Demonstration Cases they have helped co-design. As explained in the following section, the emphasis of validation and evaluation is however on different aspects of the Demonstration Cases and ultimately responds to different objectives.



Figure 3. The Impact Value Chain, demonstration cases and validation / evaluation strategy

2.1.4 Using multiple Demonstration Cases with embedded Use Cases for validation and evaluation purposes

Within the E-OCVM framework, evidence is gathered by demonstrating 'fitness for purpose' whereby stakeholders can judge if the concept is capable of being fit for their own purposes. Practically, this requires grouping results within a 'Case Based Approach' whereby "a 'case' is a structure for grouping evidence about critical validation aspects such as business, safety, human factors, environment, and standardisation" into a clear structure in order to describe the potential of the concept under evaluation (EUROCONTROL, 2010. pp. 50). As the concept proceeds along the Concept Lifecycle Module (CLM), the focus of the Case-Based Approach changes from providing evidence that the concept is fit for purpose by means of detailed assessments, to supporting stakeholders by providing the evidence they require to make investment and implementation decisions. At the same time, the Case-Based





Approach provides guidance on the design of suitable activities to obtain the evidence required for the validation strategy.

The decision to base SecInCoRe's validation and evaluation strategy on Demonstration Cases is consistent with this view. The main difference with the standard E-OCVM approach is that, instead of organising cases around specific aspects such as business, safety, standardisation and so on, Demonstration Cases will be either defined from a project perspective (with regard to one or more specific aspects of the CIS Concept), or structured around holistic scenarios (i.e. hypothetical but realistic situations collaboratively defined with end-users). In the latter case, Demonstration Cases are related to different phases of crisis management which simultaneously involve all the different elements considered important for the validation and evaluation of SecInCoRe (the CIS Specification Modules in Figure 2).

The decision to adopt a strategy based on holistic Demonstration Cases potentially exposes the project to some of the *pitfalls of validation* that the E-OCVM methodology warns of (EUROCONTROL, 2010. pp.10). The following problems appear to be potentially relevant to the case of SecInCoRe:

- validation being driven by the capabilities of methods, tools and platforms instead of the converse. Validation activities should be designed to achieve the validation objectives, so planning must ensure that the requirements for the correct methods and tools can be established in time;
- 2. particular risks emerging when problems fall between the responsibilities of the different actors involved in the validation process;
- 3. failure to use past project results leading to the unnecessary repetition of work;
- 4. failure to adequately document an activities and particularly the assumptions associated with it. This can severely limit the use of the data;
- 5. failure to anticipate the needs for integration of data from different activities. If the integration of data from different activities is not considered during the identification of their assumptions and metrics (so that these can be shared where necessary), there is little chance that the results can be combined later.

In relation to points 1 and 2, the organisation of a Demonstration Case requires the cooperation of teams involved with different aspects including: the development of Demonstrator Implementations, collaboration with stakeholders to co-design Scenarios and Use Cases, the monitoring of ELSI implications, the alignment of the case with the general validation and evaluation strategy, the collection and analysis of data before, during and after the Demonstration Case. To ensure that the validation and evaluation activity achieves its aims and contributes to the overall strategy, an appropriate protocol is required to coordinate the activities of different teams and for checking the alignment of Demonstration Cases with SecInCoRe's validation and evaluation objectives.

Points 3 to 5 are particularly relevant given that, due to the need to involve and motivate stakeholders, the organisation of a Demonstration Case can only be planned to a limited extent. The emergent nature of Demonstration Cases is a crucial value to SecInCoRe's validation and evaluation strategy also because the outcomes and impacts of SecInCoRe are ultimately related to the capacity of the concept to respond to the evolving needs and requirements of end users. Procedures for the collection of





data from Demonstration Cases will consequently have to be flexible and modular, adapting to the emerging needs of Demonstration Case, while at the same time being guided by a design that allows for the comparison of data across Demonstration Cases and for their analysis along relevant dimensions including stakeholders' characteristics, crisis phases, national and international contexts, sectors of intervention.

To these aims, the overall design for the validation and evaluation strategy follows a *multiple-case embedded design* (Yin, 2003), whereby the overall validation and evaluation strategy is based on the aggregation of evidence collected from Use Cases embedded in multiple Demonstration Cases. The general design of a single Demonstration Case (the *embedded* nature of the design) and its relation to project elements is represented in Figure 4 below.



Figure 4. Relation between Demonstration Cases and Demonstrator Implementations

At the most abstract level, a Demonstration Case is the container in which different stakeholders, elements and components required for validation and evaluation are embedded including:

- Demonstrator Implementations, created by adapting and pre-populating Reference Implementations according to the needs and objectives of the Demonstration Case
- Different categories of stakeholders that participate in all phases of the Demonstration Case (including setting the objectives of the Demonstration Case, the definition of a realistic and relevant Demonstration Scenario, the ongoing identification and co-generation of embedded Use Cases, interactions with Demonstration Implementations, the validation of the fitness for purpose of SecInCoRe concept on the basis of the results and activities of the Demonstration Case)





- A Demonstrator Scenario, i.e. a narrative about a potential crisis situation that is co-designed by project team members and stakeholders
- One or more *embedded Use Cases* that detail the interactions between stakeholders and Demonstrator Implementations according to a set of objectives, challenges, opportunities jointly and dynamically defined by stakeholders and project team members. When involved in Use Cases, stakeholders can be characterised according to their role as *direct or indirect users* of SecInCoRe
- Data which can be retrieved, processed, modified and communicated by stakeholders in the demonstration case. Realistic data is a prerequisite to facilitate actual experiences with the SecInCoRe concept.

The coordination and structuring of the different phases involved in the planning, preparation, execution and analysis of a Demonstration Case will be based on a Demonstrator Case Protocol (DCP). The Protocol will provide guidelines and, when appropriate, pre-defined templates to ensure that the following activities are performed in a consistent way so as to ensure comparability across different Demonstration Cases:

- Preparatory activities including the identification of general aims, validation and evaluation objectives of a Demonstration Case, its preliminary technical and implementation requirements, overall ELSI implications (see the Phase 1 Template in Chapter 6)
- Definition of a Demonstration Scenario and of one or more initial Use Cases through the involvement of stakeholders
- Definition of more specific validation and evaluation objectives, identification of ELSI issues and of specific requirements for the development of Demonstration Implementations based on the Demonstration Scenario and Use Cases collaboratively designed with stakeholders
- Adaptation of instruments for qualitative and quantitative data collection before, during and after the Demonstration Case
- Guidelines for preparing a Demonstration Case database and a Demonstration Case report

Beyond making sure that data collection is consistent with the overall validation and evaluation strategy, the use of a Demonstration Case Protocol and of the associated templates will ensure proper communication and coordination among different teams involved in the preparation, execution and analysis of a Demonstration Case.

Data collected at different levels, different stages of different units of analysis in a Demonstration Case relates to both validation and evaluation activities because:

- Information collected at the Demonstration Case level relates to both validation and evaluation activities since it includes:
 - Information on the status of Demonstrator Implementations collected at the beginning of the Demonstration Case, that will be used for the validation of project objectives with reference to the KPIs and KPAs set in the DoW (for example, number of data sources covered by the project)
 - Information on stakeholders (including the nature and characteristics of the organisations, their crisis management practices, their current





management models), that is needed to identify relevant dimensions for cross-case comparisons

- Information collected at the Scenario Level is related to evaluation, since once a Demonstration Scenario is agreed upon with stakeholders it will be possible to collect information on their current practices and response (the Zero Scenario required for evaluation according to SEQUOIA)
- Information collected at the Use-Case level during and after the Demonstration Case relates to both validation and evaluation activities, since it permits observation, measurement and collection of information on the interactions between end-users and Demonstrator Implementations

Each Demonstration Case can thus be equated to an experiment in which expectations (hypotheses) about the outcomes of SecInCoRe in the specific context represented by the Demonstration Scenario and within the boundary established by the involved stakeholders are tested against the actual outcomes of the Demonstration Case. These experiments 'validate' the current status of fit between the potential of SecInCoRe technologies and their prospective use environment (which is made-up from organisational practices, policies, legacy technologies and much more) as well as the usefulness of the technology. Demonstration Cases are also formative evaluation experiments in the sense that they provide insight into how further design efforts in relation to dimensions of the environment (e.g. organisational or policy-innovation) or innovation in relation to SecInCoRe technologies could enhance this fit.

The *multiple-case* aspect of the overall validation and evaluation design aims at increasing the external validity of results through logical generalisation based on a cycle of hypothesis generation – experiment - hypothesis generation. The feedback provided from the validation-oriented analysis of Demonstration Cases will be used to improve, where needed, the design of Reference and Demonstrator Implementations and to refine the concept. Meanwhile the input generated from the evaluation of socio-economic impacts will eventually assist with the creation of business cases and business models that can improve the adoption of SecInCoRe and its sustainability.



Figure 5. The multiple-case embedded design

The *multiple-case* aspect of the overall design is represented in Figure 5. The inclusion within the Demonstration Case Protocol of data collection tools and instruments addressing different stages and different units of analysis within Demonstration Case will permit the aggregation and comparison of validation and evaluation results at different level of analysis such as:

- Comparison across Demonstration Scenarios (e.g., validation of fitness-forpurpose for different crisis phases or fields)
- Comparison across stakeholders (for example according to their organisational characteristics, structure of command chains, current crisis management models)
- Comparison of validation results aggregated according to CIS Modules
- Comparisons of evaluation results on socio-economic impact in different Demonstration Scenarios





Work on the definition of the Demonstration Case Protocol is on-going. The current status and the Template from Phase 1 are presented in Chapter 6.

2.1.5 Validation and evaluation expectations: the project perspective

To identify a preliminary list of validation and evaluation objectives and strategies, a round of consultations was held with project partners and Advisory Board members. Detailed results from the consultations are available in the OpenAtrium platform, while the main elements emerged from consultations and relevant for the design of the Validation and Evaluation Strategy are here summarised.

Collaboration practices and ELSI

- Partners agree with the methods utilised to formulate problems, identify solutions and users' needs, such as co-design workshop and participant observation.
- Major issues raised by different partners and stakeholders concern data quality and procedures for the maintaining of the inventory; trust in the system, information security, negotiation of meaning and relevance, role improvisation, new responsibilities and liabilities
- Partners suggest that EU bodies should promote maintenance of the system in case it is adopted for the purpose of a Pan-European multi-agency common information space
- Partners raised the diversity of organisational practices, crisis management models, perspectives and languages as key issues

Pan European Inventory

- Project partners were asked to envisage who would be most interested in the system. Amongst the emerging categories were emergency responders working in planning phases and training.
- When asked about the most innovative aspect of the inventory, project partners share the belief that an interdisciplinary European disaster base contains several important aspects, above all in relation to the CIS and to the secure exchange of information between agencies.
- Partners were asked to assess the 'value added'⁹ offered by the Inventory. A clear majority of the partners assessed the value as significant but there were also some suggestions for further improvement. These included the addition of 'Lessons learned' boxes that would contain information on what was wrong, what was right, what worked and what did not.

Validation of ConOps with AB¹⁰

• Participants were very interested in the role that SecInCoRe could have in preparedness and training activities. In the case of preparedness activities, SecInCoRe is most relevant to maintain interoperability, as concept will improve

⁹ The extent to which information is beneficial, provides advantages from its use

¹⁰ A detailed report on activities involving the Advisory Board is available in Deliverable 1.6 "Second Report on Advisory Board Activities".





sharing information and materials among different countries and different organisations.

- AB members have identified several benefits that the project could provide: among them is the possibility to access a system that connects multiorganisational and multi-national databases. The result will be an increase and improvement in the collaboration among emergency services of all European countries.
- A particular issue stressed by the AB concerned trust issues: trust in technologies, information, people involved all needs to be supported as a matter of social practices.
- Participants discussed the possibility of including data provided by spontaneous volunteer organisations in SecInCoRe.

The indications here reported have been compared and integrated to other perspectives of validation and evaluation objectives including the CIS Modules (top-down) perspectives and the identification of specific validation and evaluation objectives based on analysis of ELSI.

2.1.6 Indicators and metrics for evaluation and validation

For evaluation purposes, quantitative and qualitative indicators for success for SecInCoRe needs to be specified and related to SEQUOIA impact areas. For validation purposes, indicators needs to be defined in relation to SecInCoRe main objectives as specified in the DOW, operationalised in D4.2 and documented in the list of requirements maintained in the JIRA database. Although the definition of specific indicators in on-going and related to the specification of Demonstration Cases, in this section we provide indications on the work that is being undertaken first in relation to evaluation indicators, then in relation to validation indicators.

From an evaluation perspective, we follow the SEQUOIA methodology and divide impact at the more general level into *economic impact* and *social impact*. However, "each of these two are further subdivided into more specific impacts" (Passani et al., 2012. pp.8¹¹). The next step is to "provide an accurate description of each impact of the indicators/proxies chosen for their assessment, and of the metrics used for their qualitative/quantitative judgment/measurement".

Following indications provided by the Sequoia methodology (Passani et al., 2012), impact areas are divided into the following subsections:

Economic impact:

- financial impact
- technological impact
- environmental impact

Social impact:

¹¹ Passani, Antonella and Monacciani, Fabiana and Van der Graaf, Shenja and Spagnoli, Francesca and Bellini, Francesco and Debicki, Marie and Dini, Paolo (2012) Sequoia: a methodology for the socio-economic impact assessment of software-as-a-service and internet of services research projects. Research evaluation . ISSN 0958-2029 (Submitted)





- impact on employment and working routine
- knowledge production and sharing
- social capital

As shown in Table 2 and in Table 3 impacts are divided in further subcategories.

Economic Impact			
Financial Impact	Technological Impact	Environmental Impact	
Investment cost (total project project)	Operational efficiency	Saving on energy consumption	
Maintenance cost	Accessibility	Saving on travel costs	
Labour cost for implementation	Effectiveness	Saving on storage-related costs	
	Satisfaction	Technological waste production	
	Security		

Table 2. Overview of Economic impact

Social Impact			
Impact on employment and working routines	Knowledge production and sharing	Social Capital	
Increment in skilled personnel employment	Scientific impact	Social capital increment for project participants	
Impact on general employment	Knowledge sharing	Social capital increment for users and beneficiaries	
Improvement in working routines	Support of ICT usage for all and democratic participation		

Table 3. Overview of Social Impact

We have begun to define such indicators informed by our initial formulation of expected outcomes and objectives (see Table 4). Considering the project aims to produce a CIS concept, not a single product, these are at varying levels of abstraction or concrete-ness and under development. They current status is captured in the Table 4. Further details can be found in the specification of major outcomes in D4.2 and in Appendix 1 where we list candidates for quantitative and qualitative evaluation indicators that are under consideration.





Added Value enabled by SecInCoRe	Expected outcomes	SEQUOIA impact areas
New Partnerships	Increase in the number and quality of new relations	Social capital
Better Common Understanding	Evidence of more coordinated actions	Impact on employment and working routines; technological impact
More Informed	Users can find 'new', 'useful and 'relevant', domain specific information more easily	Knowledge production and sharing
Better Collaboration	Enhanced capacity to liaise with relevant actors; better support for collaboration and interoperability	Impact on employment and working routines; social capital; technological impact
Better Pan-European Collaboration	Enhanced capacity to cooperate across EU borders, integration into EU mechanisms and infrastructures	Knowledge production and sharing, social capital; technological impact
Make Unknowns Visible	To richer and more dynamic awareness of available resources; increased knowledge about best practices, wider appreciation of unknowns	Knowledge production and sharing
Trusted Relationships	Taxonomy fits users' needs; ELSI guidelines are live/lived/living; CIS is flexible, brings together multiple perspectives, and enables the configuring of awareness.	Social capital; knowledge production and sharing;
Economical	It offers more/higher quality compared to current practices without increasing cost	Financial impact; environmental impact
Security	Users are more willing to share lessons learnt thanks to the confidentiality, discretion and/or anonymisation support provided by SecInCoRe	Technological impact; Knowledge production and sharing





Cloud	SecInCoRe meets ELSI requirements as well as users' expectations to use the Cloud in crisis management preparation as a secure and reliable platform for information management, planning and collaboration with users from various locations and organisations	Technological impact; Knowledge production and sharing
Scalability	Routines still work; increase in the numbers of systems and partners connected	Financial impact; technological impact
Efficiency	Enhanced emergency responders' capabilities to address crises and collaborate	Financial impact; technological impact
Enhanced Quality of Information/Interactions	Effective support for the generation and use of high- quality information; greater support to intra- and inter-agency emergency response collaboration and interoperability	Technological impact; Impact on employment and working routines
ELSI sensitive	Template for MOU exist; ELSI taxonomy integrated into system interactions; capacity to strengthen the security and safety of European citizens as well as their privacy and civil liberties, supportive of wider European values of equality and solidarity	Knowledge production and sharing
Standardisability	Meta-data protocols processes are comparable; processes can be put into a familiar frame of work; facilitate the adoption of standardised processes (e.g., training preparations)	Technological impact; Impact on employment and working routines
Level playing field for industries	Providers of data sets and information systems are able to offer services to organisations European wide; users are able to compare services amongst	Knowledge production and sharing





	providers across Europe	
Living and Inclusive	Users find it possible and easy to contribute to and modify SecInCoRe	Technological impact; impact on employment and working routines
Flexibility	Users are able to develop different shapes of CIS according to their needs	Technological impact; Impact on employment and working routines

Table 4. Expected outcomes, objectives and SEQUOIA impact areas

From a validation perspective, an updated identification of validation objectives reflects:

- the main project objectives (see DOW) and the CIS concept modules specified identified in D4.2;
- validation requirements identified through internal consultations;
- other socio-technical requirements as they emerge from work on ELSI in WP2

Qualitative and quantitative SMART indicators for each validation module are derived from the High-Level Requirements (HLR) documented in the JIRA system (hereafter JIRA requirements). HLR are part of the CIS concept, requiring adoption efforts per application of the concept either for reference implementations, demonstration cases or productive use. Linking the definition of SMART validation indicators to high-level JIRA requirements is consistent with the strategy defined in D4.2, Section 2.1.1 and offers several advantages:

- The list of JIRA requirements is periodically updated;
- Given the emergent and co-designed nature of Demonstration Cases, the definition of SMART validation indicators and their use in Demonstration Cases requires a constant dialogue between different project partners. Coordination is particularly important to ensure that the selected indicators, while contributing to the overall VES strategy based on comparison across Demonstration Cases, can also be Specific, Measurable, Achievable, Relevant and Time-Bound in the context of a specific Demonstration Case and given the status of Demonstration Implementations. The use of JIRA facilitates this dialogue, since specific procedures for JIRA-related activities are already in place as documented in D4.2, Section 4.1.2;
- High-level requirements in JIRA may require a further articulation in sub-tasks for validation and evaluation purposes, and this level of detail can be incrementally improved on the basis of previous validation and evaluation activities;
- By documenting the list of qualitative and quantitative indicators associated to each high-level requirement in the JIRA database, it will be possible for implementing parties and for the validation / evaluation team to modularly assemble data collection instruments responding to the specific needs of each





Demonstration Case while ensuring that consistent and comparable indicators are used in different cases;

- By mapping each high-level requirement in JIRA to SEQUOIA impact areas and CIS validation modules, it will be possible to aggregate validation and evaluation data across Demonstration Cases and present them using standardized categories in validation and evaluation reports;
- The documentation of a set of qualitative and quantitative indicators linked to high-level requirements and impact areas offers added value to stakeholders interested in developing self-assessment tools to judge the fitness for purpose and impact SecInCoRe can make for their organisation.

The mapping of SMART indicators and impact areas on JIRA requirements is an ongoing process. It will be refined and incremented as Demonstration Cases are further specified and SecInCoRe concepts are developed. Some examples of the work being undertaken are provided below (Table 5, Table 7 and Table 7).

JIRA REQUIREMENT SICR-9 When managing a CIS, prompt users to reflect on ELSI **CIS MODULES** MENTIONED IN CONSULTATIONS Collaboration practices yes ELSI taxonomy integrated into system interactions; Cloud; ELSI SecInCoRe Expected Outcomes sensitive Impact Areas Social capital; knowledge production and sharing in **SEQUOIA** POSSIBLE INDICATORS

PROJECT ASSESSMENT: Enhanced attention to ELSI and capacity to address them documented in Demonstration Implementations. broad dissemination of ELSI guidelines with documented feedback from stakeholders, including standardisation bodies. *VALIDATION*: Users report an increased awareness of ELSI after the Demonstration Case (item on post-case questionnaire). Users found ELSI-related information clear and useful for their practices (item on post-case questionnaire). Positive user reactions to ELSI support during use, in questions or comments (during-case observation). *EVALUATION*: Are users informed or trained about ELSI in their current practices / Zero Scenarios? Which tools are currently used to assist users reflecting about ELSI? In which ways can being more aware with SecInCoRe ELSI support enhance trust and collaboration with other stakeholders including civil society? (Interview or focus group).

Table 5. JIRA requirement and possible indicators. Example 1

JIRA REQUIREMENT		
SICR-135 Make data accessibility between users visible		
CIS MODULES	MENTIONED	IN
Collaboration practices; Taxonomy	CONSULTATIONS	





	no
SecInCoRe Expected Outcomes	Enhanced quality of information / interactions; Enhanced Trust, Efficiency; More informed
Impact Areas in SEQUOIA	Technological impact; knowledge production and sharing; Economic impact

POSSIBLE INDICATORS

PROJECT ASSESSMENT: Function implemented in Demonstration Implementations. *VALIDATION*: Users are satisfied with the detail of information on data acces and availability (item on post-case questionnaire). Users have identified new sources for information they needed for the Demonstration Case they were not aware of (item on post-case questionnaire). The information provided has shortened the time required to identify and access relevant information (item on post-case questionnaire). *EVALUATION*: Comparison between details on data accessibility in SecInCoRe and in current practices (post-case interview or focus group). Estimate on possible increases in efficiency in data gathering through the use of SecInCoRe (post-case interview or focus group), enhanced security and trust through being able to see what others can see (post-case interview or focus group).

 Table 6. JIRA requirement and possible indicators. Example 2

JIRA REQUIREMENT		
SiCR 34 Integration with current system and cross-platform suitable		
CIS MODULES		MENTIONED IN
NeC		CONSULTATIONS
		yes
SecInCoRe Expected	Cloud; Economical; Scalability	
Outcomes		
Impact Areas in	Technological impact; Financial impact; Environmental impact	
SEQUOIA		
POSSIBLE INDICATORS		

ASSESSMENT: development of communication system verified, usable and provided for at least one First Responder organisation. VALIDATION: Users would consider integrating their current systems and platforms into SecInCoRe (item on post-case questionnaire). Comments on SecInCoRe's understanding of requirements for current system and platform integration (during the case, possibly user journal or project team observation; after-case questionnaire item). EVALUATION: Description of advantages and problems encountered during the Demonstration Case and how these could impact on the efficiency of collaborations (interview or focus group). Estimation of the potential costs an organisation has to face to participate in SecInCoRe, or conversely of potential savings. Estimation of potential reduction / increase in technological waste if the organisation decides to participate in SecInCoRe (interview or focus group).




Table 7. JIRA requirement and possible indicators. Example 3

A list reflecting the current status of work on a subset of high-level JIRA requirements tentatively identified as candidates for validation and evaluation through Demonstration Cases is reported in Appendix 2: JIRA requirements and possible indicators. The list and detail is by no means exhausting, and it will be further specified to trace the connections between the results of previous consultations and the updated list of validation requirements. Appendix 2 also indicates which elements that had been identified as validation objectives in previous consultations will be excluded from evaluation and validation, explaining the reasons for the decision.

2.1.7 Assessing project progress through KPI

The assessment of the project achievements in relation to the project objectives is being conducted within WP5. The main aim of this activity is to assess the state of advancement according to project aims and related indicators provided in the DoW. The assessment of achievements has been undertaken through co-design workshops, ethical impact assessment, reporting in deliverables and publications. The data gathering on these achievements in WP5 will systematically continue with the involvement of stakeholders and project partners in charge of the activities and will be part of each validation and evaluation report.

In line with this, several indicators will be traced through one or more Demonstration Cases to map the minimum standard of the project. Table 8 reports the KPIs that had been identified in the DoW, and indicates how information to assess the progress of the project will be collected in the course of validation and evaluation activities.

A table summarising the progress of the project using the listed KPIs will be included in each Demonstration Case report. This formal assessment will allow tracing the advancement of the project during its development and will assist in providing a final picture of activities and aims reached when the project concludes. Results of the data gathered according to the KPIs will be partially contained in D5.4 (M30) and fully described in D5.5 (M36).

Objective	Sub-objective	Measurement	КРІ	Relation to validation and evaluation activities
Pan European inventory	inventory of information management processes	 identification of different emergency management models which are mostly 	Number of emergency management models	Assessment of ease of adding new models through at





	applied in five major countries within Europe	stored in the inventory	least one demonstration case.
inventory of data sets	 expansion of the CAST database about more than 25%, comprising more than 50% of inputs per dataset 	Expansion of the database more than 25% from the first collection	No longer relevant as CAST is not open. Instead a comparison with existing inventories has been carried out in WP2.
	 inclusion of at least two cross border crisis with involvement of First Responder organisations as well as Police authorities 	Number of cross border crisis engaging FR organisations and Police Authorities	Achieved in existing inventory; formal report will be provided in the next validation report.
	 usage of data sets in at least two additional projects 	Number of projects in which have been possible the integration of data sets	Assessed at the end of Demonstration Case I
	 integration of data sets in at least two different lectures 	Number of lectures in which have been integrated data sets	Assessed through internal partner evaluation.
inventory of information systems	 identification of more than 20 information systems mostly used in more than two of the major 	Number of information systems identified in the inventory	Assessed at the end of Demonstration Case II Assessment of





		countries in Europe and in more than five crisis included in inventory		ease of adding new IS through at least one demonstration case.
	inventory of business models	 identification of different business models used in five major countries and five crisis included in inventory 	Number of business models identified in the inventory	Assessed at the end of each Demonstration Case until objective is reached
				Assessment of ease of adding new IS through at least one demonstration case.
	inventory of cross cutting ELSI	 consideration of all cross cutting ELSI covering more than 80 % of German, UK, Greece and one 	Extent of the ELSI covering based on	Assessed at the end of Demonstration Case II
		additional major country's regulation	countries.	+ Assessment of ease of adding new IS through at least one demonstration case.
Common Information Space	definition of a taxonomy of data sets, standards, processes and information systems	development of one or multiple taxonomies covering all data sets, standards, processes and information systems recorded in achieving Objective 1	Number of taxonomies developed	Assessed through consultations with relevant stakeholders





	 consideration of at least five most common used taxonomies for every field (data sets, standards,) by reasoning integrating/neglecting specific characteristics 	Number of taxonomies considered	Assessed through consultations with relevant stakeholders
	 Uptake of results in at least one standardisation procedure for crisis management models and XML-Standards each 	TBD	
design of knowledge base and network enabled communication system	 derivation of one overall knowledge base concept which enables the record of more than 80% of the data gathered in Objective 1 	Number of knowledge base concept developed	Assessed at the end of Demonstration Case III
	 design of communication concept realisable in SecInCoRe (dependency to Sub- objective 3.2) and usable for at least one First Responder organisation and one Police authority (confirmation of more than one) 	Design of one CIS	Assessed at the end of Demonstration Case III
	 documented acceptance towards ELSI guidelines by more than three First Responder organisations and two Police authorities (measured according to response to workshops, 	Extent of the acceptance of ELSI guidelines by more than 5 organisations	Assessed at the end of Demonstration Case III



-



	interviews and questionnaires with end-users considering this aspect)		
	 dissemination of ELSI guideline at one conference focusing on ELSI issues 	Numbers of conferences where have been discussed ELSI issues	ELSI Guidelines paper accepted for ISCRAM 2016, ELSI Guidelines part of workshop at PSCE 2016
design of a secure dynamic situation-aware disaster cloud infrastructure	 definition of a disaster cloud infrastructure enabling access and role specific information provision to end-users identified (interviews, questionnaires) 	Definition of 1 disaster cloud enabling access to users with 75% of positive feedback of all cases	Assessed at the end of Demonstration Case II
	 provision of data will be appropriate in more than 75% of all pilot cloud service applications in validation activities (measured according to response to workshops, interviews and questionnaires with end-users considering this aspect) 	Indicators described by the verification	Assessed at the end of Demonstration Case II





	seamless federation of heterogeneous information systems	 definition of a standardised XML- based language which enable a cooperation with more than 60% of the information systems identified in Objective 1 	Indicators described by the verification	Assessed at the end of Demonstration Case II
		 usage of respective results in at least two additional projects 	Number of projects where are used results	Assessed at the end of Demonstration Case II
Conceptual integration of available technology	implementation of pilot cloud services and provision to end-users	 development of cloud service verified, usable and provided for at least one First Responder organisation and one Police authority 	Indicators described by the verification	Assessed at the end of Demonstration Case II
		 outage of pilot service in not more than 10% of the test cases documented 	Indicators described by the verification	Assessed at the end of Demonstration Case II
	implementation of communication system and integration to end-user environments	 development of communication system verified, usable and provided for at least one First Responder organisation and one Police authority 	Indicators described by the verification	Assessed at the end of Demonstration Case II
		 outage of system in not more than 10% of the test cases documented 	Indicators described by the verification	Assessed at the end of Demonstration Case II
Validation and evaluation	new crisis management model	 development of at least one crisis management model accepted by more than 75% of end- 	TBD	





	users (measured according to response to workshops, interviews and questionnaires with end-users considering this aspect)		
	 consideration of at least five most common used crisis management models by reasoning integrating/neglecting specific characteristics 	TBD	
conclusions on business models	 development of at least one business model accepted by more than 50% of end-users (measured according to response to workshops, interviews and questionnaires with end-users considering this aspect) 	TBD	
	consideration of at least five most common used business models by reasoning integrating/neglecting specific characteristics	TBD	

 Table 8. Measurement to validate the achievement of the project

2.1.8 Outline of the remaining Chapters

The remaining Chapters provide further indications on the implementation and definition of the validation and evaluation strategy. Chapter 3 introduces the work on the identification of stakeholders, while Chapters 4 and 5 deal with the CIS





Demonstrator and the related Documentation. Chapter 6 presents the work completed so far on the definition of the Demonstration Case Protocol and on the identification of first Demonstration Cases for validation and evaluation activities.







3 Summary of project stakeholders, their needs and involvement

This section develops the mapping of stakeholders started in D5.2.

In particular, the difference between end-users and stakeholders is clarified here. Endusers are those who may directly interact with the technological components of the SecInCoRe system (such as category I and category II responders, volunteer agencies). The term 'stakeholders' refers to a broader group of people who may indirectly benefit or be affected by the system. This includes citizens whose data may be processed with the help of SecInCoRe. The main purpose of the section is to show how starting from a general map of the stakeholders (D5.2), it is possible to identify key organisations for validation and evaluation activities.

Validation will, on the one hand, be performed through demonstrations where people will directly interact with the SecInCoRe system. On the other, evaluation will also be performed through qualitative methods to assess the impact of the socio-economic system even where no direct usage of the demonstrator is involved

In D5.2 stakeholders in three different areas were identified: public sector, private sector and civil society. Within the three categories specific professional figures were identified as stakeholders or end-users of the project (a thorough classification is provided in D5.2 and in D4.2, Appendix B).

However, at the current stage of the methodology implementation it is crucial to better define the mapping of end-users and stakeholders that will be involved in validation and evaluation activities.

Taking into account advice from project reviewers, partners and the AB, it has been decided that the first round of validation and evaluation with external parties will be organised in relation to training and preparedness activities. However, it is possible that, following future development of the project, further validation and evaluation activities will be performed according to operational stages of the crisis (such as the initial response, consolidation and recovery phases) involving a wider scope of stakeholders and end-users.

In line with this, the identification of stakeholders and end-users for the validation and evaluation of SecInCoRe in relation to the activities that are currently identified is defined as *such professional figures working in the emergency sector that are in charge of preparedness and training activities*. Such figures are related to public services and are mainly first responders and police authorities.

Indeed, referring to the work done in D4.2 (Appendix C and particularly point C.2), it is possible to identify some key figures in charge of the preparedness phase. As reported in D4.2 (p. 339) '*Preparation means all activities that intend to prepare for response to dangerous incidents. A special focus is on planning activities and training. Preparation does also subsume preparative resource allocation for special happenings to be able to react quickly in case of incidents (for instance, rescue services prepare for incidents at soccer stadiums). Results from preparation activities are relevant as soon as an incident happens'. This step is properly called "contingency plan".*

So, taking into account D4.2, the main stakeholders and end-users that will be engaged in validation and evaluation activities are the professional figures working in





emergency planning, that can be founded in several main categories, across the public and private sectors, including local and health authorities.

Continuing the work done in D4.2 (section B), it is possible to extrapolate the following categories of stakeholders and end-users that will be involved in the first round of activities of validation and evaluation (Table 9):





A Direct Users and indirect users

Direct Users
Public sector
First responder services (Police, Fire, Emergency Medicine)
Crisis management staff
IT managers and staff
Municipalities:
Emergency planners
IT managers and staff
Researchers (Risk Governance)
Health bodies:
Emergency planners
IT managers and staff
Public Infrastructure (Transport, Highway, Harbour, Underground, Airport):
Emergency planners
IT managers and staff
Pan-European institutions (as potential hosts for the SecInCoRe system)
Emergency planners
IT managers and staff
Urban planners
Private Sector
Public utilities (Water, Gas, Electricity, Telephone):
Emergency planners
IT managers and staff
Private Emergency Services:
Emergency planners

Table 9. Direct and indirect users involved in the validation / evaluation activities

However, looking particularly at the examples gathered in D4.2 in relation to the stakeholders involved in the specific phase of preparedness where "*Preparation means all activities that intend to prepare for response to dangerous incidents. A special focus is set to planning activities and training*" (p. 335, D4.2), groups of actors





that absolutely need to be involved in the activities, due to the centrality of their actions, are the following (Table 10):

First Responder planning department
First Responder exercise planning staff
Researchers

Table 10. Direct users main categories involved in the preparedness phase

Such specification also reflects the data gathered from the collection of the zero scenarios on training and preparedness activities. Indeed, looking at the current practices described by people working in the emergency sector (and specifically in health services, police authority, fire brigade and local authority) emerges that figures generally involved in this preliminary phase of the emergency is the personnel working in the Emergency planning Unit.

However, this categorisation is very much related to the first round of evaluation and validation and it is important to stress that the more comprehensive categorisation developed in D5.2 is still valid and other actors involved in other phases of the emergency management cycle, will be considered in other iterations of validation.





4 Common Information Space Demonstrator V1

The Common Information Space Demonstrator is a compilation of all Reference Implementations of SecInCoRe. The concept and the architecture is described in section 4.1. The details about the recent implementation status are explained in the following sections.

4.1 Concept

The CIS concept comprises a Cloud based Emergency Information System (CEIS) concept. To facilitate and simplify uptake of this concept in terms of demonstration cases and productive use, reference implementations are designed and implemented within the project (to be continuously extended after the project). The concept intends to add value to existing information systems which might or might not need additional ICT services; reference implementations are either realised by referring to existing systems or adopting open source packages. SecInCoRe assembles and adapts this range of open source tools and provides unique integration and functionality through its common information space concept, taxonomies, inventory and network enabled communication concepts.

CEIS targets every phases of a crisis, described in the crisis management cycle (Response, Recovery, Mitigation, Preparedness) and also supports various stakeholders in their individual task accomplishment in the public and private sector as well as civil society. To show the SecInCoRe advantages in a live system, at least three reference implementations are planned. The high-level architecture of the implementations is shown in Figure 6. The implementation on the left is the Open Atrium (OA). It enables a structured representation of all concepts and demonstrators of SecInCoRe. After that, the OA offers the possibility to extend the contents in a collaborative way with community members. Another small implementation is the 'Contribute' functionality, which can be used by everyone to contribute relevant information (meta-data or documents) into the Knowledge Base (KB). The next implementation is the Semantic Media Wiki (SMW), which should be used as a collaborative ontology creation tool. The last, but important implementation is the Open Semantic Framework (OSF). This implementation indexes the data of all other implementations, as well as the internal (Past disaster database, etc.) and external databases. General and SecInCoRe-internal ontologies are used to enable the semantic search in all indexed data sources. These sources contain SecInCoRe outcomes as well as domain specific data.







Figure 6. Reference Implementations

4.2 Reference Implementations used in Demonstrator implementations

In the following section, various Reference Implementations, which SecInCoRe use in demonstrator implementations, are described.

4.2.1 Open Semantic Framework

In a first step, a very basic search system was installed based on Open Semantic Search, also presented in D3.3.

After a detailed analysis, Open Semantic Framework was identified as the best fitting base for the search system. This system should enable an easy and domaincustomized way to find the needed domain specific data. At the moment the system has the possibility to trawl file systems, analyse the files found with an uploaded ontology and make them searchable. The search offers only basic functionalities now, but will be improved within the next few months. Particularly, no database connection is established yet and the semantic tagging is performed with a single ontology. Later on, ontologies from within the SecInCoRe project, from the SMW and from external domain ontologies should be integrated. The ontology data is used to tag the indexed files with corresponding concepts of the ontologies and to filter the search results. Further functionalities will be developed. The most recent GUI is shown in Figure 7

	D5.3 Validation Strategy, Version 2 (ic) Public deliverable	DecInCoRe
Home » fire		
Filter by structural engineering: • true (1)	SecInCoRe Enter your keywords	Filter by dataset: • True (3)
Filter by fire brigade: • true (1)	Search The search found 3 results in 0.502 seconds.	Filter by human resources (employees): • true (1)
Filter by deaths: • true (1)	Search results 2005 - Buncefield Oil Depot Explosion and Fire, UK.pdf 2010 - Love Parade Stampede, Germany (UPB).pdf	Filter by country: • true (1)

Figure 7 SecInCoRe OSF GUI

4.2.1.1 Planned future implementations

The above described systems and functions are the current development state. Concerning the different timeslots of the demonstration cases, different further developed versions of the systems will be available. The figure below shows the most recent mock-ups of the search and its integration into a single web application with other systems. The first mock-up shows the result page of the search. On the left is the menu, which allows to choose the project and the desired demonstration implementation. The functions behind the menu items are mainly further developments of the above described systems. The right hand part is the search result list. The list offers filters, which are based on imported domain specific ontologies (The filters at the left). After that, the "additional information" section shows information, which are extracted from Linked Open Data sources and are related to the keyword, searched for. Additional further information could be added below. For example, small map or hierarchy views. In the middle, a standard search result list is shown, which contains the additional extracted metadata and the possibility to open the result in a different view. The user can open the document in a more detailed view, can open the original document (i.e. the .pdf) or show it in a map or hierarchy context.





		Searchf field	Search		
nCoRe	Search Hierarchy Map	Details			
iearcch		1			1
lpload	Filters	Document title 01/01/2016	Materia	OPEN	Additional information
have to favor and the	Taxonomy	Content of the large large	metdutata:	OPEN:	
have intormation		Lorem IpsumLorem IpsumLorem Ipsum	Author: XY	Details	
atabases	Category	Lorem IpsumLorem IpsumLorem Ipsum	Topic: XY	Hierarchy	
	Subcategory	Lorem IpsumLorem IpsumLorem Ipsum	Source: XY	Map	LOD Infos
letworking	Subcategory	Corem (psumCorem (psumCorem (psum			
oncept	Subcategory	Document title			
		01/01/2016	Metadtata:	OPEN:	
owTo	Category	Content Lorem Ipsum	Author XY	Details	
-1-4		Lorem IpsumLorem IpsumLorem Ipsum	Tagin VV	Original	
e Lub	1	Lorem Ipsum Lorem Ipsum Lorem Ipsum	Type: PDF	Hierarchy	
		Lorem Insum Lorem Insum Lorem Insum	Source: XY	Map	
					Map
	Author	Document title		0.051	
	Filetype	Control of the second	inetautata.	OPEN:	
		Content Lorem Ipsum	Author: XY	Details	
		Lorem Ipsum Lorem Ipsum Lorem Ipsum	Topic: XY	Original	
		Lorem Ipsum Lorem Ipsum Lorem Ipsum	Type: PDF	Hierarchy	
		Lorem IpsumLorem IpsumLorem Ipsum	Source: XY	мар	
					1
					1
					1

Figure 8 Search results

The hierarchy context is shown in the second mock-up. The result document is placed in the middle and all available detailed information are displayed at the bottom. The upper part visualizes the alignment of the document concerning different ontologies. The document is aligned at the corresponding categories by an automatic topic extraction. For example if the document describes the matrix organization of a fire brigade in Brussels, the topics "Fire brigade" "Brussels" and "matrix organisation" will be extracted. The document would be displayed in the taxonomy "PPDR organizations" in the category "Fire Brigade", which is a sub category of "Fire fighting unit" and parallel in the "Processes" taxonomy in the category "Organization concept". After that, the logical position of "Brussels" would be shown as a continent, country, and city hierarchy. A click on a category could expand it and show other related documents and others, which are connected to the same topics as the first document. More detailed information about the search concept and the integration/ relation with the other implementations follow.







Figure 9 Hierarchy view

4.2.2 Open Atrium

A first version of the structure of the CIS concept documentation (Figure 10) is provided to the public. For this purpose, an adapted Open Atrium solution was implemented with regards of SecInCoRe needs. This platform aims to show developed concepts, demonstrate first solutions and to call other to collaborate with the SecInCoRe consortium on a strategic level. Therefore, users could navigate through all outcomes of SecInCoRe using the CIS concept structure or the respective menus. The first draft of the content is inserted and will be enhanced by all project partners over the remaining project phase.







Figure 10 CIS Concept [D4.2]

4.2.2.1 SecInCoRe OpenAtrium platform concepts and features

The following section outlines the Spaces and Sections conceptual model of the SecInCoRe Open Atrium deployment (Figure 11).

- A "**Space**" is a subset of content within your Open Atrium instance that is shared among a collection of users (members). Hence, a "Space" can be used for a Project, Department, Microsite or any other collection of related content and people.
- A "Section" is a collection of content within a specific "Space" that is tightly related, or private to a specific set of users. A "Section" can be used for specific working areas within a Space, such as a Discussion or Wiki. Further, a "Section" can be assigned specific access controls to limit its visibility.







Figure 11 OpenAtrium Spaces and Sections conceptual model

The following section outlines the Members, Groups and Teams Access Control principles of the SecInCoRe Open Atrium deployment.

- Spaces have Users assigned to them called "Members"
- "Members" can have special permissions, such as Edit and Create
- A "Group" is a collection of users with related roles or interests that span across multiple Spaces.
- A "Group" can represent a specific company or organisation, or it can represent a common role, such as "researcher", "training planner" or "first responder"
- Groups are used to assign access control to specific Sections within Spaces.
- Groups are used for Notifications.
- A "Team" is an ad-hoc collection of users within a specific Space that share a related purpose.
- "Teams" are used to assign private access control to specific Sections within Spaces.
- "Groups" estend beyond individual Spaces whereas "Teams" are specific to a particular Space.
- Teams are used for Notifications.







Figure 12 Open Atrium Members, Groups and Teams Access Control principles

For example, in the SecInCoRe project and internally within the consortium, a **Space** can represent a high-level domain objective, such as ELSI, NEC, CI. These can be shared selectively with Advisory Board members either on the individual member, or Group basis. Open Atrium also integrates with industry standard Identity Management protocols (LDAP), making it extensible and compatible with the Federated Identity Management demonstrator presented in section 4.2.6.

For public-facing content, **Spaces** could represent Training courses, Dissemination or Workshops.

Examples of **Sections** within each SecInCoRe Space include sections for discussion, scheduling, task management, file / image upload and discussion.

A **Group** could be representative of a given organisation, such as SecInCoRe consortium members, a regional police force or government institution, AB members, Researchers, Public sector workers.

Teams and **Private sections** can be formed to bring together multiple groups, for training or workshops, allowing multiple stakeholders from different organisations to work together in a specific domain on a given task.

4.2.3 Semantic Media Wiki

The Semantic Media Wiki (SMW) is based on the Media Wiki software. It enables the semantic storage of all contents (e.g. categories of a taxonomy) and the underlying structure of the wiki. This can be used to develop taxonomies with users. The recent implemented version is a very early instance of the Semantic Media Wiki with no additional features. The plan is, to create a concept for the SMW, which enables a simple and intuitive way for collaborative content editing. The structure of the community generated domain specific content should be used as an ontology for the search in OSF.

For the community-based ontology a collaborative semantic platform is planned.





4.2.4 Knowledge Base

The Knowledge Base is the implementation of the inventory categories and in this way the inventory builds the basis of the Knowledge Base. Therefore, the inventory follows two lines: first a comprehensive analysis of information systems, business models, processes and data sets was started. Further to ensure a sustainable usage of the system existing databases, glossaries and ontologies will be integrated and added to the inventory content. The Inventory contains at the moment two SecInCoRe-owned databases: An overview of past disasters is stored in the Past Disaster Database and a second database contains domain relevant information systems. The work on the overview of European processes and corresponding documents is on-going. The aim is to create a critical mass of information and support mechanisms (e.g. templates) that can ease community contributions.

4.2.5 External Applications

The CEIS concept aims to improve the communication and the access to information in the domain. There are several systems already at the market, which could be used to reach these aims. Therefore, the above-mentioned implementations are complemented by external systems. For example, the communication and group creation within the domain members can be established by securely adapting existing chat or social applications. The feasibility of integrating this emerging requirement into the Federated Identity Management service will need to be further evaluated. Existing end-to-end security approaches as described in the NEC concept in D5.3, section 4.2 should be made use of and extended where the social applications cross the SecInCoRe CIS boundary. Results of previous research projects will be integrated in demonstrator implementations if the respective demonstration case requires such available functionalities, i.e. by the integration of the CIK_AppFramework.

4.2.6 Federated Identity Management, AAA and SSO to the CIS

One of the cornerstones of the CIS concept is the facilitation of collaborative work between different stakeholders from different organisations and from different countries. To that effect, research has been conducted into best practices in organisation-wide and trans-organisational Identity Management.

Such IDM (Identity Management) solutions enable for passwords to be managed and changed at a central place, then distributed to external systems automatically using rules and password policies. External password changes are also detected and the IDM solution takes appropriate and pre-specified action. Passwords can be reset and can be sent to users in a secure way, with this applying end-to-end in the CIS.

If a new user is added to the CIS, depending on a user's business role, or the group to which they belong, the pre-defined rules in each group will allow a new user to instantly have accounts created on each CEIS component with the default group / role membership access rights.

The IDM solution therefore connects to all relevant systems, syncs user attributes and memberships and can automatically apply rules.

External organisations should be able to integrate their existing Identity Management solutions into the SecInCoRe cloud-based CIS IDM, in order to quickly and transparently provide their members with access to the CIS. This will require





Federated Identity Management and will be subject to further research, development and integration work.

4.2.6.1 NEC AAA Demonstrator

An early prototype Identity Management solution was presented at the Dortmund plenary meeting in October 2015. The hardware used for the AAA / IDM demonstrator were:

- D-Link DIR-615 Wireless N 300 Router, with DD-WRT installed to replace the factory firmware.
- The router's WiFi network was configured to use 802.11i WPA2-AES Enterprise as the encryption technique.
- A remotely deployed Synology DS211+ NAS to facilitate LDAP and RADIUS, with which the router grants or denies access to devices (users) requesting Wi-Fi access.

An LDAP server consisting of a database of end-user identities and their access privileges, together with a RADIUS server were used as a AAA solution to 802.11ienabled NIC access. A WiFi access point was configured to facilitate WPA2-enterprise network access, by requesting the access point authenticates and authorises users via a RADIUS server, which in turn was connected to a LDAP database. The RADIUS server received username and password credentials from end-users and forwards these to the LDAP server, which in turn verifies them, then checks its database to confirm whether the stated end-user is authorised to access the WiFi network.

dd-wrt.com c	control panel		f Time: 14:21:1	Firmware: DD-WRT 7 up 8 min, load av	v24-sp2 (03/25/13) s verage: 0.00, 0.06, 0.0 WAN IP: 192.168.0.11
Setup Wireless Services	Security Access Restricti	ions NAT / QoS	Administration	Status	
Basic Settings Radius Wirele	ess Security MAC Filter	Advanced Settings	WDS		
Wireless Security wl0				Help	more
Physical Interface ra0 SSID [SecInCol Security Mode WPA Algorithms Radius Auth Server Address Radius Auth Server Port Radius Auth Shared Secret Key Renewal Interval (in seconds)	Re wifi] HWAddr [14:D6:40:0 WPA2 Enterprise AES Image: Secret Key 3600	224 (Default: 1812)		Security Mode: You may choose WPA Personal, W RADIUS. All devic must use the san With N-Mode you WPA2/AES.	from Disable, WEP, PA Enterprise, or zes on your network ne security mode. ir must use
	Save Apply Settings	1			

Figure 13. WIFI access point configuration

The 802.11i WiFi access point is configured to authenticate end-users using WPA2-Enterprise, meaning that either a username / password pair is required to get network access, or a smartcard containing a PKI private key. The IP address of the cloudbased RADIUS server, along with the shared secret necessary to access the RADIUS server is configured into the Access Point.





1			Directory Serv	/er		2 -	E X				.0
	Settings	Create - Edit	Delete		Email	Y Search	5				
	Backup and Restore	admin	Directory/Diskstat	ion default a		Norm	al		-	* =	
	👤 User	alex				Norm	source	Monitor		_	
Co	Group		Add	Edit	RADIUS Se	rver		7 -			
-	G Google Apps Single Sign-On	Settings		Vame	IP address	Subnet mask	Secret key	🖌 En	able		
FI		Clients	DIR_6	15_DDWRT	90.154.240.143	255.255.255.255	secretkey	~		-	
		🧏 Block List									
		E Log								^	
										~	
										M 5.2	

Figure 14. RADIUS Server network access

On the cloud side, the 802.11i WiFi Access Point's IP address is specified and only an access point from that IP address with a specific shared secret can access the cloudbased RADIUS server. The shared secret is configured on the RADIUS server. This ensures upmost security. All username / password pairs are transferred through AES, EAP or equivalent strongly encrypted tunnels.

					91	00	08
Settings	Create - Edit	Directory Server Delete Description	Email	P − ⊡ X ▼ Search Status			R
Backup and Restore	admin alex	Directory/Diskstation default a		Normal	source Monitor	- * =	
Co: Cogle Apps Single Sign-On	Settings Clients Block List Log	Common Settings Authentication port: Select the source against Local users LDAP users Domain users Import root certificate to Download Root Certifica	RADIUS Serve	***i ***i r authenticates users: devices if you use a self-signed or Syn	P — E	× 396 3%	5.2

Figure 15. RADIUS Server settings

The RADIUS server is configured to authenticate users against the LDAP (directory) server. A separate LDAP server can be observed on in the background, containing a





database of users, which can or can not access specific resources, e.g. Access Points or CEIS components. As can be observed in the Directory Server window, each user can belong to one or many 'groups', thus inheriting group-wide access permissions.

0%0	DiskStation home			···· 🙆)			1.47	(/s	. II. i		15:09	4	\$	2.83K/s ຈີ 	15:23
	No Internet			<۷	Secl	nCo	Bey	wifi					<	Wi-Fi		
°a	TP-LINK_5AFC3C	WiFi Sense		s	ecurity							-1		SecInCoRe wifi		a
-	connected, open,	Will Schild		8	02.1	K EAF	Þ							SecinCoRe	wifi	
(k.	Premier Resort			lo	lentity							1		Secilicone	WIII	_
					alex	rd								Status Connected		- 8
ſ.	SecInCoRe wifi Secured			ĺ	••••	••••	••					ר		Signal strength		- 8
	Enter your usernam	ne and password												Excellent		- 8
	alex				<u> </u>	Show p	passw	ord						Link speed 150Mbps		- 1
	•••••		0	Ŀ								1		Security 802.1x EAP		- 1
	ОК	Cancel			С	ancel	_	_		Conne	ect	_		IPv4 address)	- 8
				a ¹	\mathbf{w}^2	з е г	r t	5	6 / L	7 J	i ⁸ c	90 00		IPv6 address	-	- 8
				۹ (۵) #	&	*		+	=	(fe80::208:22ff	:fe56:3d0f	
				а	S	d	f	g	h	j	k			Cancel	Forget	- 8
Netv	vork settings			\uparrow	z	×	с	v	b	; n	m	$\langle \times \rangle$		Apple Network		
ſ.	\$			100	Ŷ					_	,!?	0		Not in range		
Conne	cting Flight mode			123			Engl	lish (UK)			\leftarrow		57		+

Figure 16. RADIUS Server Authentication different devices

Figure 16. RADIUS Server Authentication different devices shows a Windows machine and an Android tablet presenting the end-user with a WPA2-Enterprise username / password challenge in order to access the SecInCoRe 802.11i network.

	Directory Server	7 - E X	
🔯 Settin 💽	RADIUSS	Server P — E X	
Settings	Refresh Clear Save		
Backu	Type Date & Time	Event	
User Clients	Auth 2016-02-15 15:26:02	Login incorrect: [alex/ <via auth-type="EAP">] (from client DDWRTrou</via>	
	Auth 2016-02-15 15:26:02	Login incorrect: [alex/ <via auth-type="EAP">] (from client DDWRTrou</via>	
Le Group Block List	Error 2016-02-15 15:26:02	[mschap] Invalid LM-Password	
Concle	Auth 2016-02-15 15:20:41	Login OK: [alex] (from client DDWRTrouter port 0 cli 00-08-22-56-3D	
G Sign-C	Auth 2016-02-15 15:20:41	Login OK: [alex] (from client DDWRTrouter port 0 via TLS tunnel)	
	Error 2016-02-15 15:20:41	[mschap] Invalid LM-Password	
	Info 2016-02-15 15:18:23	Ready to process requests.	
	Info 2016-02-15 15:18:23	Loaded virtual server inner-tunnel	
	Info 2016-02-15 15:18:23	Loaded virtual server <default></default>	
	Info 2016-02-15 15:18:22	Exiting normally.	
	Info 2016-02-15 15:18:22	Signalled to terminate	
	Info 2016-02-15 15:18:02	Ready to process requests.	
	Info 2016-02-15 15:18:02	Loaded virtual server inner-tunnel	
	Info 2016-02-15 15:18:02	Loaded virtual server <default></default>	
	Info 2016-02-15 15:18:00	Exiting normally.	





Figure 17. RADIUS Server audit log showing multiple access attempts

An audit log of access attempts by specific username / password pairs at the Access Point is maintained on the RADIUS server.

This solution will in future be further developed to support smart card, hence certificate-based authentication, bringing a high level of security and accountability to NEC access. This infrastructure also allows for CIS components, for example Open Atrium to authenticate with this central Identity Management service (the LDAP server), meaning that a single database can contain access privileges to every CIS element. Administration of user access rights is thus conducted at one central service, with the ability to easily revoke user rights in cases of identity theft or end-users no longer being part of a given organisation, or if an access device is misplaced.

4.2.6.2 Validation and outcomes from the NEC AAA Demonstrator

Following the presentation of the proposed AAA solution, consortium partners identified an existing pan-European solution for network access, whose architecture closely resembles the SecInCoRe CIS AAA solution, namely – Eduroam and to some extent, Edugain. Eduroam can be mapped to NIC AAA, while Edugain to CEIS AAA. These successful best-practice patterns will form the basis of the SecInCoRe Federated IDM solution, bringing with them proven assurances of Pan-European (and global) adoption leverage to organisations wishing to join and to integrate their existing IDM solutions into the SecInCoRe cloud-based CIS.



Figure 18. Eduroam: Ubiquitous Network Access

A high-level overview of the Edugain deployment pattern. As of April 2005, more than 350 institutions in 18 countries participate in Eduroam.







Figure 19. Map of countries participating in Eduroam

4.2.6.3 Ongoing research and implementation of the CIS AAA service

Current research into Single-Sign-On and Federated Identity Management has been conducted and has identified a number of suitable implementations. The shortlist of technologies to be further exercised and their suitability to SecInCoRe's goals confirmed include OpenLDAP, FreeRADIUS, MIT Kerberos, Dogtag, 389 Directory Server, FreeIPA, OpenIDM, phpLDAPadmin and Microsoft Active Directory. The suitability of these technology stacks will largely depend on typical end-user devices and demonstration scenarios. More importantly, a deployment pattern should be followed with an implemented reference implementation, allowing scope for future extensibility and third-party IDM integration. Currently, the best suited IDM'solution for Windows is Microsoft's Active Directory, while for Linux-based machines, the most mature solutions appear to be 389 Directory Server and FreeIPA. A table illustrating these two stack's characteristics is listed in Table 11:

	389 Directory Server	FreeIPA
Use	General purpose	Single domain, focused on identity management
Flexibility	Highly-customizable	Limitations to focus on identity





		and authentication
Schema	Default LDAP schema	Optimised, special schema for identity management
Directory Tree	Standard and flexible hierarchy	Flat tree with a fixed hierarchy
Authentication	LDAP	Kerberos or Kerberos and LDAP
Active Directory Synchronization	Bi-directional	Unidirectional, Active Directory to FreeIPA
Password Policies	LDAP-based	Kerberos-based
User Tools	Java Console and standard LDAP utilities	Web-based UI and special Python command-line tools

Table 11. Possible implementation

FreeIPA is essentially an equivalent to Microsoft's Active Directory (AD), but focuses on the needs of Linux and UNIX systems. To be clear, FreeIPA is not a replacement for AD, it is rather an "overlord" for Linux/UNIX environments that can stand by itself or be a subordinate to Active Directory.

Active Directory not only integrates several services (namely: LDAP, Kerberos, and DNS) under one hood, but it also allows for more complex relationships between identity sets. For example, traditionally, we think about an LDAP server (or a group of LDAP servers sharing the same replicated data) as a single namespace. AD can not only handle different namespaces, but can also manage complex relationships between them. These capabilities solve real world problems and led to the following two major results:

- 1. AD became a dominant identity solution in the enterprise and
- 2. This allowed environments to become much more complex. Identity data could now be organized into multiple different domains or (even) collections of domains called forests (see *Figure 20*).

A tree typically represents a subdomain of an organisational domain. For example, if the organisation is SecInCoRe, a tree would represent the Dortmund, Rome or London location, i.e. rom.secincore.eu, lon.secincore.eu etc. A forest encompasses and manages each tree, or organisational location / department. SecInCoRe's Identity Management solution would manage the entire forest, with access rights easily transferrable between locations – something of significant value where end-user mobility is frequent.

Cross-forest trust entails trust between separate organisations and / or IDM solutions. This will be the topic of further research and integration, resulting in the SecInCoRe Federated Identity Management solution. Cross-forest trust also encompasses social





media SSO technologies, such as OAuth2 – a technology not directly mappable or compatible with SAML, the SSO standard popular with academia.



Figure 20. Trust between federated domain controllers

Forest = different subdomain, e.g. different organisations. Cross-forest trust is important and encompasses not only technological, but also procedural and administrative practices by a peer organisation. EduRoam does outline such best practices, which will be reflected within the SecInCoRe CISD.

Further reading has identified the following deployment considerations, namely:

- It is best to use a Samba Active Directory Domain Controller (AD DC) on the server if you have mostly Windows machines and a single forest topology.
- Use FreeIPA if the majority of your machines are Linux or other UNIXcompatible systems. Client side configuration for Linux is mostly automated and is available in most distributions.
- FreeIPA is great for integrating existing Active Directory forests. The flow is mostly automated.
- Support for Linux-specific access controls is built in if client side uses SSSD.





5 Manual for first version of the Common Information Space System

This manual describes the usage of the main reference implementations of SecInCoRe. All descriptions refer to the version of 10th February. All logins could be requested via email: <u>secincore-upb@lists.upb.de</u>

5.1 Integrated GUI

A quick draft is done, to show all reference implementations within one GUI. It is cumbersome to have a different URL for each CIS subsystem and as such, the CEIS integrated GUI aims to unify these modular and functionally isolated subsystems into one SecInCoRe branded User Interface. This early prototype of the Integrated interface is accessible via: <u>http://31.171.251.73/</u>

You can use the tabs to switch between the different implementations. The key tabs are described below. OpenAtrium as a fine-grain access management knowledge base solution is accessible via a dedicated tab in the Integrated GUI, but considering the complexity of the platform, it is described in further detail in section 5.2.

5.1.1 Search

The search implementation offers the possibility, to search in the domain specific data in the inventory. The usage of the recent search is quite simple.

The URL where the search could be found is: <u>http://178.22.69.94/</u>

SecInCoRe	
Enter your keywords	
fir	
Search	

Figure 21. Search function

When the URL is open, you are prompted to Login. Please insert your data and click "Login".

After this step you will see the search field. Type in your keyword to search for and click "Search".

You will see the search results in the middle of the screen. Open a result by clicking at it. There is the document title and the plaintext of the result shown.

If you want to see the result in the raw format with all links and tags, go to "export", choose "rdf+xml" and "Open".





Back on the result screen (step 3) there are filters shown at the left and right side of the results. These filters refer to tags which are found in the search results. Filter your results by clicking on the filters.

5.1.2 Semantic Media Wiki

The Semantic Media Wiki is planned as a collaborative ontology creation tool. The concept is not final established, therefore the usage is not described in detail.

The URL is: <u>http://31.171.251.73/mediawiki/</u>

5.1.3 Databases

The past disaster database and the information system database are stored as SQL databases.

The raw databases are accessible at http://31.171.245.222/sqlbuddy/

To browse the information system database go to:

http://31.171.245.222/sqlbuddy/#page=browse&db=InformationSystems&table=Inform ationSystems

5.1.4 External applications

For external applications no instructions are given here, as these are due to be further researched and integrated in a later project phase into the SecInCoRe reference implementations. Example applications could include the following. Please find the instructions on the relevant website.

- LinkedIn will prove invaluable as an Identity Management and social networking provider, as the quality and trust inherent in the platform will ensure a higher degree of trust when performing profile attestation. As demonstrated internally within SecInCoRe when seeking out appropriate Advisory Board members, LinkedIn has no peer in terms of lead quality. However, ELSI issues revolving around previous reports of LinkedIn selling data to advertisers should be considered.
 - <u>https://help.linkedin.com/app/home</u> help centre
- File sharing application not configured yet.
- Pidgin or an equivalent XMPP-based IM solution / bridge <u>https://www.pidgin.im/</u>

5.2 Open Atrium

Open Atrium is an open source platform that enables organizations to create best in class community driven websites through powerful knowledge management and social collaboration tools. The framework allows organizations to easily integrate existing software and additional features, while remaining extensible enough to change as the organization or scope of the knowledge base and user base grows. The SecInCoRe OpenAtrium cloud-based deployment can be accessed directly at: http://185.12.5.114/. A first draft for dealing with the functionalities of Open Atrium in the context of SecInCoRe and the use for documenting and discussing the SecInCoRe CIS concept





is described in D4.2, especially regarding the practical use and responsibilities within the project.

A further description and explanation can be found in Appendix 5: SecInCoRe OpenAtrium User Manual.





6 Validation and evaluation plan: protocols, instruments, Demonstration Cases and timeline

This section provides further details concerning the specification of the elements needed to implement SecInCoRe's evaluation and validation strategy according to the principles outlined in Chapter 2. Work is on-going, and will be integrated in a living version of the Validation and Evaluation Strategy document.

6.1 Demonstration Case Protocol

A Demonstration Case Protocol is being developed in consultation with project partners to cover all aspects in the lifecycle of a Demonstration Case, starting from its planning, to its definition in cooperation with stakeholders, to its execution, to the collection of data in different phases and to their analysis and reporting.

Different Templates will be used as part of the Demonstration Case Protocol. Templates are at the same time an instrument to collect structured and consistent information on a Demonstration Case to be included in the Demonstration Cases Database, as well as a tool for favouring collaboration and cooperation among all project members and teams involved with different aspects of the Demonstration Case. Two templates will be used to cover different phases in the planning of a Demonstration Case:

- 1. A Demonstration Case Template will be used by project team members to:
 - a. collect and exchange information on the preparatory phases of a Demonstration Case;
 - b. define the general aims and objectives of a Demonstration Case and clarify its role within the overall Validation and Evaluation Strategy;
 - c. list possible Demonstration Scenarios that will be then discussed, refined and modified with stakeholders;
 - d. To collect feedback and observations from an ELSI and evaluation/validation perspective;
 - e. to identify and refine the Demonstration Implementations that will be required for running the Demonstration Case.
- 2. A Use Cases Template will then be used to:
 - a. Define the final Demonstration Scenario that has been developed in collaboration with Stakeholders;
 - b. Define a set of embedded Use Cases related to the Demonstration Scenario. Although Use Cases are expected to evolve as stakeholders participate in the Demonstration Case, a detailed mapping of initial challenges, opportunities and expectations concerning the interactions between stakeholders and Demonstration Implementations will help to interpret and analyze any emerging needs or uses that deviate from initial expectations
 - c. Develop the specific data collection instruments that will be used before, during and after the Demonstration Case (questionnaires, system logs, list of topics for semi-structured interviews with stakeholders, topics to be covered in focus groups with stakeholders, observational protocols)





The Demonstration Case Template is provided in Appendix 4, and several examples of populated Demonstration Case Templates are reported in the following sections.

As a first general indication, data collection instruments for different phases and units of analysis in a Demonstration Case will include the following:

- Collection of data on Zero Scenarios through semi-structured interviews with stakeholders on their current practices in the defined Demonstration Scenario (before demonstration). A more detailed description of Zero Scenarios and several examples of Zero Scenarios collected from project partners in the preceding months are presented in Appendix 3– Zero Scenarios.
- Collection of quantitative data and indicators on the status of Demonstration Implementations at the beginning of the Demonstration Case
- Tools for quantitative data collection on user activities during the Demonstration Case. Part of this can be achieved through logging or otherwise recording user actions during the Demonstration Case, but this should be subject to close scrutiny from an ELSI perspective
- Tools for quantitative data collection on the status of the Demonstration Implementation after the Demonstration Case
- Tools for the collection of qualitative data on user-system interaction during the Demonstration Case. This will include unstructured or semi-structured interviews at different stages of the Demonstration Case, focus groups with stakeholders, journals kept by end-users and project members as well as participant observation (particularly if project members are to be involved as trainers, facilitators or coordinators in the Demonstration Case). Use of nontextual data (videos, screenshots, pictures of working environments, audio recordings) will also be considered when appropriate.
- Tools for the collection of qualitative information from end-users after the Demonstration Case through semi-structured interviews, questionnaires and focus groups. This part will be modelled on the SEQUOIA framework

A predefined structure for collecting and reporting results from Demonstration Cases will be defined as part of the Protocol. Results and reports from different Demonstration Cases will be collated in a Demonstration Case Database that will include, for example, system logs, transcripts or summaries of interviews, collected questionnaires, focus group reports, draft and final validation and evaluation reports¹². This is subject to the agreements detailed in the SecInCoRe Research Ethics Protocol and Code of Conduct

One important element to note with regard to the use of indicators is that there is a clear overlap between indicators identified according to SEQUOIA areas of impact, indicators related to validation modules and indicators (KPIs) related to project KPAs and sub-objectives. To this aim and to avoid the duplication of data collection efforts, quantitative and qualitative data regarding all required indicators will be collected before, during and after Demonstration Cases. The reporting practice developed in the Demonstration Case Protocol will specify that the collected indicators will be aggregated in different ways:

¹² D1.2 "Research Ethics (first version): Research Ethics Protocols, relevant authorisations and informed consent"





- According to KPAs, for assessing progress in relation to project objectives
- According to CIS Modules as identified in D4.2, for validation purposes
- According to SEQUOIA impact areas, for evaluation purposes

6.2 Draft plan for the first round of validation and evaluation

The methodology described in D5.3 is going to support and address all the demonstrations that will be performed in order to validate and evaluate the sociotechnical system that the project is currently developing. However, as highlighted at the first review meeting by reviewers, the scope of the project in relation to the first phase of validation and evaluation activities was redefined as enhancing collaboration, exchange and interoperability for preparedness and training activities. It remains that SecInCoRe serves every phase of the crisis management cycle.

Within the overall validation and evaluation strategy, different Demonstration Cases need to address multiple scales of action so that we can measure how the final project results achieve the project goals. In the end, there will be five Demonstration Cases covering different scenarios: (1) one EU, (2) one cross-border, (3, 4) two local, and (5) one organisational (Figure 22).

- (1) Collaboration/interoperability at the EU level. An example would be the refugee crisis. This can be filled out by mixing two things:
 - what kinds of challenges and needs were the impetus for the grant call in the first place; and
 - what sorts of collaborative interactions exist in the case studies that describe EU level governance.
- (2) A more detailed Demonstration Case for a cross-border collaboration to see both how such interactions require breaks from routines and to see how they build to a more EU-level style of interaction. An example would be collaboration between Dortmund and Lancaster around a planning for pandemic risks.
- (3,4) Two local Demonstration Cases to be able to understand the relationship of our system to current routines (such as flooding in Lancaster and refugee reception in Dortmund at present).
- (5) A Demonstration Case for collaboration within an organisation would be valuable to see if SecInCoRe could encourage new partnerships and interactions within a single organisation.







Figure 22. Demonstration Cases covering different scenarios

The organisation of dedicated Demonstration Cases will follow the implementation of the SecInCoRe concept and the work of analysis and understanding accomplished in all the WPs. Above all, the organisation of Demonstration Cases will be scheduled and discussed with stakeholders involved, not just with project partners. For all these reasons, the organisation of validation and evaluation activities will be a continuous process that has to take into account several factors that cannot be considered at the time of writing this document. Although it is not possible at this time to define in detail how and when the Demonstration Cases will be run, it is however possible to envisage a roadmap that reflects the current state of the work and the next phases that are actually planned.

We are eager to extend the validation activities dynamically either based on WP5driven demands or driven by external requests; a minimum set of activities is described below. First of all, a workshop based on a cross-border European is being organised together with stakeholders from two different countries, including members of the Lancashire Local Resilience Forum (LLRF) in the UK. This demonstration will be organised using a Demonstration Scenario based on the collaboration among different countries allowing users to interact with a Common Information Space. This point is crucial for the participation of the LLRF that will interact with a system consisting of different functions instead of the ones given by their current system (the Resilience Direct system). This use-case is foreseen in May (M24) as established in the timeline described in D5.2.

Even if it is not confirmed at the moment of the writing, a demonstration on the use of SecInCoRe in training and preparedness will be organised with the Dortmund Fire Brigade. According to the Demonstration Case Template reported below, the first




demonstration about a training exercise in planning will be organised in Dortmund approximately in May, the second case dealing with a real training exercise in planning is foreseen by August or September.

Finally, the demonstration use-case will be organised on the current refugee crisis and this is foreseen to be completed by M34 (as defined by D5.2). It is important to stress that further Demonstration Cases will be organised according to project needs.

6.3 Demonstration Case: Lancashire Local Resilience Forum

The first activity of validation to be conducted will be in collaboration with the Lancashire Local Resilience Forum and will be based on the preparedness phase of the emergency. In order to prepare the demonstration, the ULANC team has started to complete the template that will be used to organise activities giving also inputs for the demonstrator implementation. This template is in a draft form and will help to organise the activity.

Demonstr	ULANC 1			
ation				
Case ID:				
Demonstr	Co-Design Experimentat	tion		
ation				
Case				
Name:				
Created	Katrina Petersen	Last Updated	Katrina Petersen	
By:		By:		
Date	11 February 2016	Date Last	19 February 2016	
Created:		Updated:		

Demonstration Case Name: Co-Design Experimentation

Short description and main aims of the demonstration case

International scenario in which actors from different countries cooperate and exchange data to prepare for future crises.

Collaboratively with potential users experiment with the SecInCoRe system as designed in order to help, jointly, develop solutions to problems or questions we have already identified, highlight areas of value, and pinpoint areas that need more work. The aim is to have enough of a system (on paper and in software/technology) in order to see the system in action, to see the system being used for an activity the user would already have to do, such as develop new locally relevant plans.

The main aims are to explore how:

- gaps in knowledge are identified and needs for filling in are defined
- lessons learnt might be shared across national borders





- new sources of information or interactions begin to be collaborated with
- trust is built in new partners and relationships
- managing different ways of defining risk.

Emergency Phase(s) covered in the demonstration case

Planning/Preparedness P.2

Short description of the possible Scenario(s) identified for the demonstration case

Scenario ID	Name
1	A pandemic outbreak. Pandemics do not respect borders and, with increased travel, will spread rapidly. This means an outbreak in one place is a concern for all places, and for <i>all</i> emergency responders.
	Emergency responders will be affected by pandemics in various ways. For example, they may be involved in the direct planning and/or response to a pandemic and/or their personnel will likely also be affected (i.e. infections, having to stay home and look after ill family members, out of school children, fear of infection), which could compromise their ability to attend to other emergencies. While health professionals may be affected in both ways, police and firefighters may be affected more in the second case. Cascading consequences also severely reduce societies' capacity to run normal services, from banks to supermarkets. In the worst case scenario, a pandemic can lead to public panic and disorder. In this case, police and firefighters will be called upon to uphold the rule of law in a context where they may have severe staff limitations.
	The planning for and response to pandemics requires considerable data collection and sharing, some of which is sensitive data. This data also needs to be shared across a wide range of stakeholders, from small scale elderly care businesses, to diagnostic and treatment data across national borders and health institutes. Pandemics will also place considerable strain on Internet and communications technologies, as technological forms of communication (i.e. remote) will be relied upon heavily across society as a means to stay informed without having to come into face-to- face contact. People may even be asked to work from home during a pandemic. In such a scenario, cloud-based computing, which can stretch to accommodate raising demands, will be vital.
	Scenario 1 explores how pandemics are being planned for and how an outbreak would be dealt with in both Germany





It would also offer an opportunity to explore the different organisations which are involved in pandemic planning/response across the national contexts and allow emergency responders to learn from one another in regards to how they are conceptualising possible pandemic scenarios – e.g. what is a 'worst case scenario' in the UK may be conceptualised differently in Germany – and the steps they are taking to bolster society, but also themselves as responding organisations, during an actual pandemic outbreak.We currently have access to Dortmund Fire (DF) and Lancashire Local Resilience Forum (LLRF). DF has been involved in a German research project called GenoPlan regarding the workableness of Dortmund's city administration in case of a pandemic. Through DF we may be able to gain access to participants in other relevant organisations. LLRF, which is composed of diverse stakeholders across various different organisations, is also involved in local pandemic planning and, in the case of outbreak, response.2Sharing lessons across a border about flooding: for example, have a small team of planners in the UK and another small team in Germany working at the same time. On day 1, they each work in their respective groups to prepare lessons learnt about, for instance, flooding, and then day two they work at sharing it.3Planning for a new hazardous spill in Lancaster that has not been previously dealt with, but has potentially been planned for/mitigated/managed in Dortmund in a region with similar environmental and demographic contexts. Building this type of plan would bring together a range of stakeholders, public and private, environmental organisations, humanitarian organisations, businesses, and emergency responders.		and the UK. Each country has its own national pandemic plans/protocols. Exploring how different emergency responders within each country are preparing their communities and themselves for a pandemic outbreak – i.e. what their role is in planning/response within the community, as well as how they are preparing themselves as an organisation which will be affected by pandemic – would highlight unique organisational structures, different levels of involvement and concern with pandemics (i.e. different needs for data/information), and how these differences may influence the sharing of information and data during a pandemic outbreak.
 We currently have access to Dortmund Fire (DF) and Lancashire Local Resilience Forum (LLRF). DF has been involved in a German research project called GenoPlan regarding the workableness of Dortmund's city administration in case of a pandemic. Through DF we may be able to gain access to participants in other relevant organisations. LLRF, which is composed of diverse stakeholders across various different organisations, is also involved in local pandemic planning and, in the case of outbreak, response. Sharing lessons across a border about flooding: for example, have a small team of planners in the UK and another small team in Germany working at the same time. On day 1, they each work in their respective groups to prepare lessons learnt about, for instance, flooding, and then day two they work at sharing it. Planning for a new hazardous spill in Lancaster that has not been previously dealt with, but has potentially been planned for/mitigated/managed in Dortmund in a region with similar environmental and demographic contexts. Building this type of plan would bring together a range of stakeholders, public and private, environmental organisations, humanitarian organisations, businesses, and emergency responders. 		It would also offer an opportunity to explore the different organisations which are involved in pandemic planning/response across the national contexts and allow emergency responders to learn from one another in regards to how they are conceptualising possible pandemic scenarios – e.g. what is a 'worst case scenario' in the UK may be conceptualised differently in Germany – and the steps they are taking to bolster society, but also themselves as responding organisations, during an actual pandemic outbreak.
 Sharing lessons across a border about flooding: for example, have a small team of planners in the UK and another small team in Germany working at the same time. On day 1, they each work in their respective groups to prepare lessons learnt about, for instance, flooding, and then day two they work at sharing it. Planning for a new hazardous spill in Lancaster that has not been previously dealt with, but has potentially been planned for/mitigated/managed in Dortmund in a region with similar environmental and demographic contexts. Building this type of plan would bring together a range of stakeholders, public and private, environmental organisations, humanitarian organisations, businesses, and emergency responders. 		We currently have access to Dortmund Fire (DF) and Lancashire Local Resilience Forum (LLRF). DF has been involved in a German research project called GenoPlan regarding the workableness of Dortmund's city administration in case of a pandemic. Through DF we may be able to gain access to participants in other relevant organisations. LLRF, which is composed of diverse stakeholders across various different organisations, is also involved in local pandemic planning and, in the case of outbreak, response.
3 Planning for a new hazardous spill in Lancaster that has not been previously dealt with, but has potentially been planned for/mitigated/managed in Dortmund in a region with similar environmental and demographic contexts. Building this type of plan would bring together a range of stakeholders, public and private, environmental organisations, humanitarian organisations, businesses, and emergency responders.	2	Sharing lessons across a border about flooding: for example, have a small team of planners in the UK and another small team in Germany working at the same time. On day 1, they each work in their respective groups to prepare lessons learnt about, for instance, flooding, and then day two they work at sharing it.
	3	Planning for a new hazardous spill in Lancaster that has not been previously dealt with, but has potentially been planned for/mitigated/managed in Dortmund in a region with similar environmental and demographic contexts. Building this type of plan would bring together a range of stakeholders, public and private, environmental organisations, humanitarian organisations, businesses, and emergency responders.





SH ID	Name	Stakeholder Category Code		
1	Local Authority Emergency Planners	PU.M.1		
2	Information Manager	PU.M.4		
3	Local Resilience Forum Sub Group based on appropriate theme	- PU.M.5		
4	Health Services Planners	PU.HB.1		
5	Health Services Information Manager	PU.HB.4		
6	Social Services crisis management staff	PU.HB.6		
7	Police Operation Commande	er PU.PA.7		
8	Police Information Manager	PU.PA.3		
9	Fire Operation Commander	PU.ER.6		
10	Fire HazMat Advisor	PU.ER.7		
11	Resilience Direct Officer (UK	PU.ER.13		
12	LRF/JESIP training group	PU.ER.11		
13	Utilities Safety Managers	PU.Pu.5		
14	Utilities Security Managers	PU.PI.6		
15	Environmental agency scientists			
16	Meteorological office scientists			
17	Chemical company risk managers			
18	Humanitarian Groups	PV.CS4		
19	Public information officer			
Contact	details for stakeholders involv	ed in the Demonstration Case		
SH ID	Contact person(s)	Contact details		
1				
Do (som	e or all) stakeholders belong t	o larger organizations / consortia?		
Name a	and contact details	IDs of the stakeholders that are members of the organization / consortium		
Lancas	hire Resilience Forum			





	Dortmun	nd Fire	
	Stakehold	ders description	
	SH ID	Description	
	1		
	Preparatio	on of the Demonstration Case	
	Please de Demonstr stakehold or planne	escribe all the activities that have taken place until now to prepare the ration Case, including your previous interactions / consultations with ders and any other preparatory activities that have already been executed ed.	ł
	 Intr res inte 	roductory interactions with Lancashire LRF, including presentation about search intentions, project goals, and desires for eractions/collaborations.	
	 Ob LR Est 	oserved an exercise to test plans for a city-bound chemical plant that the RF requires to be revisited every three years.	
	• Set	etting up visit to local Coast Guard Operations Centre.	
	 Inv at I 	viting key LLRF members to a loss of electricity due to flooding workshop Lancaster University	1
	• En	ngaging with Lancaster civil authority member of the LRF in an advisory pacity	
	 Set tes 	etting up meeting to explore Lessons Direct, a lessons-learnt system in st mode in the UK.	
	Co to b	oordinating with TUDO/UPB to figure out an issue that would be of benefi both set of stakeholders we have to work with.	t
	Expectation	ons and assumptions concerning Stakeholders' needs and involvement	
	On the ba	asis of your previous consultations with Stakeholders, please describe:	
	(a) the n Demonstr	major incentives and obstacles for Stakeholders to participate in th ration Case:	е
	The incen being said	ntives and obstacles will depend on the demonstration case chosen. Tha d, here are a few general thoughts:	at
•	they are work in pr would be	e using a similar system that is UK wide and while it is popular it is still rogress. Being able to learn from this process is as valuable to them as for us	a it
	they stil involved a to be aski on a pool	Il struggle to determine how to define things such as: who should b and to what extent, who qualifies as "vulnerable people", what question ing to help define the extent of the risk and for who. Having a way to dra- of knowledge to help this would be of value to them.	e s w
.	as we p an obstac	plan to bring people in the UK and Germany together, language could b cle. However, this is a very real obstacle which would impede workin	e g





together in an emergency and, thus, exploring it in a mock exercise is highly instructive.

(b) how you think they will contribute to the Demonstration Case in terms of sharing their data, activities, expertise, practices

--the LLRF is about developing trust in multi-agency work, and the Lancashire group already does regular collaborative work. Seeing what they do in order to work successfully together can provide a framework for practices to design our system around.

--they have given us access to Resilience Direct, which means we can start to see how we might be able to connect to already existing national information systems.

--RD is intended to have a collaborative/CIS style aspect that is more than just a place for everyone to reference the same documents, but these features are underdeveloped still.

--Dortmund Fire has already worked on a German project called GenoPlan, which aims to ensure that the Dortmund administration can continue to function in the event of a pandemic. Dortmund Fire would bring its expertise from this crossagency/organisation project.

(c) which assumptions regarding Stakeholders' participation and involvement need to be fulfilled for the Demonstration Case to achieve its aims

--it needs to force them to do something that cannot be solved by using Resilience Direct or working with their normal more local or neighbouring contacts.

--it needs to provide them with useful techniques, practices, tools, or relationships for further growth in their own routines. This can be from understanding how and when and with who to share lessons learned, better understanding what kind of data or forms needs to be automated, understanding better how to define risks or affected populations, to learning new organisations/contacts with which they can exchange valuable information.

(d) how you intend to cope with possible defections or difficulties.

TBD.

Preliminary definition of use cases associated with the Demonstration Case

Please describe (in as much detail as possible given the current definition of the Demonstration Case) the Use Cases that are potentially associated with this Demonstration Case and one or more of the proposed embedded Scenarios

Reference Implementations that will be needed for the Demonstration Case

Please provide details of the Reference Implementations that you expect will be used in the Demonstration Case

Demonstration Implementations

Given the overall aims of the Demonstration Case, the current knowledge of stakeholders' needs and expectations and the current status of Reference Implementations, please explain what you think is needed to develop Demonstrator Implementation(s) that can be used for this Demonstration Case





--a way for our knowledge base to interface with existing databases. We cannot expect everything to be imputed.

--a partially functioning CIS. This is where our greatest value will be for this demonstration as it is something that is underdeveloped in the RD.

--an interface that shows the ELSI connection to the search results/CIS interactions, not just references ELSI guidelines as a separate document to go visit.

Inventory and Semantic Models

Starting from the current status of the Knowledge Base, please describe which elements of the Inventory (specifically, the available data sources and semantic models) will be used for this Demonstration Case. Comment on the adequacy of the KB for the aims of the Demonstration Case, and please indicate any additional data sources that you expect to be able to integrate in the Knowledge Base before stakeholders start interacting with Demonstrator Implementation(s) in this Demonstration Case.

--Inventory case studies:

- The 2009 H1N1 pandemic
- Chemical Spills

--Crisis management models:

- Risk Assessments environmental, chemical, civil
- Collaboration plans/MOUs (Memorandum of Understanding)
- Incident command procedures

--Information Systems:

TBD

--Data-Sets:

Uncertain what kind of data we will be given access to in advance, while some of this should be known prior to workshop, a certain level of uncertainty is advantageous for exploring ad-hoc interoperability practices.

Tentative timeframe for the Demonstration Case

Please provide details about the possible timeframe for the Demonstration Case (including any preparatory or co-design activities) and about the expected duration of the Demonstration Case.

Day 1: 14:00 – 17:30 – Co-Design Workshop with Lancashire Resilience Forum + Advisory Board

Day 2: 09:00 – 13:00 – Continuation of Co–Design Workshop

Day 2: 14:00 – 17:30 – SecInCoRe Plenary Meeting and debriefing





Comments from the	validation / evaluation team
GENERAL COMME	NTS:
VALIDATION / EVA	LUATION MODULES
Terminology	
Stakeholders	
Collab Practices	
And ELSI	
Taxonomy	
ConOps for CEIS	
HLRD	
Modular System	
Architecture	
NEC concept	
Semantic Framework	
Knowledge Base	
Ĵ	
Comments from the	Demonstration Implementation team
Additional comment	s from other Project Partners

6.4 Demonstration Case: Dortmund exercise

Based on the overall CIS demonstrator several sub-sequences of demonstration implementation will be defined with regard to the respective case.

The Fehler! Verweisquelle konnte nicht gefunden werden. (Fehler! Verweisquelle konnte nicht gefunden werden.) illustrates a setup, an assortment of reference implementations for a demonstration implementation and the dedicated demonstration cases. The demonstration case is divided in two scenarios which will take place at different locations but simultaneously. The first scenario deals with a simulated training exercise planning in a structured workshop. The second one dealing with a real training exercise planning.

Demonstr	2
ation	





Case ID:							
Demonstr	Preparation for	Preparation for training exercise in Dortmund					
ation							
Case							
Name:							
Created	Christina	Schäfer,	Last	Updated	Christina	Schäfer,	Torben
By:	Torben Sauer	land	By:	-	Sauerland		
Date	10/02/2016		Date	Last	19/02/2016		
Created:			Update	ed:			
Demonstra	Demonstration Case Name: Preparation for training exercise in Dortmund						

Short description and main aims of the demonstration case

Training is a major issue for Fire Brigades in Germany to be prepared in case of an incident. Identifying sufficient scenarios, possible flows of the scenario with relevant events having an impact on the exercise, and therefore on activities in the response of an incident. This is a task, which may be supported with the SecInCoRe demonstrator implementation. Hence, this case and demonstrator aims to assist respective officers in the preparation of training exercise. The overall demonstration case is split up in two escalation levels. First a structured workshop, to identify first impression in the use for planning a training exercise and further real operation to gather long-term experiences.

The overall goal is to achieve based on the described evaluation methodology formative evaluation of various IT components included in the Demonstrator Implementation. In general, an evaluation of the whole CIS concept would be favoured.

Concrete Questions in the evaluation for this case:

1. needed information in the metadata of the search results

2. functionalities for enabling collaboration and information sharing

3. lacks to support tasks in the context of a CIS

4. using the prototyping method in the domain of PPRD and consequences for the method

Emergency Phase(s) covered in the demonstration case

P.2

Short description of the possible Scenario(s) identified for the demonstration case

Scenario ID	Name	
1	Planning for a simulated training exercise and possible setups (short-term demonstration case)	-
2	Planning for a real training exercise and possible setups (long-term demonstration case)	





List of stakeholders involved in the Demonstration Case				
SH ID	Name		Stakeholder Category Code	
1	Fire Brigade Dortmund		PU.ER.11	
Contact	details for stakeholders involv	/ed	I in the Demonstration Case	
SH ID	Contact person(s)		Contact details	
1	Detlev Harries		Detlev Harries <dharries@stadtdo.de></dharries@stadtdo.de>	
Do (som	e or all) stakeholders belong	to I	larger organisations / consortia?	
Name a	and contact details	IC of	Ds of the stakeholders that are members f the organisation / consortium	
Stakeho	Iders description			
SH ID	Description			
1	The fire brigade Dortmund firefighting and ambulance	d c un	consists of voluntary and professional its. It has about 1800 members.	
Preparation of the Demonstration Case				
The Demonstration Case is settled in a big fire brigade in Dortmund – Germany (see picture below).				
Demonstrator Implementation				
	Pre-Scenario During-Scenario	Po: Civ	ist-Scenario vil Society ion of Use Case	





The overall demonstration case is twofold: First, the Fire Brigade prepares an imaginary big training exercise. The planning is done by a few staff members of the fire brigade maybe with help and hints from members of other organisations. The training exercise will cover a topic which helps to improve the skills of tactic and operative staff. It will involve several different units (firefighters, ambulances, police and other - e.g. municipal – units). The SecInCoRe demonstrator implementations could help the planning staff in several ways to prepare the training exercise. Details below. Further demonstrator implementations are placed in the fire brigade over a wider timeframe to enable the support of the preparation of a real training exercise, using their own workflows (scenario 2).

Expectations and assumptions concerning Stakeholders' needs and involvement

Scenario 1: The fire brigade Dortmund is quite big and has its own research facilities. A long cooperation between the C.I.K. and them leads to a strong relationship. The fire brigade is keen to test our project results and to help us, improving them. The main obstacle is missing time caused by the current refugee crisis. For example, the fire brigade is not performing big training exercises at the moment, because of the stress, helping the refugees. Nevertheless, they will probably share non-confidential data with us and participate in one or two days of workshops with a few persons. To fulfil the aims of the demonstration case, they have to share some information with us and participate in at least one workshop day. If they are not able to participate at all, we have to find one or two different fire brigades to execute the Demonstration Cases (see figure Itinerary for demonstration cases).

Scenario 2: The initial situation is quite similar to scenario 1. The main difference is, that the fire brigade doesn't need to attend a workshop, but has to have a real training exercise to plan. They have to use the system for this task and find useful information for that.







Preliminary definition of use cases associated with the Demonstration Case

All Use Cases involve the fire brigade Dortmund.

Scenario 1:

• UC1 – Find inspiration for a topic

Applications: PAST DISASTER DB, SHARE INFORMATION Every training exercise planner in every city has to think about practicable and useful topics for the training exercises.

The planning staff could use the past disaster database to get input about different past disasters. They could use the underlying scenarios, the description of the course and the mentioned problems, to define their own training exercise. To reach this goals, the following action flow is planned:

- The user opens the SecInCoRe GUI.
- He navigates to the past disaster database.
- He scrolls down the past disasters.
- He finds an interesting disaster. He opens the disaster. He finds the description of the disaster and metadata he could use.
- He finds contact details of a person who has more information about the past disaster. He contacts this person within the SecInCoRe "Networking" application.
- The person shares more useful documents with the user via the SecInCoRe "Share information" application. The person asks for other information, the user has (e.g. special)

UC2 – Find information about planning a training exercise

Applications: SEARCH

There are different information needs, when planning a training exercise in a fire brigade.

- A) How to plan the training exercise
- B) How to execute the training exercise
- C) How to evaluate the training exercise

To find relevant information for all these steps, the SecInCoRe search could be used. To reach this goals, the following action flow is planned:

- The user opens the SecInCoRe GUI.
- He navigates to the search.
- He searches for relevant information to one of the information needs.
- He gets a relevant result document. He opens the document. He uses the information found.
- He navigates back to the search results, refines his search using the filters





and finds other interesting documents.

• He saves a document to his local computer.

• UC3 – Connect to planning staff of other organizations Applications: SEARCH =>PEOPLE

When the search is performed, the contact to authors of the found documents could be appreciated. To reach this goal, the following action flow is planned:

- The user searches for documents (See UC2).
- The user finds a relevant document. The user finds attached author information.
- The user contacts the author of the document.
- They swap information about the contents of the document. Each of them get useful hints for the preparation of training exercises or general issues.

• UC4 – Share own information with the community Applications: UPLOAD

The planning staff get an incentive to upload data into the SecInCoRe system. (Could be the intrinsic motivation, when they understand the usefulness of the system or some features in the system, which honourees the upload.) Once the user is motivated, the following action flow is planned:

- The user thinks about relevant documents, which are not confidential.
- The user opens the SecInCoRe GUI.
- The user navigates to the upload section.
- He uploads some documents.
- He gets positive feedback from within the application.
- UC5 Find information about useful software concerning training exercises Applications: INFORMATION SYSTEM DB

If the planning staff explores the SecInCoRe GUI, the information system database could attract his attention. He thinks about the used software in his organization and wants to get some ideas of other/possible better information systems. To reach this goal, the following action flow is planned:

- The user opens the SecInCoRe GUI.
- The user navigates to the information system database.
- The user takes a look at the contained information systems and the information provided.
- The user finds an interesting information system.
- He visits the website of the system to get more details.
- UC6 Find information about SecInCoRe





Applications: OPEN ATRIUM, HOW TO When the planning staff is familiar with SecInCoRe, more detailed information about the project could be appreciated. To get this information, the following action flow is planned:

- The user needs explanation concerning the applications.
- The user opens the SecInCoRe GUI. He navigates to the How To page.
- He reads about the different applications, the connection between them and the SecInCoRe project.
- He navigates to the Open Atrium page.
- The user explores the SecInCoRe concepts in Open Atrium.
- The user wants to get in touch with the project consortium.
- The user contacts the consortium.

Scenario 2:

All Use cases are possible for the second scenario. While planning a real training exercise order and characteristic of the use cases may change depending on the real situation.

Reference Implementations that will be needed for the Demonstration Case

Open Semantic Framework

In a first step, a very basic search system was installed based on Open Semantic Search, also presented in D3.3.

After a detailed analysis, Open Semantic Framework (OSF) was identified as the best fitting base for the search system. This system should enable an easy and domaincustomised way to find the needed domain specific data. At the moment the system has the possibility to trawl file systems, analyse the files found with an uploaded ontology and make them searchable. The search offers only basic functionalities now, but will be improved within the next few months. Particularly, no database connection is established yet and the semantic tagging is performed with a single ontology. Later on, ontologies from within the SecInCoRe project, from the SMW and from external domain ontologies should be integrated. The ontology data is used to tag the indexed files with corresponding concepts of the ontologies and to filter the search results. Further functionalities will be developed.

Knowledge Base

The Knowledge Base is the implementation of the inventory artefacts and in this way the inventory builds the basis of the Knowledge Base. Therefore, the inventory follows two lines: first a comprehensive analysis of information systems, business models, processes and data sets was started. Further to ensure a sustainable usage of the





system existing databases, glossaries and ontologies will be integrated and added to the inventory content. The Inventory contains at the moment two SecInCoRe-owned databases: An overview of past disasters is stored in the Past Disaster Database and a second database contains domain relevant information systems. The work on the overview of European processes and corresponding documents is ongoing.

Semantic Media Wiki

The Semantic Media Wiki (SMW) is based on the Media Wiki software. It enables the semantic storage of all contents and the underlying structure of the wiki. The recent implemented version is a very early instance of the Semantic Media Wiki with no additional features. The plan is, to create a concept for the SMW, which enables a simple and intuitive way for collaborative content editing. The structure of the community generated domain specific content should be used as an ontology for the search in OSF. For the community-based ontology a collaborative semantic platform is planned.

Foreign Systems

The CEIS concept aims to improve the communication and the access to information in the domain. There are several systems already at the market, which could be used to reach these aims. Therefore, the above-mentioned implementations are complemented by external systems. For example, the communication and group creation within the domain members can be established using existing chat or social applications.

Demonstration Implementations

Dortmund demonstration case "Training exercise planning"

Based on the overall CIS demonstrator several subsequences of demonstration implementation will be defined with regard to the respective case.

The demonstration case is divided in two scenarios which will focus on similar topics. The first scenario will be about the planning for a simulated training exercise of the fire brigade Dortmund. The second scenario will focus on the planning of a real training exercise in the same fire brigade. The second scenario will build open the lessons learned and maybe the inserted data from the first scenario.

Open semantic framework (OSF)

Especially regarding the search OSF, added content considering planning and conducting of exercises for fire brigades was required. The inventory (including all tasks T3.1, T3.2, T3.3) focus on these aspects and provide relevant information.

A first version of the search functionality was described in D3.3 as the mechanism to publish and retrieve information based on the inventory content and is extended to fulfil the requirements of the demonstration case.





Past-Disaster Databas	e (PD-DB)	
An important task in th scenarios. Therefore, th demonstrator implement	e definition of training exercises are the PD-DB is a valuable source of inform tation "Training Exercise in Germany".	ne definition of realistic nation and added to the
Home » fire		
Filter by structural engineering:	SecInCoRe	Filter by dataset: • True (3)
	fire	Bilter by human
Filter by fire brigade:	Search	resources (employees):
• true (1)	The search found 3 results in 0.502 seconds.	• true (1)
	Search results	
Filter by deaths:	2005 - Buncefield Oil Depot Explosion and Fire, UK.pdf	Filter by country:
• true (1)	2010 - Love Parade Stampede, Germany (UPB).pdf	• true (1)
	SecInCoRe OSF GUI	

Foreign Systems - Information Sharing (IS) and Networking (N)

For integrating the functionality of sharing information, the SecInCoRe project used existing technologies to 1) support user with already known applications and 2) to focus not on the implementation of existing technologies but to integrate them in the context of CIS. Therefore, ownCloud and LinkedIn was chosen to map the requirements regarding networking and sharing of information between first responder.

Inventory and Semantic Models

The knowledge base has to be extended to provide sufficient data regarding training, and methods for training exercises and possible scenarios. Tasks T3.1-T3.4 will support the work for defining needed information.

Tentative timeframe for the Demonstration Case

The case begins with a one-day opening workshop. A first semi-structured questionnaire will collect previous experiences of the participants and general problems in the field of preparing a training exercise, existing gaps in information sharing practices. After the introduction of the CIS, the demonstration implementations and the use of it, the participants can test and use the system independently for about four weeks. In this time frame all searches are logged and the participants should give direct feedback about the implementation and use via integrated feedback functionality. At the end of the free testing period, a final workshop is planned, which





enables direct feedback and a detailed analysis of the implementation.

Scenario 1:

About 1-2 days:

- First an introduction about the respective demonstrator and the overall goal
- Timeframe to use the demonstrator in a dedicated order, with respective tasks
- Dedicate short workshop in the end to gather feedback and evaluate the case

Scenario 2:

About 1 month:

- First an introduction about the respective demonstrator and the overall goal
- Timeframe about 1 month for using the demonstrator for the mentioned purpose
- Dedicate workshop in the end to gather feedback and evaluate the case

Comments from the validation / evaluation team

GENERAL COMMENTS:

VALIDATION / EVALUATION MODULES

Terminology			
Stakeholders			
Collab Practices			
And ELSI			
Taxonomy	X		
ConOps for CEIS			
HLRD			
Modular System Architecture			
NEC concept			
Semantic Framework	X		
Knowledge Base	X		
Comments from the Demonstration Implementation team			

Scenario 1:

A first version of the demonstrator implementation for this case has to be available. At





least the above mentioned applications have to work in a way, that the user interaction is possible as described in the use cases. After that, the fire brigade has to have time to participate with planning staff on the workshop.

Scenario 2:

A version of the demonstrator has to be available, which offers a stable and unmonitored use of the implementations by the stakeholders. After that, relevant information have to be available and the fire brigade has to have a suitable real training exercise in July or August.

Comments from the ELSI team

Additional comments from other Project Partners

6.5 Demonstration Case: refugee crisis

Another option in order to run an activity of validation is to work on an international scenario where international agencies are involved in the management of the flow of refugees. This scenario would be particularly relevant for the period in which the project is working. The template provided by KEMEA will see further changes but provides a sense of preparations of this activity.

Demonstrati	10177		
on Case ID:			
Demonstrati	Refugee Crisis		
on Case			
Name:			
Created By:	Center for Security	Last Updated	
	Studies - KEMEA	By:	
Date	15/02/2016	Date Last	
Created:		Updated:	
_	• ·· • • •		

Demonstration Case Name: Refugee Crisis

Short description and main aims of the demonstration case

International scenario where national and international authorities and agencies are involved in the management procedure of the flow of refugees. The goal of this demonstration case is to emphasize the evolving of the international phenomenon of the refugee crisis, where the collaborative efforts of multinational agencies (now not only European) are essential for the management of a growing problem as has turned for the EU. The current situation regarding the refugee crisis can be described briefly here. In 2015 more than 1 million refugees crossed the Mediterranean Sea and the



D5.3 Validation Strategy, Version 2 (ic) **Public deliverable**



Aegean Sea due to the events in Syria and Middle East, in order to enter the EU mainly from Greece and Italy. Of these refugees nearly 940.000 applied for asylum (BBC.com, 2016), and the number is expected to grow considerably for the year of 2016. Hotspots are the EU approach to record and distinguish migrants from refugees; detailed analysis of the description of the Hotspots has been carried out by KEMEA in D2.4 and D3.3 of SecInCoRe. The recording process of third-country nationals is complicated, and a lot of information needs to be processed. Initially, the refugees are offered psychosocial support in case it's necessary, and they are provided with the basic needs such as water, food and clothing. In the next step, the registration and identification process starts and Law Enforcement Agents (LEAs) from the Hellenic Police, with the help of translators of FRONTEX and NGOs. The data recorded at this stage are: A) Name, B) Nationality and C) Birth Date. Moreover, if the third-country nationals have some other documents (e.g. passport, Degrees, etc.), these are also recorded in a national database, administrated by the Hellenic Police in a closed national network, using a national application; the data is shared upon request by agencies such as Europol / Interpol or other agencies, in accordance with the degree of sensitivity of the data as it may be for example medical data etc. In the next step, Photos and Fingerprints of the third-country nationals are recorded and stored in the national database. The information is cross checked with EURODAC to see whether the third-country national has re-entered the EU from another country. Apart from EURODAC, the information is cross checked with the Schengen Information System (SIS) and Visa Information System (VIS) to find out if the third-country national is considered to be wanted from other Countries. In case there is no conflict in the previous step, the national application sends the A) Fingerprint data, B) Member state of Origin, C) sex, D) reference number used by the Member states, E) Date on which the fingerprints were taken, F) Date on which the data were transmitted to the Central system, G) operator user ID, H) dates on which is related with the arrival, departure, asylum application date, etc. At this point, a medical record is created for the thirdcountry nationals and medical examinations are performed. Finally, the third-country nationals are guided to a debriefing regarding the legislation applicable for refugees, where they are informed of their rights and responsibilities.

Emergency Phase(s) covered in the demonstration case

The emergency phases in this demonstration case are multiple and with different characteristics, due to the nature of the crisis which commences with:

- the human lives (rescuing the refugees),
- the entrance of unknown people in the EU,
- the management of emergency health issues as identified on the spot and the medical treatment (hypothermia, diseases, wounds, pregnant women etc.),
- the treatment of vulnerable categories of refugees (children, pregnant women, handicap people etc.),





- identification and registration of the refugees / migrants (in limited local facilities that is impossible to deal with the thousands of people that arrive every day),
- separation of refugees and migrants for further asylum applications,
- facilitation and housing of the refugees,
- transportation and relocation of the refugees.

Short description of the possible Scenario(s) identified for the demonstration case

Scenar	io ID	Name		
1 A number of refugees have been located at sea and selected by the Hellenic Coast Guard vessel; they brought at land and the authorities must decide who be to the vulnerable categories in order to take care of the urgent need of medical care, and lead the others to defined procedure for registration and identification.		ees have been located at sea and are ellenic Coast Guard vessel; they are the authorities must decide who belong tegories in order to take care of those in dical care, and lead the others to the or registration and identification.		
2 During registration and identification, certain people are identified as not fitting the profile of the refugee, hence mus be separated by the other refugees and initiate the process of sending back to their country or to Turkey through the bi lateral agreement signed between EU and Turkey. This involves the collaboration between the authorities operating on the Hellenic premises (hence, EU) and the Turkisk counterparts.		and identification, certain people are ng the profile of the refugee, hence must other refugees and initiate the process heir country or to Turkey through the bi- signed between EU and Turkey. This ration between the authorities operating emises (hence, EU) and the Turkish		
3 False identification is recognised through the SIS system hence actions of criminal law are initiated by the Helleni authorities (police) for the detention of the holder of the fak identification document. It must be emphasised that ther are different cases of false documents: they may be actuall false, or they may be real but stolen. In the second case unless the document has been reported as stolen, it is ver		is recognised through the SIS system iminal law are initiated by the Hellenic or the detention of the holder of the fake ent. It must be emphasised that there of false documents: they may be actually be real but stolen. In the second case, it has been reported as stolen, it is very		
		Furthermore, an individual may be recognised as a person with criminal record (could be even wanted) when the fingerprints are recorded (Eurodac); this is an information that will be available through databases such as Europol / Interpol.		
List of stakeholders involved in the Demonstration Case				
SH ID	Name		Stakeholder Category Code	



D5.3 Validation Strategy, Version 2 (ic) **Public deliverable**



1	Hellenic Police			
2	FRONTEX			
3	Hellenic Coast Guard			
4	First Reception Servic (F.R.S.) (Hellenic Ministry Interior)	ce of		
5	Europol			
6	European Asylum Suppo Office (EASO)	prt		
7	Eurojust			
8	Office of the United Nation High Commissioner for Refugees (UNHCR) Greece	ns or in		
9	Local/regional Health Center	er		
10	Local council authorities			
11	NGOs			
Contact	details for stakeholders involv	ved in the Demonstration Case		
SH ID	Contact person(s)	Contact details		
1				
Do (some or all) stakeholders belong to larger organisations / consortia?				
Name and contact details		IDs of the stakeholders that are members of the organisation / consortium		
Hellenic Police		Ministry of Interior and Administrative Reconstruction		
Hellenic Coast Guard		Ministry of Shipping and Island Policy		
FRONTEX		DG MIGRATION AND HOME AFFAIRS		
F.R.S.		Ministry of Interior and Administrative Reconstruction/ Ministry of Citizen		



D5.3 Validation Strategy, Version 2 (ic) **Public deliverable**



		Protection	
EUROPOL		DG MIGRATION AND HOME AFFAIRS	
EASO		DG MIGRATION AND HOME AFFAIRS	
EUROJ	JST	DG MIGRATION AND HOME AFFAIRS	
UNHCR		United Nations	
Stakehole	ders description		
SH ID	Description		
1	The Hellenic Police is rest borders and deliver them registration of the respective	sponsible for detecting immigrants in land to the F.R.S. Also is responsible for the re data into EURODAC system.	
2	FRONTEX is supporting the National Authorities in the detection and SaR missions, during the Registration and Identification of the immigrants, in the Debriefing and risk analysis of the individuals and assists the national authorities to return the immigrants who are not eligible for international asylum.		
3	The Hellenic Coast Guard is responsible for detecting immigrants in sea level and deliver them to the F.R.S. Furthermore, is responsible in managing and executing SaR missions in collaboration with FRONTEX personnel.		
4	F.R.S. is responsible for the residence, recording of their data, immediate provision of their health needs and to inform all immigrants for their legal rights and the relevant procedures according to National law.		
5	EUROPOL assists FRONTEX during the Risk analysis process and also is supporting national authorities to investigate all individuals for possible facilitation/being part of criminal networks. Furthermore, both aforementioned organisations assist national authorities to identify, register and fingerprint alongside with EASO and Eurojust.		
6	EASO personnel in addition identification registration are asylum application procedu	on to the assistants provided during the nd fingerprinting phases also supports the ures.	
7	EUROJUST will assist the trafficking networks.	roughout the investigations to dismantle	





8	UNHCR	
9	Local/regional Health Center or Hospital personnel will offer medical attention to immigrants, it will also record the "first personal details and it will create a medical file for each individual.	
10	Local council authorities will support F.R.S. with the catering/feeding and clothing of the immigrants.	
11 NGOs are supporting F.R.S., the local Health Centers/Hospitals in providing medical services in immigrants in need and in the clothing and catering.		
Preparati	on of the Demonstration Case	

The demonstration case has been researched and designed by KEMEA in collaboration with the respective authorities and ministries, where information is gathered and analysed to fit the purpose of the demonstration scenario, with great effort to the simplification of the procedures and details that are continuously evolving, as it is a phenomenon that is under progress. The access to personnel and information is particularly difficult primarily due to the extreme conditions and timeframes that the personnel must operate and the expansion and advancement of the data and the procedures. The timeframe required for the preparation of this demonstration case has been 2 full months of interaction with the aforementioned authorities and agencies, updating the data and procedures along.

Expectations and assumptions concerning Stakeholders' needs and involvement

The major incentive for stakeholders to be involved in the demonstration case has been the idea of preparedness both in terms of procedures, the technologies, the interaction with other agencies involved during the management of such situations as these described earlier. It would serve as a good platform for training, or even exploring new concepts and identifying gaps, as the experience of the different stakeholders is more valuable than any theoretical prediction.

As mentioned earlier too, an expected difficulty to have the stakeholders participate would be due to their very heavy schedule, as the refugee crisis situation is in progress and the capacity of the personnel of the different agencies is limited. The only way to handle such issues of availability, would be to organise their participation (in either procedure suggested above) well in advance, in a central location accessible to all.

Preliminary definition of use cases associated with the Demonstration Case

D3.3 and D2.4 Hotspots

Reference Implementations that will be needed for the Demonstration Case





D3.3 and D2.4 Hotspots

Demonstration Implementations

The main idea is to develop a system that will promote the training of the stakeholders for preparedness but also the interaction and exchange of ideas that will be surface during the training. It has to be a system that will be user friendly and assist them in their daily tasks, and it is important to have their feedback to gather data such as that; this would be a great exercise for us too to refine and optimise the system. Given the issues that were aforementioned in this document, it is essential that system functionalities will assist their operation in any of the emergency phases, highlighting the problem that they may encounter during these phases.

Inventory and Semantic Models

Starting from the current status of the Knowledge Base, please describe which elements of the Inventory (specifically, the available data sources and semantic models) will be used for this Demonstration Case. Comment on the adequacy of the KB for the aims of the Demonstration Case, and please indicate any additional data sources that you expect to be able to integrate in the Knowledge Base before stakeholders start interacting with Demonstrator Implementation(s) in this Demonstration Case.

Tentative timeframe for the Demonstration Case

If end-users were to participate and test the demonstration case and the system, it would be fair to say that about 1 month would be necessary if we try to involve them separately because there are different kind of stakeholders involved. Furthermore, I would recommend as an alternative to have an event like a small workshop with representatives from the local authorities who participate to the procedures in a refugee crisis management; this may require good planning as most of the people involved are rather busy, hence we will need to organise this well in advance. In the case of the workshop, 2 days would be sufficient, as we will need to introduce them to the system during the first day, and then have the second day dedicated to the demonstration scenario.

Comments from the validation / evaluation team

GENERAL COMMENTS:

VALIDATION / EVALUATION MODULES

Terminology

Stakeholders





Collab Practices	
And ELSI	
Taxonomy	
ConOps for CEIS	
HLRD	
Modular System Architecture	
NEC concept	
Semantic Framework	
Knowledge Base	
Comments from the	ELSI team
Comments from the	Demonstration Implementation team

Additional comments from other Project Partners





7 Conclusion

In conclusion, the contribution of this Deliverable is the setting of the final validation and evaluation strategy adopted by SecInCoRe. Starting from the work done in D5.2, the definition of the methodology has followed the project development as well as the project's needs.

The deliverable provides a clarification of the methodology according to the triangulation between the E-OCVM performance framework (which includes KPAs and KPIs) and the SEQUOIA evaluation approach.

Doing so, this deliverable allows to trace the main actions that will follow in the next months through a process of validation and evaluation based on Multiple Demonstration Cases.

One of the major results of the document has been the building of a comprehensive strategy taking together the work done in all WPs. For this reason, the identification of Demonstration Cases and related indicators are linked to High-Level Requirements collected in the live JIRA system (WP4) and are fundamental for the next phase of validation and evaluation (WP5).

In order to run Demonstration Cases, the tools and procedures here stored will be further developed and used to organise, prepare and coordinate Demonstration Cases. Moreover, the three Demonstration Case Descriptions already collected for the preparatory phase of different Demonstration Cases are possible candidates for the next run of validation and evaluation activities that will be conducted in the following months.





8 Literature index

- Ebrahim, A.S., Rangan, V.K., (2010). The limits of non-profit impact: a contingency framework for measuring social performance, Harvard Business School General Management Unit Working Paper n. 10-099 retrieved from http://www.hbs.edu/faculty/Publication%20Files/10-099.pdf
- Eurocontrol. 2010. European Operational Concept Validation Methodology Version 3.9. Volume I
- German Regulation DV 100. 2007. Leadership and Command in Emergency Operation. Command and control System.
- Passani A., Bellini F., Spagnoli F., Ioannidis G., Satolli L., Debicki M., Crombie D., (2014) MAXICULTURE Deliverable 2.3 – Socio-economic impact assessment methodology (V3.0 - revision 2)
- Passani, A., Monacciani, F., Van Der Graaf, S., Spagnoli, F., Bellini, F., Debicki, M., & Dini, P. (2014). SEQUOIA: A methodology for the socio-economic impact assessment of Software-as-a-Service and Internet of Services research projects. *Research Evaluation*, 23(2), 133-149.
- Passani, Antonella and Monacciani, Fabiana and Van der Graaf, Shenja and Spagnoli, Francesca and Bellini, Francesco and Debicki, Marie and Dini, Paolo (2012) Sequoia: a methodology for the socio-economic impact assessment of software-asa-service and internet of services research projects. Research evaluation. ISSN 0958-2029 (Submitted)
- Yin, R. K. (2003). Case study research, design and methods, 3rd ed. Newbury Park: Sage Publications. ISBN 0-7619-2553-8





9 Annexes

The annexes will contain

- Appendix 1: list of Sequoia indicators
- Appendix 2: JIRA requirements and possible indicators
- Appendix 3: first collection of zero scenarios
- Appendix 4: Demonstration Case Template
- Appendix 5: SecInCoRe OpenAtrium User Manual
- Appendix 6: questionnaires and focus group guidelines mentioned in the text of the Deliverable





9.1 Appendix 1: list of Sequoia indicators

The Sequoia methodology has been applied to SecInCoRe project allowing to map the main areas of impact and to tailor related indicators to estimate the socio-economic impact of SecInCoRe.

Economic Impact

Financial impact

- Investment cost (total cost of implementation)
- Cost of adaptation of SecInCoRe to existing systems
- Working time to adapt SecInCoRe to an existing tool
- Need of hardware/software to implement SecInCoRe and its cost (Does SecInCoRe need hardware/software to be implement?)

Technological impact

Operational efficiency

- Time to access to the information
- Time to get in the systems
- Presence of a how to guide and assessment of the tool
- Time to upload an information
- Time to retrieve an information
- Number of clicks to reach key information for everyday work
- Time to set up tailored CIS demonstrator
- Assess the level of interoperability among different systems

Accessibility

- Usability. The extent to which information is clear and easily used
- Understanding. The extent to which data are clear without ambiguity and easily comprehended
- Navigation of the KB. The extent to which data are easily found and linked to.

Effectiveness

- Relevancy. The extent to which information is applicable and helpful for the task at hand
- Number of source with definition of author of information

Satisfaction

• Presence and assessment of incentives.

Security

- Creation of login credentials and its assessment
- Extent of the clarity of the process about who and how release credentials





Environmental impact

Saving on energy consumption

- quantify energy used (comparison with other systems) Saving on travels costs
 - Travel costs during the use of SecInCoRe (in a certain period of time)

Resources efficiency

- quantify resources needs (comparison with other systems)
- quantify time for organising resources on the field

Social Impact

Impact on employment and working routine

- Improvement on working routines (Please describe how does your working routines change using SecInCoRe)
- Improvement on employment (Please describe how does SecInCoRe could impact employment in your organisation/institution)
- Time saved in the working routine using SecInCoRe (Please describe how does your working time change using SecInCoRe)

Knowledge production and sharing

Knowledge sharing

- Number of European disasters inserted in the dataset
- Number of different typologies of disaster
- Number of different sizes of disaster
- Covering different typology of stakeholders involved in different disasters
- Number of datasets linked to SecInCoRe
- Total number of sources available in SecInCoRe
- Number of emergency management models identified in the Inventory
- Number of information systems identified in the Inventory
- Number of business models identified in the Inventory
- Number of developed data sharing protocol
- Assess the easiness of exchange information among two or more parties
- Assess the quality of information
- Assess the awareness about past disasters using SecInCoRe

Support of ICT usage for all and democratic participants

- Number of countries involved
- Number of agencies involved
- Number of stakeholders
- Extent of the support informational self-determination
- Extent of the support non-discriminatory practices





- Assess privacy and restrictions
- Assess collaboration across nations, etc. using SecInCoRe in the respecting of differences

Social capital

Social capital increment for users and participants

- Assess the level of trust in exchanging information using SecInCoRe CIS
- Assess the level of trust using the Cloud (or similar) support (CEIS)
- Assess how SecInCoRe support people in lessons learnt reporting so that this does not lead to blame
- Assess how SecInCoRe make users' duty of care regarding technology maintenance known
- Assess the increasing of collaboration network using
- Assess how SecInCoRe support integration of existing

Evaluating the SecInCoRe Project

Social capital increment for project participants

- Extent of the increase of the network
- Extent of the increase of competences acquired

Scientific impact

- Number of project outputs in terms of scientific production
- Relevance of interdisciplinary activities in SecInCoRe
- Open access contribution
- Open access to research community





9.2 Appendix 2: JIRA requirements and possible indicators

JIRA REQUIREMENT SICR 113 Support informational self determination			
CIS MODULES ConOps; Collaboration practices		MENTIONED CONSULTATIONS no	IN
SecInCoRe Expected Outcomes	ELSI sensitive		
Impact Areas in Impact on employment and working routines; Knowle SEQUOIA production and sharing		Knowledge	
POSSIBLE INDICATORS Assess the extent of supporting informational self-determination			

JIRA REQUIREMENT SICR 114 Support inclusiveness through search				
CIS MODULES Taxonomy		MENTIONED IN CONSULTATIONS yes		
SecInCoRe Expected Outcomes	Make unknowns visible; quality of information / intera	Trusted relationships; Enhanced actions		
Impact Areas in SEQUOIA	Technological impact; Knowledge production and sharing			
POSSIBLE INDICATORS Number of data stored in the inventory. Assess the amount of data stored				





JIRA REQUIREMENT SICR 116 Support equal access			
CIS MODULES ConOps; Collaboration practices		MENTIONED CONSULTATIONS no	IN
SecInCoRe Expected Outcomes	ELSI sensitive		
Impact Areas in SEQUOIA	Impact on employment a production and sharing	and working routines;	Knowledge
POSSIBLE INDICATORS Assess the extent of equal access			

JIRA REQUIREMENT SICR 117 Support diversity across nations, agencies, users.			
CIS MODULES MENTIONED CONSULTATIONS			
framework		yes	
SecInCoRe Expected Outcomes	New partnerships; Better relationships	common understanding; Trusted	
Impact Areas in SEQUOIA	IMpact on employment a production and sharing; Soc	and working routines; Knowledge cial capital	
POSSIBLE INDICATORS			
Number of countries involved			





JIRA REQUIREMENT SICR 118 Strive for simplicity in design			
CIS MODULES ConOps; Semantic framework		MENTIONED IN CONSULTATIONS yes	
SecInCoRe Expected Outcomes	More informed; Living and inclusive		
Impact Areas in Technological Impact SEQUOIA			
POSSIBLE INDICATORS Assess system understanding			

JIRA REQUIREMENT SICR 119 Support non discriminatory practices				
CIS MODULES Collaboration practices No			IN	
SecInCoRe Expected ELSI sensitive; Trusted relationships Outcomes				
Impact Areas in Impact on employment and working routines; Knowle SEQUOIA production and sharing		Knowledge		
POSSIBLE INDICATORS Assess the capacity to support non-discriminatory practices				





JIRA REQUIREMENT SICR 120 Enable direct communication between users				
CIS MODULES Collaboration practices		MENTIONED CONSULTATIONS yes	IN	
SecInCoRe Expected Outcomes	To support collaboration and interoperability; Efficiency; Better collaboration		ency; Better	
Impact Areas in SEQUOIA	Impact on employment and working routines; Knowledge production and sharing; Social capital			
POSSIBLE INDICATORS Assess the easiness of exchange information among two or more parties				

JIRA REQUIREMENT SICR 121 Support people in lessons learnt reporting so that this does not lead to blame				
CIS MODULES Collaboration practices		MENTIONED IN CONSULTATIONS no		
SecInCoRe Expected Outcomes	Trusted relationships; Cloud; ELSI sensitive			
Impact Areas in SEQUOIA	Impact on employment a production and sharing	and working	routines;	Knowledge
POSSIBLE INDICATORS Assess the extent of supporting lessons learnt				





JIRA REQUIREMENT

SICR 122 Support social and organisational practices of interoperability

CIS MODULES		MENTIONED IN		
Collaboration practic architecture	es; Modular system	yes		
SecInCoRe Expected Outcomes	To support collaboration and interoperability; Efficiency; Better collaboration			
Impact Areas in SEQUOIA	Impact on employment and working routines; Knowledge production and sharing; Social capital			
POSSIBLE INDICATORS				
Assess interoperability through the system				

JIRA REQUIREMENT SICR 122 Support social and organisational practices of interoperability				
CIS MODULES Collaboration practices		MENTIONED IN CONSULTATIONS yes		
SecInCoRe Expected Outcomes	Enhanced quality of information / interactions; Better collaboration			
Impact Areas in SEQUOIA	Impact on employment and working routines; Knowledge production and sharing; Social capital			
POSSIBLE INDICATORS Assess level interoperability using SecInCoRe				




JIRA REQUIREMENT SICR 126 Support people in keeping the inventory and/or the CIS relevant **CIS MODULES MENTIONED** IN CONSULTATIONS Collaboration practices yes SecInCoRe Expected Enhanced quality of information / interactions Outcomes Impact on employment and working routines; Knowledge Impact Areas in **SEQUOIA** production and sharing **POSSIBLE INDICATORS** Assess incentives to populate the database

JIRA REQUIREMENT SICR 138 Function to create private online data sharing communities			
CIS MODULES Collaboration practices		MENTIONED CONSULTATIONS yes	IN
SecInCoRe Expected Outcomes	Bettr collaboration; Cloud; L	iving and inclusive	
Impact Areas in SEQUOIA	Impact on employment a production and sharing; Soc	and working routines; cial capital	Knowledge
POSSIBLE INDICATOR Assess the level of trust	S in exchanging information us	ing SecInCoRe-	





JIRA REQUIREMENT SICR 14 Author of Inform	nation		
CIS MODULES Semantic framework		MENTIONED CONSULTATIONS yes	IN
SecInCoRe Expected Outcomes	Trusted relationships; Clouc	1	
Impact Areas in SEQUOIA	Impact on employment a production and sharing	and working routines;	Knowledge
POSSIBLE INDICATOR Number of sources with	S author		

JIRA REQUIREMENT SICR 146 Help create trust in regards to security of the cloud			
CIS MODULES Collaboration practices		MENTIONED CONSULTATIONS yes	IN
SecInCoRe Expected Outcomes	Cloud; Security; Trusted rel	ationships	
Impact Areas in SEQUOIA	Impact on employment a sharing	and working routines;	knowledge
POSSIBLE INDICATOR	S		





IN

JIRA REQUIREMENT SICR 153 Create flexibility so that the system can incorporate new sources of data **CIS MODULES MENTIONED** CONSULTATIONS Semantic framework; Knowledge base yes SecInCoRe Expected Flexibility; Living and inclusive; Outcomes Impact Areas in Technological impact; Impact on employment and working **SEQUOIA** routines POSSIBLE INDICATORS

Number of datasets linked to SecInCoRe

JIRA REQUIREMENT SICR 158 Make users' duty of care regarding technology maintenance known			
CIS MODULES Collaboration practices		MENTIONED CONSULTATIONS yes	IN
SecInCoRe Expected Outcomes	Efficiency;		
Impact Areas in SEQUOIA	Technological impact		
POSSIBLE INDICATOR ssess users' duty of care	S e technology maintenance		





JIRA REQUIREMENT SICR 165 Support, do not replace other processes/systems			
CIS MODULES ConOps; Nec		MENTIONED IN CONSULTATIONS yes	
SecInCoRe Expected Outcomes	Scalability; Flexibility; Stand	lardisability	
Impact Areas in SEQUOIA	Technological impact; finan	cial impact	
POSSIBLE INDICATOR Assess the value of syst	S ems integration		

JIRA REQUIREMENT SICR 167 Support lingui	stic translation	
CIS MODULES Collaboration practices		MENTIONED IN CONSULTATIONS yes
SecInCoRe Expected Outcomes	New partnerships; More info	ormed; Make unknowns visible;
Impact Areas in SEQUOIA	Impact on employment ar impact	nd working routines; Technological
POSSIBLE INDICATOR Percentage of document	S is translated	





JIRA REQUIREMENT SICR 168 Support operational translation between different organisations **CIS MODULES** MENTIONED IN CONSULTATIONS Collaboration practices; Taxonomy yes Enhanced quality of information / interactions; Standardis-SecInCoRe Expected ability; Efficiency Outcomes Impact Areas in Impact on employment and working routines; Technological **SEQUOIA** impact; knowledge sharing **POSSIBLE INDICATORS** Assess easiness of exchange information

JIRA REQUIREMENT SICR 169 Support trans	lation through taxonomy	
CIS MODULES Taxonomy		MENTIONED IN CONSULTATIONS yes
SecInCoRe Expected Outcomes	Better common understandi	ng;
Impact Areas in SEQUOIA	Impact on employment ar impact; knowledge sharing	nd working routines; Technological
POSSIBLE INDICATOR Assess accessibility	S	





JIRA REQUIREMENT SICR 177 Provide tools to help reflect on the quality of the data in the inventory **CIS MODULES MENTIONED** IN CONSULTATIONS Collaboration practices; Knowledge Base no SecInCoRe Expected Enhanced quality of information / interactions Outcomes Impact Areas in Impact on employment and working routines; Technological **SEQUOIA** impact; knowledge sharing POSSIBLE INDICATORS Assess the quality of information

JIRA REQUIREMENT SICR 179 Create and pr	ovide guidelines for data use	
CIS MODULES Collaboration practices		MENTIONED IN CONSULTATIONS yes
SecInCoRe Expected Outcomes	Better collaboration; Enh interactions; Standardis-abi	nanced quality of information / lity
Impact Areas in SEQUOIA	Impact on employment a sharing	and working routines; knowledge
POSSIBLE INDICATOR Presence of a how to gu	S ide	





JIRA REQUIREMENT SICR 181 When presenting data, provide guarantees that data is secure and trustworthy/accurate **CIS MODULES MENTIONED** IN CONSULTATIONS Collaboration practices yes SecInCoRe Expected Trusted relationships Outcomes Knowledge production and sharing Impact Areas in SEQUOIA POSSIBLE INDICATORS Implementation of 1 tool explaining guaranties about trust

JIRA REQUIREMENT SICR 182 Prompt users to consider privacy, anonymisation and access restrictions			
CIS MODULES Collaboration practices		MENTIONED IN CONSULTATIONS yes	
SecInCoRe Expected Outcomes	ELSI sensitive; Cloud; Secu	rity	
Impact Areas in SEQUOIA	Knowledge production and working routines	sharing; impact on employment and	
POSSIBLE INDICATOR	S ictions		





SICR 183 Incorporate/de	evelop data sharing protocols		
CIS MODULES		MENTIONED CONSULTATIONS	IN
Collaboration practices;	taxonomy	no	
SecInCoRe Expected Outcomes	Better collaboration		
Impact Areas in SEQUOIA	Impact on employment ar impact; knowledge sharing	nd working routines;	Technological
POSSIBLE INDICATORS			
Number of developed da	ata sharing protocol		

JIRA REQUIREMENT SICR 188 Offer access to the CEIS for the different stakeholders			
CIS MODULES ConOps		MENTIONED IN CONSULTATIONS yes	
SecInCoRe Expected Outcomes	Security; Better collaboratio	n; Living and inclusive	
Impact Areas in SEQUOIA	Impact on employment ar impact; knowledge sharing	nd working routines; Technological	
POSSIBLE INDICATOR Numbers of different lev	S els of access		





JIRA REQUIREMENT SICR 25 Indicate data quality through supporting data accuracy			
CIS MODULES Semantic framework; kn	owledge base	MENTIONED CONSULTATIONS yes	IN
SecInCoRe Expected Outcomes	Enhanced quality of informa	ntion / interactions	
Impact Areas in SEQUOIA	Knowledge production and s	sharing	
POSSIBLE INDICATOR Assess quality of informa	S ation		

JIRA REQUIREMENT SICR 31 SecInCoRe should be resource efficient	
CIS MODULES ConOps	MENTIONED IN CONSULTATIONS no
SecInCoRe Expected Efficiency Outcomes	
Impact Areas in Financial impact; environme SEQUOIA	ental impact
POSSIBLE INDICATORS Quantify resources in terms of resources	





JIRA REQUIREMENT SICR 34 Integration with current system and cross platform suitable **CIS MODULES** MENTIONED IN CONSULTATIONS ConOps; Nec yes SecInCoRe Expected Scalability; Flexibility; Standardisability Outcomes Financial impact; environmental impact; technological impact Impact Areas in SEQUOIA POSSIBLE INDICATORS Number of existing technologies integrated. Number of systems integrated

JIRA REQUIREMENT SICR 38 SecInCoRe should be economically affordable			
CIS MODULES ConOps		MENTIONED IN CONSULTATIONS yes	
SecInCoRe Expected Outcomes	Economical; Efficiency		
Impact Areas in SEQUOIA	Financial impact		
POSSIBLE INDICATOR Total costs of the system	S ns and comparison with other	systems	



L



JIRA REQUIREMENT SICR 40 SecInCoRe should not incur additional expenses			
CIS MODULES ConOps		MENTIONED II CONSULTATIONS no	N
SecInCoRe Expected Outcomes	Economical; Efficiency		
Impact Areas in SEQUOIA	Financial impact		
POSSIBLE INDICATOR	S		

JIRA REQUIREMENT SICR 41 SecInCoRe should be energy efficie	ent
CIS MODULES ConOps	MENTIONED IN CONSULTATIONS no
SecInCoRe Expected Economical; Efficie Outcomes	ncy
Impact Areas in Environmental imp SEQUOIA	act
POSSIBLE INDICATORS Quantify energy needed	





JIRA REQUIREMENT SICR 42 Time to access information			
CIS MODULES Semantic framework; Kn	owledge base	MENTIONED IN CONSULTATIONS no	
SecInCoRe Expected Outcomes	Efficiency; more informed		
Impact Areas in SEQUOIA	Technological Impact		
POSSIBLE INDICATOR	S cess information		

JIRA REQUIREMENT SICR 56 Advanced search capabilities				
CIS MODULES Semantic framework		MENTIONED IN CONSULTATIONS no		
SecInCoRe Expected Outcomes	Make unknowns visible; I interactions	Enhanced quality of information /		
Impact Areas in SEQUOIA	Impact on employment a sharing	and working routines; knowledge		
POSSIBLE INDICATOR Assess relevancy	S			



I



JIRA REQUIREMENT SICR 68 Guidelines regarding ELSI			
CIS MODULES Collaboration practices		MENTIONED IN CONSULTATIONS yes	
SecInCoRe Expected Outcomes	Cloud; ELSI sensitive		
Impact Areas in SEQUOIA	Knowledge production and working routines	sharing; impact on employment and	
POSSIBLE INDICATOR	S that response to ELSI Guide	lines	

JIRA REQUIREMENT SICR 84 Assistance to re	educe decision making time	
CIS MODULES ConOps; Collaboration p	oractices	MENTIONED IN CONSULTATIONS no
SecInCoRe Expected Outcomes	Efficiency; Better collaborat	ion
Impact Areas in SEQUOIA	Technological impact; Imp routines	pact on employment and working
POSSIBLE INDICATOR Time to access the infor	S mation	





JIRA REQUIREMENT SICR 88 Search based o	on location, type of disaster	
CIS MODULES Semantic framework; Kn	owledge base	MENTIONED IN CONSULTATIONS yes
SecInCoRe Expected Outcomes	Make unknowns visible; More informed	
Impact Areas in SEQUOIA	Knowledge production and sharing	
POSSIBLE INDICATORS		
Number of European disasters inserted in the dataset. Number of different typologies of disaster. Number of different sizes of disaster		

JIRA REQUIREMENT			
SICR 92 Enable differen	t level of detail of information		
CIS MODULES ConOps; Semantic fram	ework	MENTIONED CONSULTATIONS yes	IN
SecInCoRe Expected Outcomes	Trusted relationships; Security; Cloud		
Impact Areas in SEQUOIA	Technological impact; Knowledge production and sharing		
POSSIBLE INDICATORS Assess quality of information			



L



JIRA REQUIREMENT			
SICR 98 SecInCoRe users need an improved awareness of past disasters			
CIS MODULES ConOps; Semantic frame	ework	MENTIONED CONSULTATIONS yes	IN
SecInCoRe Expected Outcomes	More informed		
Impact Areas in SEQUOIA	Technological impact; Knowledge production and sharing		
POSSIBLE INDICATOR Assess the awareness a	S bout past disasters using Sec	cInCoRe	





9.3 Appendix 3: first collection of zero scenarios

In line with the SEQUOIA methodology selected for project evaluation, one of the most relevant steps to define the added value produced by the project is the comparison between the situation without the project and how the situation changes with the project implementation.

To do that the start of the process is the gathering of examples of the so called Zero Scenario, namely the current situation of how stakeholders work for reaching specific purposes without SecInCoRe. As a first indication of the type of data related to the identification and assessment of Zero Scenarios according to SEQUOIA, we provide a list of Zero Scenarios collected from project partners in the preceding months.

As affirmed in D5.2, due to the complexity of the field, to the several emergency services involved and also to the differences among countries, it is not possible to derive only one Zero Scenario against which to compare the SecInCoRe concept. Therefore, several different scenarios are described.

At the current stage of the project, Zero Scenarios are collected on the basis of the real working experiences of Advisory Board members. A questionnaire (Annex VI) was completed by all members of the Advisory Board and then specific interviews were organised with some of the members to collect more information about the preparation and training activities.

Following the definition of preparedness activities contained in D4.2, The Zero Scenarios provided refer to the planning activities and to the training activities for events related to the following emergencies:

- Fires
- Floods
- Health emergency

These Zero Scenarios were built on the working routines of different stakeholders accordingly to the definition of stakeholders working in preparedness activities given in D5.2 and D4.2 engaged as first responders in the following organisation:

- Health services
- Police
- Fire brigades
- Local Authorities

The aim is to provide a picture of the current work of the figures potentially users of the project. Information stored in this deliverable will be enlarged in the future steps to gather further information according to the Demonstration Case Protocol.

Zero Scenario 1: preparedness and training activities in a Fire scenario in Germany

Fire brigades scenario





The Zero Scenario for planning the emergency is based on the real experience of a Fire Department in Germany. Data are collected from the direct experience of a Chief Fire personally involved in operations and planning.

The real case referred to is one of the major fire disasters to have occurred in Germany in the last 10 years. The location concerned was a factory situated in a port area. To solve the situation specific plans were applied to the emergency.

According to the Department Chief Fire Officer that replied to our interview and in charge of Incident Commander for larger scale incidents either on-scene or in staff room, also deputises for Chief Fire Officer and Fire prevention, the command process in Germany follows a similar cycle to the one foreseen by the Humanitarian Process Cycle (HPC)¹³. For the HPC elements for prepare, manage and deliver a humanitarian response are:

- needs assessment and analysis
- strategic response planning
- resource mobilisation
- implementation and monitoring
- operational review and evaluation.

However, in the case of the German Fire Brigades the command structure follows a relatively similar cycle envisaged by regulation Leadership and Command in Emergency Operation, FwDV 100¹⁴.

The first step is to assess the situation, specifically the operational issues it creates and how they impact on the wider operational area.

This is followed by an assessment of resource requirement and then the development of a strategic plan to resolve the situation. Tactical plans are then devised which will include command locations and resource management and mobilisation. The effect of these plans is continuously monitored and adjusted depending on its effectiveness in combating the situation.

To respond to the real incident, fire brigades have contingency plans prepared: these include plans for specific locations, such as chemical factories or football stadia and for specific types of incident, such as a train collision.

In the case of the real incident in the port area, the fire brigades combined these two approaches.

The reason is that, on the one hand they needed specific information on the area but, on the other, they also needed general information on how to react to the kind of incident, based on previous experiences of similar types of incident.

According to what said by the subject during the interview, it is important to stress that there is no space for improvisation. In his opinion, a plan is something that gives you basic information, then you have tactical information to adapt to the accident. So, the ordinary way to manage the incident is not related to the improvisation but what you learnt by a tactical level.

 ¹³ https://www.humanitarianresponse.info/en/programme-cycle/space
¹⁴ Available at:

http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/FIS/DownloadsRechtundVorschriften/Volltext_Fw_Dv/FwDV-100%20englisch.pdf?__blob=publicationFile





Due to the relevance of the plans, their production is the specific task of a sub-unit of the fire department that is engaged full time in planning during the year. The staff is made by 3 or 4 people.

These people are experienced middle-ranking officers, rather than of operational firefighters. Referring to the categorisation of SecInCoRe they can be defined as Emergency Planners.

The average gross average salary is estimated around at 53,000 Euros per annum per person¹⁵.

To produce a contingency plan for the factory they spent a couple of days adapting information that they have on the situation.

The material (non-personnel) costs of this Emergency Planning Unit is estimated at 120,000 Euros per annum. Staff salaries are in addition to this figure. It is important to understand that this is for one emergency service: police, medical and local authority bodies also have such departments and associated costs.

Regarding the use of tools or instruments used to assist in planning, maps, chemical data bases, helicopter photographs and information received via radio are the most used tools during the emergency response. These tools are equally valuable for planning and preparation.

About the level of information quality that are used to prepare a plan was said that at the moment it's not possible to assess a high level of quality. The main reason is that to plan a response there is access to standardise document plans that are good for first responders but it's difficult to have the information at specific level.

Information are not enough for long runner accidents because they are superficial. General information are important for first responders but a database with different layers with different information will help in planning having access to different materials.

What emerged is that people in planning need to have more information, they need to aggregate data. On the other hand, first responders have to receive basic information in order to be concentrate on specific information only.

The accuracy of the plan that they realised with current practices is assessed at 5, on a Likert Scale from 1 to 6¹⁶. The main issue that has to be considered is the problem of keeping the plan up to date the plan as modifications and other changes take place.

The scenario for the creation and organisation of training exercises to react to emergency is based, in part on the experiences of staff in previous, similar circumstances.

¹⁵ All information required is useful in order to understand current practices in emergency services. Current practices are also relevant from an economic point of view. In line with this was also asked to subject interviewed to report some costs of personnel working in the sector.

¹⁶ The Likert scale from 1 to 6 where 1 is vey low 2 and 6 is very high.





The main figures involved in the preparation of a full-scale training exercise in the Department of Chief Fire in Dortmund are at least 10 people full time. These people are a combination between emergency planners, operational people and training officers.

The gross average salary is estimated around 53,000 Euros per annum per person

The planning of a full scale exercise takes around 15 days with all relevant organisations (e.g. Red Cross, police) collaborating together. A further 10-12 days is usually required first to arrange the collaboration process.

At the moment it is not possible to estimated main costs that the Unit in charge of the training organisation have to sustain in order to build a training exercise besides human resources.

The kind of data used to organise a training exercise as a preparation in case of disaster is very similar to the liv operation, namely maps, chemical databases and so on. A greater emphasis however can be placed on previously learned experiences and legislation in the training scenario.

The amount of information used to prepare a training exercise is usually significant. The focus is to develop a scenario that is credible and really useful for all participants, without the time and operational constraints present during a live operation. This information can be extracted from that available to all those participating organisations. The accuracy of the training exercise created, on a scale from 1 to 6^{17} , it is 4/5 is the level of accuracy.

Once the planning is complete, around 150 people attend the exercise.

Zero scenario 2: preparedness and training activities in a Fire scenario in Greece

Local authority scenario

This zero scenario was built on real information provided by KEMEA.

Forest Fire Scenario: Marathon Wild Forest Fire, North East of Athens

At 11:05 am, on a summer day, 18th July, the alert network signals a wildfire in a mountainous woodland which is not easily observed from the fire alert network early warning towers around it. The altitude above sea level is about 700m. Prevailing weather conditions are as follows: wind direction is from the North/North East, measuring 7 on the Beaufort Scale; the Relative Humidity is 16% and the temperature is 35 Celsius. Regarding the vegetation, the mean fine fuel moisture content is 10%. Due to terrain shape and deficiencies in the network coverage, more accurate information is not available in the control centre. To evaluate a wildfire and to prevent further fire propagation, an aircraft is dispatched, while the ground forces (fire vehicles) are also directed to the area.

¹⁷ The Likert scale from 1 to 6 where 1 is vey low 2 and 6 is very high.





The main figures involved in the preparation of a plan to reply to that situation are: Civil Protection, Fire Service, Police, Ambulance Service, Military Agencies, Local and Regional Authorities (Municipalities), Volunteers and Non-Governmental Organisations etc.

The gross average salary of people involved is estimated as €2.000 per person monthly

The working days needed to establish an emergency response plan that could fit with the real situation is estimated as 1 day.

The average costs of the Unit in charge of the establishment of the emergency response plan (in addition to personnel costs) will depend on the operational needs, the number and the working hours of the fire vehicles and aerial means used, taking into account the fire propagation and the total duration of the operation. At the moment it is not possible to produce an estimation.

To produce a response, plan the following data are needed:

Weather conditions, the kind of vegetation, ground relief, available ground and aerial fire-fighting personnel and equipment, potential vicinity to urban area, shorter ground forces access, significant critical infrastructures (industries, hospitals, airports, military areas etc.)

Such data flow comes from the engaged organisations in combination with the information given by the citizens / inhabitants. The level of the information quality is estimated as adequate accordingly to the opinion of the subject interviewed.

The accuracy of the plans delivered is scored at 4.

Regarding the main figures involved in the preparation of a training exercise in the organisation are: Civil Protection, Fire Service, Police, Ambulance Service, Military Agencies, Local and Regional Authorities (Municipalities), Volunteers and Non-Governmental Organisations etc.

The gross average salary is estimated as €2.000 per person monthly-

To establish a training exercise 5 working days are needed.

The main costs of the organisation's training unit in charge of the training depends on the duration of the training, the number and the target groups of the trainees, the number and the working hours of the trainers, the number of the fire vehicles and aircraft used.

The data used to organise a training exercise as a preparation in case of disaster are: Weather conditions, the kind of vegetation, ground relief, available ground and aerial fire-fighting forces and means, potential vicinity to urban area, shorter ground forces access, significant critical infrastructures (industries, hospitals, airports, military areas etc.), taking into account the potential engaged organisations (Civil Protection, Fire





Service, Police, Ambulance Service, Military Agencies, Local and Regional Authorities, Volunteers and Non-Governmental Organisations etc.)

The level of the information that is used to prepare a training exercise is adequate due to the fact that data providers are the organisations engaged in combination with the information given by the citizens/inhabitants, as actors.

This allows an accuracy score for the plan of 4.

Zero scenario 3: preparedness and training activities in a flooding scenario in UK

Local Authority Scenario

The scenario described refers to the real emergence of flooding in Somerset, UK, in 2013/2014 and following data are provided by the County Emergency Planners directly involved in the writing of plans for the emergency. The respondent works in a multi-agency environment, as the staff officer to senior managers responsible for response and recovery phases.

First of all, according to the Humanitarian Process Cycle (HPC) elements for preparation, management and delivery of a humanitarian response applied by the Local Somerset Authority are very close to the original cycle provided by the organisation. Main steps are the following:

- Assess the problem
- Provide a plan
- Provide a response
- Response
- Analyse and evaluate results

2 people were involved in the preparation of the plan. The roles of those people are: Emergency Planner and a Manager Planner.

However, the preparation for an emergency is generally a multi-agency issue and it involves more levels: operational, tactical etc. the level of engagement of different levels depends on the scenario that has to be planned.

In this case, authorities from the County and District Councils were involved (different areas of responsibility)

The gross average salary of people involved is the following:

- Emergency Planners 40,000 Euros yearly
- Manager planners around 51,000 Euros yearly

However, such roles can varies from figure to figure. For example, equivalent level police officers and fire officer are more expensive. Continuing, a manager in districts it's around 65,000 Euros yearly.

In this case the amount depends from the work and from the amount of time spent to produce a plan.





It is estimated that for creating a simple plan it's around 20-25,000 Euros while for a bigger one it is 39,000 Euros or more. It depends from the difficulty of the plan that have to be created.

The problem is also that every agency has its own plan but having a common one elaborated in group will help reduce cost and save time.

The process of creating the relevant contingency plan is as follows it is generally written by a single person in a draft form. After that the plan is revised and modified by others with specific skillsets. The process takes around one year.

The local authority has a generic plan and other more specific sub-sections. Accordingly with the subject interviewed the plan that they are able to produce is not perfect but it's very valid. From 1 to 6 the score is 5.5.

The plan created was fit for the purpose for which it was intended, but was lacking when applied to an incident of 12 weeks duration, which had not been foreseen. Consequently, it was revised after the disaster.

The average costs of the Unit in charge of the establishment of the emergency response plan (excluding personnel costs) is estimated around 32,000 Euros annually.

At the moment, it is not possible to estimate the overall costs in terms of human resources and other costs if more than one organisation is engaged.

Regarding the kind of information used for planning it was explained that in such cases to organise a plan for floods historical data from various areas would be used, taking into account the risk factors in different zones. Flooding can have different causes: river flooding, rain flooding, groundwater flooding etc. So, the planning is risk based and the assessment of the risk is the most important part of planning. The risk assessment is carried out by the Local Resilience Forum.

Local information such as documents about the area, agricultural information, Environment Agency information is routinely and easily exchanged with local authorities.

The level of information exchange is very high and in a scale from 1 to 6 is assessed at 6.

The scenario for the creation and organisation of training exercises to react to emergency is based on the experience of the Somerset Authority in the UK too.

The main figures involved in the preparation of a training exercise in the Local Authority of Somerset are two: an Emergency Planner and a Manager

Their gross average salary can varie but can be estimated as follows:

- Emergency Planners 40,000 Euros yearly
- Manager planners around 51,000 Euros yearly

To prepare a training exercise for flooding took around six months of work.





The main costs that the Unit in charge of the training organisation have to manage in order to build a training exercise besides human resources are related to the organisation costs such as venue, people that run the exercise and food.

The cost for human resources is about 130 Euros per day for the owner of the plan. However, training is generally a multi-agency arrangement. When the training is organised within the local unit it is usually on a 1-to-1 basis.

To organise a training exercise as part of disaster preparation the kind of data must be above all realistic. Indeed, the developed scenario is in fact based on real incident information. This is taken from different relevant authorities and is easily accessed.

Both the level of the information used to prepare a training exercise, its accessibility and ease of exchange is very high.

Referring to the real disaster that occurred the accuracy of the training exercise is assessed as 6.

Police authority scenario

This Zero Scenario is related to a response of the North Yorkshire Police to major inland flooding caused by sustained heavy rain, overflowing rivers and ground water run-off in the UK.

The general work flow applied by the police shares main action envisaged by the Humanitarian Process Cycle (HPC).

Particularly, the main figures involved in the preparation of plans in the North Yorkshire Police are all the people involved in the Emergency Planning Unit. The unit currently has 3 members of staff.

The gross average salary is approximately 38,000 Euros per member of staff.

To establish an emergency response plan requires approximately one week of work. Having a plan ready to apply for the emergency ensures that generic actions are carried out quickly. Partner Agencies are notified quickly and a Shared Situational Awareness is achieved. Command and Control arrangements are well tested.

The average cost of the Unit in charge of the creating the emergency response plan (excluding human resources) is defined as minimal. All plans are constructed with partner agencies under the Lancashire Local Resilience Forum (LLRF), for a joint response from Category 1 and 2 responders under the Civil Contingencies Act 2004. These include, amongst others, the emergency services, local and regional government and Environment Agency. There is a cost in respect of preventative measures implemented, but other planning is a Human resources cost only.

The data that are used to plan a response to emergency are the following:

- Historical data from previous flooding events including river levels
- Predicted seasonal weather forecasts
- Modelling data from the Environment Agency including maps showing predicted





- Flood affected areas
- Details of Critical Infrastructure e.g. Electricity Sub Stations, Hospitals
- Water treatment facilities.
- Vulnerable people within a particular area e.g. nursing homes

The quality of the information used to prepare a plan are assessed comparing data to previous events and looking at the source of the data.

The process that has to be followed to validate a plan consists of 3 steps:

- Peer review
- Training and exercising
- De-briefs following live events

Given the result of the planning from the perspective of the subject, the level of accuracy is score as 4.

The scenario for the creation and organisation of training exercises to react to an emergency is based on the experience of the North Yorkshire Police for the preparation of flooding.

The main staff involved in the preparation of a training exercise in the North Yorkshire Police are the 3 people working in the Emergency Planning Unit. Their average gross salary is around 38,000 Euros per person, per year.

To establish a training exercise 2 working weeks are needed.

The main costs that the Unit in charge of the training organisation incurs in order to build a training exercise besides human resources are: exercise documentation, venue and refreshments.

If more than one organisation is engaged, the estimated overall costs of training in terms of human resources and other costs is around 3.870 Euros.

To organise a disaster preparation training exercise, the police need:

- Data from previous live events identifying impact and occurrences
- Debrief material from previous live events and associated recommendations
- Enquiry reports
- Previous training and exercise materials

Such information is provided through exchanges and collaboration with other agencies, open sources such as internet. and historical data

The accuracy of training exercise is scored at 5/6.

Zero scenario 4: preparedness and training activities in the health service

Medical staff scenario

In order to collect information about a Zero Scenario for preparedness and training in health services, information was collected through the experience of a medical member of staff at the Rescue Coordination Centre in Norway.





In the case of a preparation plan for health emergency, elements for preparation, management and delivery of a humanitarian response fit very well with the workflow followed by the HPC. The important aspect is that the process is a cycle so activities are conducted in parallel in a continuing working flow.

The preparation of the plan is focused mainly on two levels. The first is the Municipal responsibility: within the Municipality, 10 people work as General Practitioners (GP) for the District Medical Officer that is led by a Chief Municipality Medical Officer. However, the number of GPs varies between municipalities, depending on their size (which ranges down from 500,000 to only 350 inhabitants).

Those people organise the emergency preparedness, which is a cross-sector activity. In line with this, the Health Care planning is taken into account by the Municipality.

Organisationally, hospitals are not part of the municipal structure, but emergency planning is done in collaboration between them and the municipalities, as there has to be an operational collaboration in handling emergencies. Additionally, hospitals are in charge of some operations and also ambulances are referred to hospitals. But this changes depending on the size of the hospital. This means that during a disaster event the Municipality is responsible for operations for 24 hours 7/7 and the general practitioners have to be operational. Then there is a responsibility at the hospital level but also the Ambulance officer has a direct responsibility.

There is a wide range of salary figures estimated as follows:

- General Practitioner 200,000 Euros per year
- Ambulance Officer 70,000 Euros per year
- Ambulance worker 50,000 Euros per year

It is not possible to define the period of time to write a plan because the planning is an on-going activity. Planning is a joint venture among different sectors and every existing scenario helps in the improvement of planning and response. After an accident the evaluation phase identifies what was right and what went wrong. On this basis, the plan is improved.

The time spent by organisations in planning changes a lot from one organisation to another. Some municipalities have a dedicated office with a full time Emergency Planner. In another situation, planning can take 5% of the time of a member of staff employed on other duties.

In the hospital an emergency planner could be paid around 53,000 Euros.

The average costs incurred by the Unit in charge of the establishment of the emergency response plans (excluding human resources) are difficult to estimate. Generally, a Chief Officer earns 100,000 Euros yearly but the salaries of all the additional staff are additional to that.

The kind of data used to plan a response to a medical emergency are stored in medical and resource databases. Such databases are useful to all officers, not only for the medical doctors but also for general practitioner in the field.





Then, was asked to assess the quality of information they work with. The selfassessment of the quality of information is assessed as very high. The high quality is due to the fact that they use public data that are very trustable. The high quality of information allows to have very accurate plans. This helps very much and limit the space for improvisation.

The main figures involved in the preparation of a training exercise are:

- Emergency Committee
- Team leader
- All team members.

In some cases, specific figures can be called upon to participate in the organisation. An example is provided by the Communication Centre that organised a training on fire rescue. In this case the emergency planner had an agreement with the Fire Brigades that run the training.

The kind of information needed to organise a training exercise is mainly lessons learned from previous exercises and operations and scenario-based events. Generally, this information is of a high level of quality.

At the moment it is not possible to provide an estimation of how many working days are needed to establish a training exercise, nor the overall costs of training in terms of human resources and other costs.





9.4 Appendix 4: Demonstration Case Template

Template for demonstration case for SecInCoRe

Version 1.0 approved

Prepared by <author>

<organisation>

<date created>

Revision History

Name	Date	Reason For Changes	Version





Guidelines for populating the Demonstration Case Template

The aim of the Demonstration Case Template is to detail the elements of the Demonstration Cases (the involved Stakeholders, the embedded Scenarios, the associated Use Cases and the relative Demonstrator Implementations) in order to:

- Clarify the goals of the Demonstration Case
- Identify the technical, design and inventory requirements for the creation of Demonstrator Implementations based on Reference Implementations
- Specify the requirements and aims of the Demonstration Case in relation to SecInCoRe validation and evaluation strategy

Given that SecInCoRe is an evolving socio-technical system, Demonstration Cases will necessarily have an emergent nature since they will have to be co-designed with involved stakeholders so as to reflect their needs, expectations and interpretations of the systems and allow stakeholders to creatively make use of the possibilities it provides.

The Demonstration Case Template accounts for the evolving and emergent nature of Demonstration Cases by considering that there are two phases in the definition of a Demonstration Case:

- A preparation phase that includes project partners involved in: (a) organising and preparing the Demonstration Case through interaction with stakeholders; (b) project partners responsible for preparing Demonstration Implementations by adapting Reference Implementations to the specific needs of the Demonstration Case; (c) the validation and evaluation team, that is responsible for ensuring that data collected on outputs and outcomes related to the Demonstration Cases are integrated in the overall SecInCoRe validation and evaluation strategy.
- 2. A definition phase that includes stakeholders alongside project partners. In this phase a detailed specification of Scenarios, Uses Cases and Demonstrator Implementations required for the Demonstration Case is produced in interaction with stakeholders. Individual elements of the Demonstration Case are mapped on high-level requirements with reference to JIRA for their technical implementation, and on CIS Concept Modules and associated SMART or scenario-based indicators for evaluation and validation purposes.

[Please note that for the time being we are only presenting you with the sections of the Demonstration Case Template related to the Preparation Phase. The Template sections relevant for Phase 2 will be sent shortly, and they are expected to be filled in after interactions with Stakeholders are at a more advanced stage.]

This section provides the guidelines for compiling the Demonstration Case Template. Some Template fields already contain a short description or illustrative examples on the kind of information that partners are expected to provide.

Scenario for demonstration Identification

Scenario for Demonstration ID

• Give each Demonstration Case a unique numeric identifier.





• Demonstration Case Name

State a concise, results-oriented name for the use case. These reflect the tasks the user(s) need to be able to accomplish using the system. Include an action verb and a noun.

- Demonstration Case History
- Created By

Supply the name of the person who initially documented this Demonstration Case.

• Date Created

Enter the date on which the Demonstration Case was initially documented.

• Last Updated By

Supply the name of the person who performed the most recent update to the Demonstration Case description.

• Date Last Updated

Enter the date on which the Demonstration Case was most recently updated.

Demonstration Case Description

Name of the Demonstration Case

1. Short description and main aims of the Demonstration Case

Please insert the main aims of the demonstration case including, if possible, any specification about the main aims of the Demonstration Case (e.g., need for collaborative planning, risk definition and preparation, sharing lessons learned, building trust).

2. Emergency Phase(s) covered in the Demonstration Case

Please specify the phase(s) of the emergency using the following codes for phases and category:

Emergency Phase	Categorisation
Mitigation	P.1
Preparedness	P.2
Response	P.3
Recovery	P.4

3. Short description of the possible Scenario(s) identified for the Demonstration Case

Please describe the possible Scenarios that the team intends to propose or discuss with stakeholders during the preparation phase. The final scenario selected with stakeholders for the Demonstration Case may be one of the





proposed scenarios, a modification of the proposed scenarios or an altogether different scenario. Please identify each proposed Scenario with a unique Scenario ID.

At this stage, it would be very useful if (following the three examples reported in the Template) BAPCO, KEMEA and ULANC could fill the description according to the information they have.

4. List of stakeholders involved in the Demonstration Case

List all the stakeholders that you would like to participate (or that you expect will participate) in designing and running the Demonstration Case. Identify each stakeholder with a unique Stakeholder ID (SH ID) and use the same SH ID to refer to that stakeholder in the remainder of the Template. Please specify the category of each Stakeholder using the codes provided in the attached file.

5. Contact details for stakeholders involved in the Demonstration Case

Please provide contact details for each stakeholders. For organisations, please report the main contact person. If different departments from the same organisation are involved, please provide departmental and personal details.

6. Do (some or all) stakeholders belong to larger organisations / consortia?

List all umbrella organisations or consortia that are (even to a partial degree) involved in the Demonstration Case (such as the Lancaster Resilience Forum) and list all the stakeholder that belong to the organisation

7. Stakeholders description

Please provide a brief description for each stakeholder, their functions and their degree of involvement in both the preparation phase and the actual Demonstration Case

8. Inventory and semantic models

Please identify with as many details as possible at the preparation phase the elements of the inventory that will have to be available for the Demonstration Case. Please provide indications about specific data sets or sources and reference whenever possible the following categories:

Information in Inventory (II)	Categorisation		
Crisis management models	II.CM (Information Inventory Crisis management)		
Information systems	II.IS (Information Inventory Information System)		
Data-sets	II.DS (Information Inventory Data-Sets)		





Business models	II.BM	(Information
	Inventory Models)	Business

For the remaining fields, please follow the guidelines provided in the Template.

Comments from the validation / evaluation team

After the partners responsible for organising and running the Demonstration Case have filled in their sections of the Template, the Template will be sent to T6 as the partner responsible for validation and evaluation. T6 will insert in this section comments, suggestions and indications related to validation and evaluation and send the Template to the Demonstration Implementation team. After a further round of comments between T6 and the partner responsible for the Demonstration Case, the Template will be sent to the partners responsible for developing the Demonstration Implementations.

Comments from the ELSI team

After the partners responsible for validation and evaluation have filled in their part of the Template, they will forward it to the ELSI team. The ELSI team will insert in this section comments, suggestions and indications related to ELSI implications or requirements that are important for the specific validation and evaluation activities outlined in this Template.

Comments from Demonstration Implementation team

The partner responsible for preparing the Demonstration Implementations that will be used for the Demonstration Case will add their comments and a final consultation will be held among all the interested project partners concerning the requirements, needs, timeframe and feasibility of the Demonstration Case.

Once a preliminary definition on the main objectives and attainable demonstrators has been agreed upon by project members, consultations with stakeholders can take place and Part 2 of the Template can be compiled.

Demonstration Case Identification

Demonstr ation		
Case ID:		
Demonstr		
ation		
Case		
Name:		
Created	Last Updated	
By:	By:	
Date	Date Last	





Created:

Updated:

Demonstration Case Description and Preparation

Demonstration Case Name:

Short description and main aims of the demonstration case

Example: International scenario in which actors from different countries cooperate and exchange data to prepare for future crises.

The aims of the demonstration case include collaborative planning, risk definition and preparation, sharing lessons learned, building trust.

Emergency Phase(s) covered in the demonstration case

Scenario ID Name			Name		
1 Example: Planning for a pandemic. For example, pandemic that has been experienced someplace else b might be expected to pop up in the UK.		for a pandemic. For example, a been experienced someplace else but pop up in the UK.			
2 Example: Sharing lessons across a border: for example have a small team of planners in the UK and another sm team in Germany working at the same time. On day 1, the each work in their respective groups to prepare lesson learnt about, for instance, flooding, and then day two the work at sharing it.		essons across a border: for example, of planners in the UK and another small orking at the same time. On day 1, they respective groups to prepare lessons stance, flooding, and then day two they			
3 Example: A coast guard situation where a foreign to arrives but there is an emergency on the boat (e.g. illnes chemical hazard) that is new to the region and thus require the quick development of a new set of plans.		guard situation where a foreign boat an emergency on the boat (e.g. illness or at is new to the region and thus requires ent of a new set of plans.			
l	_ist of st	akeholders	s involved in the Demo	onstration Case	
SH ID Name		Name		Stakeholder Category Code	
	1				
	2				

Short description of the possible Scenario(s) identified for the demonstration case



D5.3 Validation Strategy, Version 2 (ic) **Public deliverable**



3					
4					
5					
6					
	Expand if needed				
Contact	details for stakeholders involv	red in the Demonstration Case			
SH ID	Contact person(s)	Contact details			
1					
2					
3					
4					
5					
6					
	Expand if needed				
Do (som	e or all) stakeholders belong	to larger organisations / consortia?			
Name a	and contact details	IDs of the stakeholders that are members of the organisation / consortium			
Examp Resilie	le: Lancashire Local nce Forum				
Stakeholders description					
SH ID	Description				
1					
2					
3					





4					
	Expand if needed				
Preparatio	on of the Demonstration Case				
Please d Demonsti stakehold planned.	Please describe all the activities that have taken place until know to prepare the Demonstration Case, including your previous interactions / consultations with stakeholders and any other preparatory activities that have already been executed or planned.				
Expectation	ons and assumptions concerning Stakeholders' needs and involvement				
On the basis of your previous consultations with Stakeholders, please describe (a) the major incentives and obstacles for Stakeholders to participate in the Demonstration Case; (b) how you think they will contribute to the Demonstration Case in terms of sharing their data, activities, expertise, practices; (c) which assumptions regarding Stakeholders' participation and involvement need to be fulfilled for the Demonstration Case to achieve its aims; (d) how you intend to cope with possible defections or difficulties.					
Prelimina	ry definition of use cases associated with the Demonstration Case				
Please describe (in as much detail as possible given the current definition of the Demonstration Case) the Use Cases that are potentially associated with this Demonstration Case and one or more of the proposed embedded Scenarios-					
Reference	e Implementations that will be needed for the Demonstration Case				
Please provide details of the Reference Implementations that you expect will be used in the Demonstration Case					
Demonstr	ation Implementations				
Given the overall aims of the Demonstration Case, the current knowledge of stakeholders' needs and expectations and the current status of Reference Implementations, please explain what you think is needed to develop Demonstrator Implementation(s) that can be used for this Demonstration Case					
Inventory and Semantic Models					
Starting from the current status of the Knowledge Base, please describe which elements of the Inventory (specifically, the available data sources and semantic models) will be used for this Demonstration Case. Comment on the adequacy of the KB for the aims of the Demonstration Case, and please indicate any additional data sources that you expect to be able to integrate in the Knowledge Base before stakeholders start interacting with Demonstrator Implementation(s) in this					





Demonstration Case.

Tentative timeframe for the Demonstration Case

Please provide details about the possible timeframe for the Demonstration Case (including any preparatory or co-design activities) and about the expected duration of the Demonstration Case.

Comments from the validation / evaluation team

Please explain how the proposed Demonstration Case fits with SecInCoRe's validation and evaluation strategy. Starting from an evaluation – validation perspective, provide details about the requirements for the design of the Demonstrator Implementation(s) design and for data collection procedures. Please provide general comments first, then followed by specific observations for each module listed below. Whenever possible given the current definition of the Demonstration Case, refer to High-Level Requirements as reported in JIRA and to SMART indicators.

GENERAL COMMENTS:

VALIDATION / EVALUATION MODULES

Terminology					
Stakeholders					
Collab Practices					
And ELSI					
Taxonomy					
ConOps for CEIS					
HLRD					
Modular System					
Architecture					
NEC concept					
Semantic					
Framework					
Knowledge Base					
Comments from the ELSI team					
Please provide y	your comments	concerning	relevant	ELSI	implications,





requirements or objectives that, at the current state of definition, you see relevant for this Demonstration Case.

Comments from the Demonstration Implementation team

Please provide your comments concerning the feasibility, timeframe and requirements for adapting the Reference Implementations to this Demonstration Case. Whenever possible given the current state of definition of the Demonstration Case needs and functioning, make reference to the specific Requirements listed in JIRA. Please also describe any requirements related to the participation and involvement of Stakeholders and any other preconditions that need to be fulfilled / addressed in order for the Demonstration Implementations to be operational and adequate to the needs of the proposed Demonstration case.

Additional comments from other Project Partners

Please circulate the Demonstration Case Template to other relevant project partners, and ask them to add their comments below.




9.5 Appendix 5: SecInCoRe OpenAtrium User Manual

The OpenAtrium home page. Public content can be browsed freely without logging in. Participation in Spaces however is not possible until a user logs in, requests and subsequently gains access to a space. Please note the green 'public' box on the righthand side, indicating that the current space is visible to all visitors of the website. A private space will state 'private' in a red box, which would only be visible to members of that space.

DecInCoRe					
Common Information Space (CIS) conce	ept documentation	ଡ ି ସ			
Common Informati	on Space (CIS) concept docu	mentation			
SecInCoRe aims to bridge not only between or	ganisations, but also within organisations among different sectors, units,	Public			
etc. or between systems to enhance the interop management. For exploring the whole concept behind the	perability and information awareness during all phases of emergency e SecInCoRe CIS use the picture below for navigation.	CIS concept documentation			
Common Information Spa	ace (CIS) concept documentation	CIS Specification			
CIS Specification	Reference Demonstrations / mplementation Pilot Studies	Demonstrations / Pilots			
Common InformationSpace (CIS) Concept (CEIS)	Reference Appendix: Appendix: mplementations Cases	Request space membership There is no content in this space.			
Terminology HLED	Open Semantic Framework (05F) - CK_ Appframework - Energency Flamning Case				
Stakeholders Architecture	OpenAtrium (04) Browser UI Refugee Child Case				

Figure 23. Screenshot of SecInCoRe OpenAtrium home page

Logging in is done by clicking the Login button in the top right of the screen. If a user does not have an account, they can create one on the same page. Please do check your spam filter for the validation email.





cInCoRe
spaces 0
log In
Isername *

inter your SecInCoRe community portal username. you don't have an username, create an account.
assword *

inter the password that accompanies your username. You forgot your password, request a new password.
Log in

Figure 24. Screenshot of SecInCoRe OpenAtrium login page

Navigating around the OpenAtrium platform can be done in a number of ways. Pulldown menus are available to communicate each space's sub-spaces and sections. There is also the option to view the site-map by hovering over the house icon, which also lists all public spaces.

A pull-down menu pops out from under the home button.



Figure 25. Screenshot showing SecInCoRe OpenAtrium navigation





The green person icon on each space signifies that the space is public. Private spaces (illustrated using a red person icon) can not at present be seen in the site-map and other navigational menus. If required, this behaviour can be modified, pending further development work.

The eye icon seen in the current tree branch or the visible leaves allows the user to cease traversing the Spaces tree and to view the Space landing page.

SecInCok	Re			
- Common Inform	nation Space (CIS) concept documentation	- CIS Specification	•	Q 👻 Peter Gray
				View Members
Site Map fo	r CIS Specification	Search	Common Information Spa	ace (CIS) concept documentation -
		SecInCoRe community	portal	
	Common Informa	tion Space (CIS) c	oncept documentation 👁	
	CIS Specifica	Demonstration Pilot Studie	on/ Reference s Implementation	
	A	۲		

Figure 26. Screenshot showing SecInCoRe OpenAtrium sitemap

Once on a Space landing page, the site-map can once again be made visible by hovering over the gear icon and selecting 'Map' from the drop-down menu.

SecInCoRe	
A Common Information Space (CIS) concept documentation 🔹 CIS Specification 📼	
CIS Specification	A Members O
The specification of the common information space concept, one of the major outcomes of SecInCoRe, is divided in two main parts:	Map Public Subscribe
Socio-technical elements of the CIS concept Cloud Emergency Information System (CEIS) concept	CIS Specification
CIS Specification	CEIS
Common Information Space (CIS) Concept System (CEIS)	CIS concept
Terminology HLRD	Request space membership
Stakeholders Modular System Architecture	There is no content in this space.
Collaboration Practices (ind. 15.1)	
185.12.5.114/node/131/map	

Figure 27. Screenshot showing how to go back to the SecInCoRe OpenAtrium sitemap





In order to be able to contribute to a space, a user must request to join the space, and the space administrator must approve the user's request.

S	lecInCoRe
	Common Information Space (CIS) concept documentation 🗸 CIS Specification 🗸
	Are you sure you want to join the group CIS Specification?
	Request message
	I would like to join this space, so I can contribute to the <u>QIS</u> specification.
	This is the text a user may send to the group administrators.
	Join Cancel
	Cancer

Figure 28. Screenshot showing how to join a SecInCoRe OpenAtrium Space

In order to be able to add content to a space, the space must contain the appropriate content sections. These can be seen under the space drop-down menu or alternatively, by clicking the section tab under the menu breadcrumb ribbon bar. There exist 4 section types.

- 1. Discussion used to discuss a given topic. This is analogous to a traditional forum. Please do note that OpenAtrium allows for this functionality under any content type, for example a document page, a calendar event or a media upload.
- 2. Calendar used for scheduling events
- 3. Documents used to create static web pages
- 4. Files used to upload files and documents
- 5. Tasks used to generate a list of 'todo' items







Figure 29. Screenshot showing SecInCoRe OpenAtrium Section navigation

If a user is on the Space landing page, then by clicking the '+' icon in the top-right corner of the ribbon bar, they will be able to create a piece of content, which will automatically be filed in the corresponding section. If a user is browsing a specific section, then the '+' icon will only offer the option to add a piece of content relevant for that section, for example if browsing the calendar, it will offer the option of creating a new event or if browsing the Documents section, it will offer the option of creating a new Document page. If more than one Document section exists in this space, the user will be able to choose where the document is filed.



Figure 30. Screenshot showing how to add content to SecInCoRe OpenAtrium





The example below shows the creation of a new Document. A document is given a title and the user is presented the option of adding content to the body of the document.

SecInCoRe	
ELSI ELSI Documents	+ 0 ★ Q → Peter Gray
SI Calendar 👒 ELSI Discussion 🔁 ELSI Documents 🗁 ELSI Files 😂 ELSI Guidelines Prototype 3 🐼 ELSI T	Fasks ELSI Timeline
Open issues	× Cancel
Open issues	Notifications
Body (Edit summary) WYSIWYG Enter the content of the document or wild here. WYSIWYG B I S E E E E E E E E E E E E E E E E E E	Groups Teams Users
Do we need a rating system? What are the pros and cons. What type of rating system? Do we want to include a disaster myth buster? E.g. people don't panic. There is no disintegration of public order.	Do not send notifications for this update.
Show page instead of file? If checked, show the node detail page (Drupal default behavior). If unchecked, show the first file attachment. Attachment	Save Unpublish View changes

Figure 31. Screenshot showing the add Document screen

OpenAtrium offers powerful content node visibility and notification options. The content can be made visible to all site users or only to space members. Notifications can be set at the group, team and user level. A link to the document can be made visible in the section drop-down menu, and the parent section where the document is to be placed can be specified. This allows for content to be moved around the various OpenAtrium spaces and sections.

Depending site-wide or space-wide access policies, content can be modified by all members of a space, or only the content creator. This can be further segmented by specifying several tiers of roles, for example members, non-members, editors, admins etc. with extremely granular permissions being made possible by OpenAtrium.





Group visibility *	
Public - accessible to all site users	
Private - accessible only to space members	
Featured image	
Choose File No file chosen	
The Image associated with the Space	
Files must be less than 2 MB. Allowed file types: png gifting ineg	
Automed me types, prig an jpg jpeg.	
Notifications	
Groups	Publishing options
× SecInCoRe consortium members - 7	Create new revision
Teams	Test content Should this be considered test content? If checked, this
	will be deleted/reverted when sandbox mode is turned off.
Users	
× Monika Buscher - 9	Authoring information
Do not send notifications for this update	Author
	CSchaefer O
	Date 12/02/2015
Menu options	E.g., 02/25/2016
Provide a menu link	Time 09:09
Link title	E.g., 17:17
ConOps for Cloud Emergency Information System (CEI	
Parent	Save Unpublish View changes
CIS concept	

Figure 32. Screenshot showing the various options on the 'add document' screen

Powerful content layout functionality using OpenAtrium's 'paragraph' feature

OpenAtrium offers significant layout benefits above a standard Drupal CMS deployment. Below the main body field, there are four additional 'paragraph' buttons. Paragraph sections are subject to ACL policies, meaning that content will not be shown to users who do not have the appropriate required rights to view the requested content.



The paragraph types available at the time of writing are:

1. Add text





D5.3 Validation Strategy, Version 2 (ic) **Public deliverable**



A text paragraph works just like the normal Body field, with the added benefits of being able to specify how the text flow is rendered. For example, the text can be rendered in two or three column layout, or even as floating 'callout' boxes.

ecli	nCoRe	
* -	Common Information Space (CIS) concept	ConOps for Cloud Emergency Information System (CEIS)
		0 * Q +
		Notifications
		Groups
⊕ те	əxt	WYSIWYG Teams
В		
Or in Th ma	he important issue of SecinCoRe is to ensure sustainabilit addition, the SecinCoRe CIS concept is even more than in ierefore, a major concept for next generation emergency anagement systems utilizing the results of SecinCoRe has	will yo f all results during and after the project and in implemented in the demonstration cases. Users y management information and resource has to be elaborated (cp. [DOW]). For that Do not send notifications for this update.
pu of de	rpose a so-called Concept of Operations (ConOps) is dev storytelling, which is explained in the following. In order to scribed here. The term Concept of Operation is defined b	Ieveloped. This will be based on the methodology to avoid misunderstandings the main terms are d by the "European Organisation for the Safety of Menu options
Lay	out	Provide a menu link
3	column	Link title
4		ConOps for Cloud Emergency Information System (CEI
		Parent
6		CIS concept

Figure 33. Screenshot showing the 'Text' feature of the 'paragraph' module within OpenAtrium. Note the Layout option.

SecInCoRe			
Common Information Space (CIS) concept	ConOps for Cloud Emergency Information	tion System (CEIS)	ଡ \star ସ
ConOps for Cloud	d Emergency Inforr	nation System (CEI	S) Amembers &
One important issue of SecInCoRe is to ensure sustainability of all results during and after the project and in addition, the	For that general purpose use cases describe steps of interactions between a stakeholder and the concent or well as internel	selection of main stakeholders has to be performed. Both modules are mentioned in one-step, since it is hard to neglect the inter-	Public
SecInCoRe CIS concept is even more than implemented in the demonstration cases. Therefore, a major concept for next generating memory management	processes in the concept to answer the stakeholder's request. Later, these specify the use of the concept in an ex-post	dependencies between relevant stakeholders and the considered situation. One important aspect to be regarded is the description of significant details for defining	Request space membership
information and resource management systems utilizing the results of SecinCoRe has to be elaborated (cp. [DOW]). For that	scenario in more detail. In [CAC06] several methods (textual, UML-based, etc.) are described for deriving use cases.	One important aspect to be regarded is the description of significant details for defining the situation and the stakeholders, so that challenges can be derived from those. For a first approach, it is important to identify	There is no content in this space.
purpose a so-called Concept of Operations (ConOps) is developed. This will be based on the methodology of storytelling, which is	Methodology for use case definition	relevant situation elements in terms of a story and the relevant roles involved within. In this example the main stakeholders are:	
misunderstandings the main terms are described here. The term Concept of Operation is defined by the "European	In order to enable an adjustable, module- based and combinable approach for use case definition the use cases comprise	"Crisis management staff Coordination groups FR commanders FR on-site command staff"	
Organisation for the Safety of Air Navigation (EUROCONTROL)" in the "European	"modules" in the following. These are similar	and the situation is as follows:	
Operational Concept Validation Methodology (E-OCVM)" and based on the term "Operational Concept". Due to the	 but more concrete than the common description of scenario elements by Sutcliffe in [Sutc98, p. 51ff.]: 	"In disaster situations which a) last for a longer period time or which imply side- effects for such a period of time and b)	
orientation of EUROCONTROL an Operational Concept and a Concept of Operation are defined as follows:	 Situation: This includes all descriptions relevant to define the boundary conditions of the use case. 	which are related with some complex background in terms of meteorology, technology, natural sciences, population,	
"An Operational Concept is seen as a high- level description of ATM IAir traffic 12.5.114/comps-cloud-emergency-information-system-ces#	 Main stakeholders: People important or relevant respectively and involved in a use case. In a first use case 	environment etc. (flooding, earthquakes with after-shocks, leakages in critical infrastructures) it is current practice to	

Figure 34. Screenshot showing how the 'paragraph' module formats the 'Text' type, according to the 3 column layout

2. Add Media Gallery







The 'media gallery' can replace the normal attachments feature, with each 'media gallery' paragraph containing one or more images, videos or files. This paragraph type can have layouts selected, controlling how media is displayed. Options include left / right floating regions, a grid gallery of media. Videos can be embedded as a preview image, as well as a fully functioning video player.

3. Add Snippet



The "Snippet" paragraph type allows you to embed text from any other content on your site. You can specify whether the Summary, Body, or full Node is embedded and also control the Layout the same as with Text paragraphs. You can also either display the Title of the referenced content or hide the title, or override the title with your own text.

By "locking" the snippet to the old revision, the old document will continue to display the original SOP even if the SOP is updated later. If you "unlock" the snippet, then it will display the latest version of the related SOP.

One of the best features of Snippets is the ability to lock which revision you want to display. Open Atrium access controls are also respected when displaying snippets. If you reference content that the user doesn't have permission to view, that snippet will be removed from the displayed text. Users still only see the content they are allowed. This provides a very powerful way to create rich documents that contain different snippets of reusable content for different user roles and permissions.

4. Add Related Content



This feature allows for other content types within the OpenAtrium platform to be referenced and inserted into the current document. It can display either a summary or the full content of another document. This includes all of the referenced document's functionality. For example referencing an external discussion will show all the discussion replies and provide a reply form, or a referenced document containing a media gallery will also shown in full.





Notes about adding content in OpenAtrium:

When floating paragraphs to the left or right, the text from other paragraphs will flow around it, just as if the media had been embedded into the WYSIWYG. To move floating paragraphs, for example images or callout text to a different location in the document, simply drag the paragraph up or down the sequence of paragraphs within the document.

It is important to note that in Open Atrium, images directly embedded into the Body WYSIWYG field becomes Public, bypassing the normal OA access control rules. However, anything added to a Media paragraph works more like the Attachment field and properly inherits the access permission of the story document being created. Thus, the Media paragraph provides a way to embed Media within documents, while retaining proper privacy permissions.





9.6 Appendix 6: questionnaires and focus group guidelines mentioned in the text of the Deliverable



SECURE DYNAMIC CLOUD FOR INFORMATION, COMMUNICATION AND RESOURCE INTEROPERABILITY BASED ON PAN-EUROPEAN DISASTER INVENTORY

Internal validation of the ELSI based on D2.3

Simona De Rosa, Antonella Passani T6 Ecosystems

July, 2015

Work Package 5

Project Coordinator Prof. Dr.- Ing. Rainer Koch (University of Paderborn)

7th Framework Programme for Research and Technological Development COOPERATION

SEC-2012.5.1-1 Analysis and identification of security systems and data set used by first responders and police authorities







The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n°607832.

Authors



T6 Ecosystems

Simona De Rosa Email: <u>s.derosa@t-6.it</u>

Antonella Passani Email: <u>a.passani@t-6.it</u>

Introduction to the survey

As part of SecInCoRe, T6 Ecosystems srl is conducting a survey addressed to the SecInCoRe partners in order to validate ELSI through D2.3.

Before starting filling-in the questionnaire, please read the entire D2.3. However, please notice that you will find texts extracted from the D2.3 that will help you answering to the questions.

We estimate that the survey will take about 45 minutes to be completed.

Please answer all questions from the viewpoint of your organisation.

Please answer each question by ticking the appropriate answer(s) or providing your answer in the designated space.

In case some questions are not clear, or show aspects you think are not relevant, please list us your suggestions/opinions to help us improving the questionnaire. Feel free to add comments after the text of the question where you think they need to be improved.

Please, rename the file by adding your initials and send the filled-in questionnaire to <u>s.derosa@t-6.it.</u>

The deadline fixed to receive the questionnaire is August 21st. If you cannot meet this deadline, please inform as asap and propose a new deadline (before the Athens meeting) so that we will not disturb you with reminders.





Thank you for the time you dedicate to this survey! In case you need any support or clarification please contact Simona De Rosa at <u>s.derosa@t-6.it</u> or Antonella Passani at <u>a.passani@t-6.it</u>

Internal validation on D2.3

Name and Surname	 	
Institution		

D.2.3 goals and needs

"The goals of the research so far have focused on determining what is needed (in terms of common data sets, guidelines, sharing initiatives, technology, etc.) in order to design ethically aware socio-technical practices in disaster IT interoperability, including the value of examining practices in situ – in location, in practice, and towards specific ends (Dourish, 2001; Suchman, 2007)" (p.12 D2.3)

 Analysing the deliverable, how do you assess the capacity of the deliverable to determine what is needed in designing ethically aware socio-technical practices?
 Please attribute a value from 1 to 6 where 1 is "totally unable" and 6 is "highly capable"

"As part of the design of this research, we were well aware that it is impossible to gain sufficiently rich understanding of emergent practices and conventions of information sharing through studies of potential users, use contexts, or technologies alone. Consequently, to better understand how problems are formulated, needs expressed, or solution envisioned, we have been employing inventive and mobile methods like co-design, participant observation, and go-along to help make visible these otherwise unknowable practices, opportunities, and consequences (Bellotti et al., 2002; Brigham & Introna, 2007; Büscher, M., Urry, J., Witchger, 2011; Dourish & Bell, 2011; Lave, 1988; Lury & Wakeford, 2012). This way, we aspire to produce both discursive and practical co-realisation of socio-technical futures (Hartswood et al., 2008) in a way that can inform practice, design, and policy." (p.12)

- 2. Do you agree with the methods envisaged to derive final conclusions on emergency services?
 - Yes
 - □ No (If not, how do you suggest to improve it?)

Data Protection





"In the development of technology and in the undertaking of research, it is essential that the SecInCoRe project upholds legal standards relating to data protection in order to protect the privacy of end users and stakeholders." (p.15)

- 3. At the current stage of the project, do you think that SecInCoRe is going in the right direction in order to protect the privacy of direct users and stakeholders?
 - Yes
 - □ No (If not, how do you suggest to improve it?)

4. To what extent does this deliverable provide useful info in this regard? Please attribute a value from 1 to 6 where 1 is "totally useless" and 6 is "extremely useful"______

Actions at the scenes

"We have also found that the needs for translation are greater than expected. While the translation of language and terminology was expected, it also appears that we need translation of roles, procedures, expectations, and technological standards." (p.34)

5. According to your experience in the sector, how do you judge the need for translation?
 Please attribute a value from 1 to 6 where 1 is "totally useless" and 6 is "extremely

useful"

6. Particularly, do you think that translations will constitute a key asset of SecInCoRe outputs?

Please attribute a value from 1 to 6 where 1 is "totally useless" and 6 is "extremely useful" (If you assign 3 or below, please describe why)

Information analysis during operations

"One of the things SecInCoRe needs to do is examine in greater detail the relationships between information exchange and evaluation at the scene, in the EOCs, during the planning as an operation begins, and planning once the initial 48-72 hours are over to better understand how data provided within a CIS becomes both trusted and relied upon." (p.35)

"SecInCoRe needs to better understand how these risks assessments take place in order to understand what new kinds of information could enhance these assessments in





invaluable ways and to avoid adding more information that simple increases the number of questions to be asked." (p.36)

- 7. Do you agree with both quoted points?
 - □ Yes
 - No (If not, please explain why_____)

Report on users goals

Looking at the section 6 "Report on user goals", please give a look at all sub-sections and answer to the following questions:

8. Do you agree with affirmation in the section Sharing and Trust?

Please attribute a value from 1 to 6 where 1 is "totally disagree" and 6 is "totally agree".

- 9. Do you agree with affirmation in section the re-emptive? risk assessment/ethical foresight? Please attribute a value from 1 to 6 where 1 is "totally disagree" and 6 is "totally agree".
 - _
- **10.** Do you agree with affirmation in the section Need to manage formal with informal, frameworks with improvisation?

Please attribute a value from 1 to 6 where 1 is "totally disagree" and 6 is "totally agree"._____

- **11.** Do you agree with affirmation in the section Inclusiveness? Please attribute a value from 1 to 6 where 1 is "totally disagree" and 6 is "totally agree"._____
- **13.** Do you agree with affirmation in the section Simplicity and Transparency? Please attribute a value from 1 to 6 where 1 is "totally disagree" and 6 is "totally agree"._____
- **14.** Do you agree with affirmation in the section Diversity? Please attribute a value from 1 to 6 where 1 is "totally disagree" and 6 is "totally agree"._____
- **15.** Do you agree with affirmation in the section Access and equality? Please attribute a value from 1 to 6 where 1 is "totally disagree" and 6 is "totally agree"._____





- 16. Do you agree with affirmation in the section Aligning local and distributes meaning making? Please attribute a value from 1 to 6 where 1 is "totally disagree" and 6 is "totally agree".
- **17.** Do you agree with affirmation in the section Need for democratic accountability and human rights protection?

Please attribute a value from 1 to 6 where 1 is "totally disagree" and 6 is "totally agree".

Summary of ELSI, based on first EIA and PIA

18. How do you judge the level of utility of EIA and PIA's exercises?

Please attribute a value from 1 to 6 where 1 is "totally useless" and 6 is "extremely useful"_____

- 19. Do you think that the following list is exhaustive?
 - □ Yes
 - No (If not, what is missing?)_____

"The consortium members identified a list of ethical issues with which they were already familiar, including: (p.43)

Access Diversity Dignity Protect against discrimination Security and managing of sensitive data Anonymity Professional Integrity Accountability Fairness"

Practical recommendations Build the system in a way that enables trust

According to following texts, to what extent do you agree with following sentences?

20. "According to almost all the interviewees, trust comes from getting to know people. SecInCoRe has to balance the technological interactions with the needs for social interactions".

Please, attribute a value from 1 to 6 where 1 is "totally disagree" and 6 is "totally agree"_____

21. "There is also the need to help establish/make accessible sharing protocols, since these protocols that help establish methods for data protection that make sharing secure and trustworthy. In this way the system has to actively





encourage legal compliance in ways that make it conscious for those engaging with the system and the data."

Please, attribute a value from 1 to 6 where 1 is "totally disagree" and 6 is "totally agree"_____

22. "The system needs to be technologically reliable for data to be entrusted to it and practices to be consistent with it. Moreover, there is a need to design CIS such that users do not perceive a loss of control. Doing so will create tensions and become a barrier to interoperability and potentially lead to data protection as a false excuse for not sharing."

Please, attribute a value from 1 to 6 where 1 is "totally disagree" and 6 is "totally agree"

- 23. "The system should be built in a way that acknowledge the balance between verbal/face-to-face and text/automation, as it is this balance that establishes trust and accountability between the two ends of the communication practices." Please, attribute a value from 1 to 6 where 1 is "totally disagree" and 6 is "totally agree"
- 24. "There is a need to gather the capabilities of all stakeholders in ways that are translatable. Without understand what other groups can do and should do, it is difficult to know what kind of data security measures need to be in place, impeding either sharing or protection. We need to gather expectations of one group from another in order to create stronger links between them, so it becomes clear whose role it is to ensure data protection."

Please, attribute a value from 1 to 6 where 1 is "totally disagree" and 6 is "totally agree"_____

25. "We need to provide guidance for users to know who to talk to in order to initiate new working relationships. Without such knowledge, data can travel through indirect pathways making protection and privacy more challenging than necessary."

Please, attribute a value from 1 to 6 where 1 is "totally disagree" and 6 is "totally agree"_____

26. "We also need to draw upon commonalities in crisis management models to aid translation and provide an information framework that does not force one agency to adopt another agencies approach but instead helps to understand (for us in terms of design needs and for our users in terms of why some data should and shouldn't be shared in a given circumstance) how the variations in the models lead to different data uses and when/who to communicate with in other agencies."

Please, attribute a value from 1 to 6 where 1 is "totally disagree" and 6 is "totally agree"_____

27. "For any of this to be successful, we need to help make accessible different conception of / perspectives on risk."





Please, attribute a value from 1 to 6 where 1 is "totally disagree" and 6 is "totally agree"_____

28. "SecInCoRe needs to develop, at minimum, guidelines for data use as it is being moves around various users over time. It also needs to manage the shifting roles that occur as incidents unfold to deal with changes in decision-making roles between agencies that lead to changes in data controllers and processors."

Please, attribute a value from 1 to 6 where 1 is "totally disagree" and 6 is "totally agree"_____

29. "We need to understand how major incidents are declared and the implications of those processes and their differences from incident to incident and from nation to nation."

Please, attribute a value from 1 to 6 where 1 is "totally disagree" and 6 is "totally agree"_____

30. "A challenging task for SecInCoRe is to create a framework that clearly defines the communication roles. To support such a framework, it needs to include knowledge of the different stakeholders, perspectives, and expectations that comprise the emergency practices."

Please, attribute a value from 1 to 6 where 1 is "totally disagree" and 6 is "totally agree"_____

31. From your point of view, what is the more critical aspect that have to be taken into account from practical recommendations? Please, provide a description

Final questions

Considering D2.3, please indicate to what extent do you agree with the following sentences by attributing a score from 1 to 6 where 1 is "I totally disagree" and 6 is "I totally agree". If you select 3, or values lower than 3, please describe why.

D2.3 defines useful concepts for the creation of the SecInCoRe socio-technical system	1	2	3	4	5	6
Which ones?						
D2.3 offers practical advices that will be implemented in the creation of the system	1	2	3	4	5	6
Which ones?						





					I	I
D2.3 stress out major issues that have to be taken into account during next steps of the project	1	2	3	4	5	6
Why? How?						
Other (please specify)	1	2	3	4	5	6
Why? How?						



D5.3 Validation Strategy, Version 2 (ic) **Public deliverable**





SECURE DYNAMIC CLOUD FOR INFORMATION, COMMUNICATION AND RESOURCE INTEROPERABILITY BASED ON PAN-EUROPEAN DISASTER INVENTORY

Internal validation of the Pan-European inventory based on D2.1

Simona De Rosa, Antonella Passani T6 Ecosystems

July, 2015

Work Package 5

Project Coordinator Prof. Dr.-Ing. Rainer Koch (University of Paderborn)

7th Framework Programme for Research and Technological Development

COOPERATION

SEC-2012.5.1-1 Analysis and identification of security systems and data set used by first responders and police authorities







The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n°607832.

Authors



T6 Ecosystems

Simona De Rosa Email: <u>s.derosa@t-6.it</u>

Antonella Passani Email: <u>a.passani@t-6.it</u>

Introduction to the survey

As part of SecInCoRe, T6 Ecosystems srl is conducting a survey addressed to the SecInCoRE partners in order to validate the Pan-European inventory through D2.1.

Before starting filling-in the questionnaire, please read the entire D2.1. However, you will find texts and tables extracted from the D2.1 that will help you answering to the questions.

We estimate that the survey will take about 45 minutes to be completed.

Please answer all questions from the viewpoint of your organisation.

Please answer each question by ticking the appropriate answer(s) or providing your answer in the designated space.

In case some questions are not clear, or show aspects you think are not relevant, please list us your suggestions/opinions to help us improving the questionnaire. Feel free to add comments after the text of the question where you think they need to be improved.

Please, rename the file by adding your initials and send the filled-in questionnaire to <u>s.derosa@t-6.it.</u>

The deadline fixed to receive the questionnaire is August 21st. If you cannot meet this deadline, please inform as asap and propose a new deadline (before the Athens meeting) so that we will not disturb you with reminders.

Thank you for the time you dedicate to this survey! In case you need any support or clarification please contact Simona De Rosa at <u>s.derosa@t-6.it</u> or Antonella Passani at <u>a.passani@t-6.it</u>

Internal validation of the Pan-European inventory based on D2.1



D5.3 Validation Strategy, Version 2 (ic) **Public deliverable**



Name and Surname_

Institution

Internal Validation on:

- 1. Pan-European inventory: concept and development
- 2. Pan-European disaster inventory: concept and development

Pan-European inventory: concept

Please read the following text about the inventory and answer to the questions.

"The inventory could, firstly, be purely a more gualitative and detailed database of past disaster events than existing resources. An example of use would be an emergency response agency in the process of developing new emergency plans, turning to the inventory to understand the breadth of and real world unfolding of potential risks and to learn from past experiences to formulate the best possible plans. Or, in a more dynamic scenario, a group of first responders actively engaged in a mission may be faced with a potentially toxic chemical spill. They could search the inventory for potentially similar cases and glean information about lessons learnt, crisis management models employed, stakeholders involved, and so on. Secondly, the inventory could include access to a library of past disaster reports and other bibliographic resources that its entries are based upon, enabling users to follow up research. Some of these resources may be openly available, others only on a basis of subscription or special request. Thirdly, the SecInCoRe Pan-European inventory could be a community resource, initially set-up, managed and monitored by the SecInCoRe project and adopted by the ERC or CRED or similar organisation, where interested parties can contribute under the guidance of experts, as well as being granted access to the information. Examples of use would include the above, but also contributions, such as response agencies providing information about past events, difficulties, their causes and solutions found during the response to a disaster, which had not been captured by official after-action reviews or which had been represented only partially, but which allow important lessons. Thirdly, the SecInCoRe Pan-European inventory could also be a gateway to data that are referred to in the inventory, utilising advanced ICT to support construction and maintenance of temporary shared information spaces. A use example would be reference to the inventory by a response agency during the response or recovery phases of a disaster, discovery of useful open or proprietary or otherwise closed datasets, and the ability to access such data either directly or request access by following links." (D2.1, p.218-219).

- In your opinion, how clear is the idea of the inventory? Please attribute a value from 1 to 6 where 1 is "totally unclear" and 6 is "perfectly clear".
- 2. What do you think it is the strongest aspect offered by the inventory?





	Please, description	provide	a
3.	What do you think is Please, description	the weakest aspect offered by the inventory? provide	a
4.	In your opinion, who responders, etc.)	will be most interested in the inventory? (Governr civil	nent, first society,
5.	What do you think is Please, description	missing in the design of the inventory? provide	a
6.	What is, in your opinion Please, description	on, the most innovative aspect of the inventory? provide	a





Pan-European inventory: development

Please read the following text about what the inventory will contain.

"Thus any inventory needs to consider **stakeholders** within first responder agencies and police authorities, but also consider how they may collaborate with other actors. Second, a range of **information management processes** need to be included in the inventory, specifically trends and constraints in the deployment of **crisis management models**, **information systems**, **data-sets used**, **and information flows** such that it becomes possible to see their relationship to successes and difficulties faced at times of interoperability. Technical and organisational interoperability is often deeply affected by the **business models** that underpin disaster response (...) We also develop a discussion of a set of **ELSI** related challenges and opportunities, where consideration as part of the inventory design can significantly add to the usefulness and value of the inventory." (D2.1 p.182).

According to the categories underlined in the text:

- 7. To what extent different types of stakeholders need to be included in the inventory? Please assign a value from 1 to 6 where 1 is "we can exclude it" and 6 is "absolutely central in the inventory"_____
- 8. To what extent different types of information management processes need to be included in the inventory? Please assign a value from 1 to 6 where 1 is "we can exclude it" and 6 is "absolutely central in the inventory"_____
- 9. To what extent different types of crises management models need to be included in the inventory? Please assign a score from 1 to 6 where 1 is "we can exclude it" and 6 is "absolutely central in the inventory"_____

To what extent different types of information systems need to be included in the inventory?
 Please assign a score from 1 to 6 where 1 is "we can exclude it" and 6 is "absolutely central in the inventory"______





- 11. To what extent different types of data-sets used need to be included in the inventory? Please assign a score from 1 to 6 where 1 is "we can exclude it" and 6 is "absolutely central in the inventory"_____
- 12. To what extent different information flows used need to be included in the inventory? Please assign a score from 1 to 6 where 1 is "we can exclude it" and 6 is "absolutely central in the inventory"_____
- 13. To what extent business models need to be included in the inventory? Please assign a score from 1 to 6 where 1 is "we can exclude it" and 6 is "absolutely central in the inventory"_____
- 14. To what extent a set of ELSI need to be included in the inventory? Please assign a score from 1 to 6 where 1 is "we can exclude it" and 6 is "absolutely central in the inventory"_____
- 15. What kind of information do you think have to be added to the inventory? Please, provide a description_____





Please, read carefully the table below before answering to the following question.

16. How relevant do you judge each criteria envisaged for ach theme? Please use the last column on the right for attributing a value from 1 to 6 where 1 is "not relevant" and 6 is "very important". Please do so for all the criteria listed in the table.

Theme	Summary of Issues	Criteria for inventory	Provide
			a score
Stakeholders	General Conclusion: not all stakeholders are at the scene of the disaster nor are first responders the only stakeholders that should be considered in an inventory of this type		
	Informally organised local community members are often involved in responding for quite a while	Include these stakeholders, how they helped, and why they were needed	
	Governments cannot address all socio-cultural issues and rely on outside help	1. Include data about their actions as well as have portions of their data that are available to such groups	2.
	Who is including changes what data is used and when.	should track what kind of data is regularly maintained by the different stakeholders	
	Issues of different terminology/jargon	specifics about the broader range of potential stakeholders and a general list of their disaster response terms	
	Different priorities, values, and requirements for trust.	Includes different stakeholder priorities and foci for specific disasters	



D5.3 Validation Strategy, Version 2 (ic) **Public deliverable**



	Different privacy and liability needs	Cannot assume all data is equal. Need to consider ethical implications of sharing data within the inventory	
Crisis management models	General Conclusion: not all use command and control, and those who do not interpret it in the same way		
	There exist a seemingly endless number of plans that derive from the general command and control model, plans that the cases demonstrated to not automatically synchronize	Need to document the variations, not just general plans. This needs to include the scalability of each plan as well as who is expected in partnership for each plan	
	Plans cannot always foresee all the agencies involved and leave roles unclear	Need to record who is involved, in detail, during given disasters to help future plans be more complete	
	The same terms are used to reference different procedures or decision- making positions in different plans	Need detailed definitions of and relationships between positions of responsibility as well as levels and scale of action for each plan	
	The existence of a common model does not imply plans exist for all situations or that one generic plan will provide guidance for crisis management during all disasters	Need to record the range of plans that exist within each country to identify gaps in other locations. It also needs to include disaster cases where different standards and plans were enacted but struggled to be made interoperable	
	ICS system does not offer much flexibility for quick change, so at times is not easily scalable or adaptable to unknowns.	Including details about models and disaster events and plans can help make visible the different potential needs and allow future users to use data to build greater flexibility into their plans	





	Not everyone operates on command and control	Need to have cases that demonstrate the variety of plans and procedures (and specifics about their frequent incompatibilities both horizontally and vertically) that are derived from the same model	
	Plans that include liaisons that regularly work with multiple agencies are more successful	Need to record when liaisons are used and why	
Data-sets	General conclusions: equally as important as the content of the data or the hazard during which it is gathered are details about how it is used, who gathers it in different circumstances, and why it could be useful. Moreover, there is no one set of rules for data gathering		
	What actually gets used during a disaster is very situation-dependent	If grouped, it should not be by hazard but by the function the data plays The inventory should track background data, level for detail, used as well	
	Sometimes a data-set works for one group but not another	The inventory should be searchable for cases such as these, when typical patterns of data-set collection did not work, their causes, and their solutions	
	Some data-sets were only referenced as lessons learnt	Should not just limit inventory to data sets already determined to be effective	
	Some data sets are available but not tested/proofed and often don't make it into the formal incident reports	The inventory needs to draw on more than just incident reports and be sure to include both what is mentioned in academic	





		research on the disasters, in the media, and in social media	
	How and who does the gathering matters as much as the data content itself	The inventory needs to include not just what data sets but who is responsible for gathering in different circumstances. It also needs to track the procedures for such shifting of responsibilities	
		The inventory should note when data-set was gathered and the frequency and longevity of the related data-sets	
	Circumstances for public access to the data-sets are not set in stone, but important to consider when gathering the data	Details about the reasoning and effects of public release need to be recorded	
	It is much easier to gather economic statistics than data on the impacts on residents	The inventory needs to address this disparity of data in order for responders to better serve the needs of victims that cannot be reduced to numbers	
	Much of this data is not in numerical form, but also in video, figures, maps, forms equally as helpful as	The range of formats that the data set is gathered in should be recorded along with data type	
	numbers.	The inventory needs to set up a search system that is capable of managing searches of multiple data format within a single search	
	Different things can be asked of the same data-set	The inventory should record to what uses the data is put (what information it is transformed into)	
Information			



.

D5.3 Validation Strategy, Version 2 (ic) **Public deliverable**

T



Systems			
	Too generic to structure use	Need record how generic systems were used in specific situations (both in terms of data gathered and products produced)	
	Too local to become integrated	Need to list local systems to understand how they structure information to see the potential for flexibility and collaboration	
	Mobile resources are vital to these system functioning	Need to collect when and in what formats access to information in the field was used. Also need to collect when such systems failed or were inaccessible to predict the limitations of any given system	
	Use patterns are hard to break	Need to include details of why an older system is still in use to help understand why their users might not transition to a new system. It should also take note to why a new system gets adopted	
	Sparsity of information from reports	Cannot rely on reports alone for Information systems data or criteria for the inventory	
Information Flows	General conclusion: it cannot be assumed that working under the same model, or even the same plan, will automatically lead to unproblematic information flow		
	Different stakeholders will have different flows. These will also vary by country, region, and potentially even hazard.	Track flow plans modifications as a disaster shifts scale Track when modifications are requested to the information flow, either	





		during a response or recommended after the response and why they were necessary	
	Different data sets have different flow patterns	Record electronic notification systems, data repositories, and criteria for specific data sets to flow to the next stakeholder/decision- maker	
	Different information systems encourage specific flows.	The inventory needs to track both flow nodes and pathways, the security and restrictions at each, and who uses which ones	
	Side-channels do and will exist	Case studies should be included that relied on such side channels for their operations and explanations for their uses should be included	
		Document such cases where personal mobile phones get used, including what technology was supposed to be used or why the data could not follow formal pathways	
		Data for the case studies needs to come from stakeholders involved in these side channels, news reports, and interviews with the individuals involved in establishing the side- channels.	
Interoperability	General Conclusion: the ability for different groups to work together depends upon everything from data format to definitions of risk to how much is shared at once		
	The ability to share data	In what format is data	





affects all potential	collected and stored.
communications and collaboration	It also needs to be able to search for different data combining success and problems.
	At what scale/resolution is data collected
	How often is the data collected
How the data will be shared matters	the inventory needs to connect information about data type with information system and flow.
	What are the standard use procedures and protocols
	Need to look at disasters that successfully employed other methods of communications. Need also to collect cases when phones were relied upon to understand why they were used rather than an alternative to incorporate into our system whatever need it is they serve.
	needs to collect data about situations in disasters where responders successfully employed methods of communication other than phones and radios
As data is shared it moves from one decision-making process to another and the criteria for assessment and	Collect the questions asked by each agency/organization of the data they use.
definitions of usefulness frequently change	Collect information about what each agency considers at risk during a disaster and how threat is defined for different hazards.





	too much data is shared at once, overloading the system.	Collect moments when systems get overloaded, why, and what creative solutions were provided.	
	liaisons or a physical centre are vital to interoperability to help align priorities, goals, and terminology	The inventory needs to record situations when these actors or places were described as vital and what problems they solved.	
		The inventory needs to produce a translator software or employ a common language for all data.	
	The MOUs between groups are as important as data format and technologies of exchange.	Need to collect MOUs at multiple different scales (national, regional, city)	
	Who has access affects the ability of different groups to be on the same page and trust each other.	Collect typical accessibility patterns for data types by region. Designing the inventory in a way that is accessible to a wider range of stakeholders can improve communication and information flow in the future.	
Business Models			
	Academics are frequently expected to provide basic data, research, and analysis during disaster response.	An inventory should include not just the data and information systems academics are involved with, but the role of the institutions in the larger response process.	
	the regional and higher scale plans would be written with intentional gaps and cannot be relied upon to structure the form interoperability or collaboration will take.	SPEDI needs to record all stakeholder business models.	





	Focusing only on first responders or government response in general will often miss major decision-making stakeholders, would not adequately define the crisis management models in use, nor would offer a complete picture of the information systems required for a response.	Business models beyond government partnerships need to be explored.	
	Interdisciplinary relationships are necessary	Inventory should be able to be accessible to both public and private actors in such a disaster response.	
	Outsourcing is becoming increasingly common in emergency response.	The inventory needs to be searchable by business model so users can compare the different situations and results.	
	Increase reliance by emergency responders upon private data providers	The inventory needs to track where data comes from and how it is obtained. It also should track successes and failures in the use of private data.	
ELSI	General Conclusions: A wide range of ELSI to do with the exceptional nature of emergencies, fairness, autonomy, dignity, liability and responsibility arise. These can be divided into emergency, information and technology ELSI to derive some key factors to inform the design of a disaster inventory.		
	More than numbers. Beyond money and life	There is a need for diverse qualitative information about past disaster events and response efforts, beyond	





	economic impacts and numbers.	
Fair representation, Inference, Including the excluded Careful Categorisation Trust in Data	Stakeholders and events should be represented fairly and truthfully, in ways that can be validated, supporting trust and cooperation.	
Long term and indirect effects	The full range of effects should be reported.	
Exceptionality of exceptions	An overemphasis on the exceptionality of disasters can cloud responsibilities to predict and prepare.	

Considering the following table on data-set collected during disasters (contained in D2.1, p. 201) please answer to the following questions.

General Incident Data	
Number ill/injured	
Number deaths	
Number damage buildings	
Damaged infrastructure	
Damaged property	
Insurance claims	
Hazard details (like earthquake ma crash location)	agnitude, fire perimeters,
Evacuation orders/persons	
Shelter locations, statuses, and evacu	lees in each shelter
Timeline of events	
Number and type of aid requests	
Staging locations	
ICP/Command centre locations	
Affected responders	
Public Health information	
Active investigations/questionnaire an statuses	nd case study results and
Food/water safety test results	
Scientific models of toxin spread	
· · · · · ·	



D5.3 Validation Strategy, Version 2 (ic) **Public deliverable**



Patient	Health information
	Number patients at each hospital
	Patient diagnoses
	Blood test results
	Finger print databases
Materia	al resources
	Hospital resources
	Food/water resources
	Transportation
Worker	ſS
	Hospital staff. specialty, training
	Emergency responders in the field, time worked
	Tasks assigned
	Unit from
Enviror	mental data:
	Hazard zones
	Weather
	Hazardous materials
Econor	mic data
	Business income gains/losses
	Affected businesses
	Response expenditures
Spatial	data
opana	Demographics
	Cultural heritage/points of cultural value
	Topographic data
	Mobile phone data
	Power infrastructure
	Transportation infrastructure
	Staging locations
	Command centre locations
	Doints of specific action (like active fire line fighting or police)
	blockades)
	Travel restrictions
	Water authorities
	vvalet authonites
	Junsaictional boundaries
	Responsibility zones
	Evacuation routes




Communication		
	warning provided	
	call-outs	
	evacuation orders	

- 3. How do you assess the completeness of the list? Please, indicate a value from 1 to 6 where 1 is "not complete" and 6 "is fully complete"_____
- 4. Referring to the previous table, if any, what kind of data do you think have to be added to the list?





5. Pan-European disaster inventory (concept)

Deliverable 2.1 "begins to develop criteria for the kinds of disaster events that would be useful to include in a pan-European inventory that forms the basis for the design of a common information space and the kind of information about the disasters that should be incorporated."

Please give a look at the paragraph "Criteria for including specific disaster events in the inventory", (D2.1 p.20) and answer to the following questions.

- Do you agree with the criteria used (D2.1, p.23) for including disasters in the inventory?
 Please indicate a score from 1 to 6 where 1 is "I totally disagree" and 6 is "I totally agree".
- 2. If you think that other criteria have to be enlisted, please indicate them here below
- Giving a look at the template (D2.1, p.25) how do you assess the correctness of the template used to collect disaster information? Please indicate a score from 1-6 where 1 is "totally incorrect" and 6 "is completely correct". If you assign 3 or lower: please indicate why_____

4. Pan-European disaster inventory (development)

5. Looking at the following table, how do you assess the level of completeness of the data set at the moment?Please provide a value from 1 to 6 where 1 is "not complete" and 6 is "fully

complete". If you assign 3 or lower: please indicate what is missed_____

Snapshot of Disaster Case Studies	Number of Cases				
Natural-Hazards	n=8				
Earthquake	2				
Epidemic/Disease	2				
Severe Weather (cold/hot/storm/flood)	2				



D5.3 Validation Strategy, Version 2 (ic) **Public deliverable**



Volcano Eruption	1
Wildfire	1
Technological-Hazards	n=5
Plane/Train Crash	1
Oil/Chemical Spill	2
Infrastructure Failure (e.g. blackouts/building collapse)	1
Explosion	1
Social-Hazards	n=4
Terrorism	2
Shooting	1
Crowd Control/Security Negligence	1
Total Number of Cases	n=17

Please give a look at all case studies described in D2.1 and answer to the following questions.

- 6. Do you think that at this stage the past disaster inventory is offering a sufficient covering of the European level of disasters? Please indicate a value from 1 to 6 where 1 is "not sufficiently covered" and 6 is "very well covered". If you select 3, or values lower, please describe why
- 7. Do you think that at this stage the past disaster inventory is offering a sufficient covering at region level? Please indicate a value from 1 to 6 where 1 is "not sufficiently covered" and 6 is "very well covered". If you select 3, or values lower, please describe why
- 8. Do you think that at this stage the past disaster inventory is sufficiently covering different kind of disasters? Please indicate a value from 1 to 6 where 1 is "not sufficiently covered" and 6 is "very well covered". If you select 3, or values lower, please describe why
- 9. Do you think that at the current stage the past disaster inventory is covering sufficiently different kinds of stakeholders? Please indicate a value from 1 to 6





where 1 is	"not sufficiently covered"	and 6 is	"very well covered". If you	select 3, or
values	lower,	please	describe	why

By utilising the http://31.171.245.222:8080/appframework/#!app/scenariodatabase

link:

Please, get access to the database where past disaster are stored and answer to the following questions about a key dimension on the impact of the information: the quality (Knight and Burn, 2005)¹⁸.

- How do you assess the reliability¹⁹ of the database? Please indicate a value from 1 to 6 where 1 is "not reliable" and 6 is "totally reliable". If you select 3, or values lower, please describe why______
- How do you assess the usability²⁰ of the database?
 Please indicate a value from 1 to 6 where 1 is "not usable" and 6 is "highly usable".
 If you select 3, or values lower, please describe why
- How do you assess the understandability²¹ of the database?
 Please indicate a value from 1 to 6 where 1 is "not understandable" and 6 is "totally understandable". If you select 3, or values lower, please describe why
- How do you assess the accessibility²² of the database?
 Please indicate a value from 1 to 6 where 1 is "not accessible" and 6 is "totally accessible". If you select 3, or values lower, please describe why
- How do you assess the consistency²³ of the database?
 Please indicate a value from 1 to 6 where 1 is "not sufficiently consistent" and 6 is "completely consistent". If you select 3, or values lower, please describe why

¹⁸ Knight, Shirlee-ann, and Janice M. Burn. "Developing a framework for assessing information quality on the World Wide Web." *Informing Science: International Journal of an Emerging Trans-discipline* 8.5 (2005): 159-172.

¹⁹ The extent to which information is correct and reliable

²⁰ The extent to which information is clear and easily used

 $^{^{21}}$ The extent to which data are clear without ambiguity and easily comprehended

²² The extent to which information is available, or easily and quickly retrievable

²³ The extent to which information is presented in the same format and compatible with previous data





- How do you assess the relevancy²⁴ of the database? 15. Please indicate a value from 1 to 6 where 1 is "highly irrelevant" and 6 is "highly relevant". If you select 3, or values lower, please describe why
- 16. How do you assess the accuracy²⁵ of the database? Please indicate a value from 1 to 6 where 1 is "not accurate" and 6 is "totally accurate". If you select 3, or values lower, please describe why
- How do you assess the amount of data²⁶ of the database? 17. Please indicate a value from 1 to 6 where 1 is "not appropriate" and 6 is "totally appropriate". If you select 3, or values lower, please describe why
- 18. How do you assess the navigation²⁷ of the database? Please indicate a value from 1 to 6 where 1 is "highly insufficient" and 6 is "totally positive". If you select 3, or values lower, please describe why
- How do you assess the efficiency²⁸ of the database? 19. Please indicate a value from 1 to 6 where 1 is "very low" and 6 is "very high". If you select 3, or values lower, please describe why
- How do you assess the value added²⁹ offered by the database? 20. Please indicate a value from 1 to 6 where 1 is "very low" and 6 is "very high". If you please select 3, or values lower, describe why

²⁴ The extent to which information is applicable and helpful for the task at hand

²⁵ The extent to which data are correct, reliable and certified free of error

²⁶ The extent to which the quantity or volume of available data is appropriate

²⁷ The extent to which data are easily found and linked to

²⁸ The extent to which data are able to quickly meet the information needs for the task at hand

The extent to which information is beneficial, provides advantages from its use







SECURE DYNAMIC CLOUD FOR INFORMATION, COMMUNICATION AND RESOURCE INTEROPERABILITY BASED ON PAN-EUROPEAN DISASTER INVENTORY

Survey for the Advisory Board

Simona De Rosa, Antonella Passani T6 Ecosystems

July, 2015

Work Package 5

Project Coordinator Prof. Dr.-Ing. Rainer Koch (University of Paderborn)

7th Framework Programme for Research and Technological Development COOPERATION

SEC-2012.5.1-1 Analysis and identification of security systems and data set used by first responders and police authorities







The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n°607832.



D5.3 Validation Strategy, Version 2 (ic) **Public deliverable**



Authors



T6 Ecosystems

Simona De Rosa Email: <u>s.derosa@t-6.it</u>

Antonella Passani Email: <u>a.passani@t-6.it</u>

Introduction to the survey

As part of SecInCoRe, the partner T6 Ecosystems srl is conducting a survey addressed to the Advisory Board members of the project.

The purpose of this survey is related to the SecInCoRe evaluation activities.

The project defines evaluation as follows: "According to the definition of impact provided by the International Association for Impact Assessment (IAIA) who specified that the impact is the difference between what would happen with the action and what would happen without it." (from Deliverable 5.2, available at http://www.secincore.eu/publications/deliverables/)

In line with this, one of the first steps indicated by the evaluation methodology is the understanding of your working routine now and in a next step we will contact you again to evaluated how the SecInCoRe results and outputs would change this.

The survey will take about 30 minutes to be completed.

Please answer all questions from the viewpoint of your organisation.

Please answer each question by ticking the appropriate answer(s) or providing your answer in the designated space.

In case some questions are not applicable to your situation, or show aspects you think are not relevant for the emergency world, please list us your suggestions/opinions to help us improving the questionnaire. Feel free to add comments after the text of the question where you think they need to be improved.

Please, notice that you can reply to this survey in a written form filling the questionnaire until August 31st or you can write at <u>s.derosa@t-6.it</u> in order to schedule a dedicated Skype call in the week from August, 24th to August, 31st.

Thank you for the time you dedicate to this survey! In case you need any support or clarification please contact Simona De Rosa at <u>s.derosa@t-6.it</u> or Antonella Passani at <u>a.passani@t-6.it</u>





Survey for advisory board and direct users

Name and Surname_____ Country _____

Position (according with table here attached)

- a. Please describe your title and position accordingly to the terms used in your organization
- b. What are you responsible for?

First part:

- 1. Please describe your work:
 - a) What organisation do you work for?
 - b) Please describe the main objectives of your organisation.
 - c) How does your organisation engage in disaster response?
- 2. In which way are you personally involved in disaster management?
- 3. Which instrument or tool do you most use to operate in such situation?
- 4. Considering the disaster circle and phases, which is the most challenging and complex phase of your work?
- 5. What do you think is the most problematic aspect of your work?
- 6. Which aspects of your working routines need to be improved?
- 7. How do you think your working routines could be improved with the adoption of new tools/concepts? Which kind of solutions you are looking for?

Second part: building a zero scenario





- 8. Please, think to a real concluded disaster (X disaster) in which you were involved and describe it.
 - a) What was your role in X disaster?
 - b) Which was the process (work flow) in which you were involved?
 - c) What technologies did you used during disasters? What for?
- 9. In the X disaster, with whom did you collaborate most?
 - a) By what means do you communicate during the X disasters?
- 10. What kinds of information/data sets did you use during disasters?
- 11. What information and/or data did you use to make decisions? Why did you use this information and/or data?
- 12. Which were the main sources of information during X disaster?
- 13. Who can access such sources of information and how?
- 14. Is access to these information/data sets free of charge or do you need to pay for accessing them? If you need to pay, how much and in which modality (yearly subscription fee, pay per use, etc.)
- 15. How did you share information with during disasters?
- 16. In general, which information/data sets are not available during crisis events, but would be beneficial?
- 17. In your opinion, how could these information/data sets best be made available before, during, or after a disaster?





- 18. In the chosen case, what did you think was the most relevant resource in order to complete your work?
- 19. In the chosen case, what did you think was the most relevant resource that you were missing in order to complete your work? And why was this resource not available
- 20. How do you judge the management of the X disaster on a scale from 1 to 6 where 1 is "highly insufficient" and "6 is "highly sufficient"?
- 21. Thinking to the results achieved in the X disaster, what could have been improved and how?





Questions to collect information about zero scenarios in relation to preparedness

Zero scenarios.

Preparedness and training activities

- 1. Thinking to the scenario that you described in the first survey, which are the main figures involved in the preparation of a plan in your organisation?
- 2. How much is their gross average salary?
- 3. Thinking to the scenario that you described in the first survey how many working days are needed to establish an emergency response plan?
- 4. Which is the medium costs that the Unit in charge of the establishment of the emergency response plan have to sustain in order to build such plan besides your human resources?
- 5. If more than one organisation is engaged, can you estimate the overall costs in terms of human resources and other costs?
- 6. In the first survey you pointed out that you used XXXX information during the emergency. Now, which kind of data would you use to plan a response to such emergency?
- 7. How do you assess the level of the information quality that you use to prepare a plan?
- 8. Given that the result of the planning. How do you assess the accuracy of the plan? Please assign a score from 1 to 6.
- 9. If the plan that you have described was really applied to the emergency, how the plan was important for the emergency and how was made by the improvisation?
- 10. According to the Humanitarian Process Cycle (HPC) elements for prepare, manage and deliver a humanitarian response are:
- A. needs assessment and analysis
- B. strategic response planning
- C. resource mobilisation
- D. implementation and monitoring
- E. operational review and evaluation.

Do you agree with the envisaged working flow or do you follow a different approach? Please describe it.

- 11. Which are the main figures involved in the preparation of a training exercise in your organisation?
- 12. How much is their gross average salary?
- 13. How many working days are needed to establish a training exercise?
- 14. Which are the main costs that the Unit in charge of the training organization have to sustain in order to build a training exercise besides your human resources?
- 15. If more than one organisation is engaged, can you estimate the overall costs of training in terms of human resources and other costs?





- 16. Which kind of data do you use to organise a training exercise as a preparation in case of disaster?
- 17. How do you assess the level of the information that you use to prepare a training exercise?
- 18. According to the disaster that you have described, how do you assess the accuracy of the training exercise? Please assign a score from 1 to 6.