CHAPTER 1

ASGARD: A Novel Approach for Collaboration in Security Research Projects

Juan Arraiza, Esther Novo, Seán Gaines, Aitor García Pablos, and Haizea Erostarbe

1.1 Introduction

Research on security at European level is a field that took greater importance until it became one of the key thematic areas of the Seventh Framework Programme (FP7) and then one of the seven societal challenges of the Horizon 2020 Programme (FP8).

In 2014, a study conducted from Czech security research funding programmes concluded, among other things, that "RTOs tend to propose projects with results which are achievable, yet without regard to their usefulness in practice; they rarely initiate voluntary involvement of the end user (except single cases); and their proposals tend to limit their ambition to results comprehendible by the RTO without much regard to the

J. Arraiza (✉) · E. Novo · S. Gaines · A. G. Pablos · H. Erostarbe
Vicomtech, Donostia, San Sebastian, Spain
e-mail: jarraiza@vicomtech.org; enovo@vicomtech.org; sgaines@vicomtech.org; agarciap@vicomtech.org; herostarbe@vicomtech.org

B. Akhgar et al. (eds.), *Technology Development for Security Practitioners*, Security Informatics and Law Enforcement,
https://doi.org/10.1007/978-3-030-69460-9_1

specifics, limits and boundaries of its future use in law enforcement practices" [1].

Also, in 2014 the European Commission, Directorate-General Enterprise and Industry commissioned a study on the final evaluation of Security Research under the FP7 [2]. The research methodology included desk research, statistical analysis of data from the CORDA database, surveys of participants and end-users, stakeholder interviews, a series of case studies and a stakeholder workshop. The last two conclusions and recommendations of this study were to "further buttress the role of end-users in all phases of Security Research Actions" on one hand and to "do more to maximise the benefits derived from the FP7 Security Research Programme and to reduce the tendency for insights and tools produced within projects to be left behind as partners move on to new projects or other priorities" on the other hand [2, p. 80]. In addition to those two key aspects, another important issue was identified as a major problem, which was that the law enforcement agencies' (LEA) expectations were not being appropriately met.

The LEAs and other security practitioners participating in FP7 security projects were normally treated as "customers", who were there to define their requirements at the beginning of the project and to evaluate the results during the final trials or demonstrations. In many occasions, they were not even members of the Consortia, but instead, they were participating as members of the projects' advisory boards. Most of the LEAs were not familiar with Research and Development, and by the end of the projects, they were expecting fully operational solutions that they could use right away, even when the research projects were targeting technology readiness levels (TRL) of "5" Technology validated in relevant environment, "6" Technology demonstrated in relevant environment, or "7" System demonstrated in relevant environment.[1] The vast majority of FP7 and then H2020 projects were never targeting TRL levels beyond "7" ("8" System complete and qualified or "9" Actual system proven in operational environment). Showing that there is still the need to improve how security project results deliver results that meet end-user needs, the main theme of the 2019 Security Research Event has been "Building Bridges:

[1] Technology Readiness Levels (Horizon 2020 work programme) – https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf

Promoting Market Uptake by Reinforcing Synergies Between Security Research and Other Funding Instruments" [3].

Back in the second half of 2013, a group of project coordinators and other principals of FP7 security research projects[2] met and decided they wanted to change some of the fundamental things on how this type of projects were being implemented. After some meetings and discussions, they agreed that they were going to collaborate in the preparation of a new project proposal designed to tackle precisely the same two key aspects that were soon afterwards included as conclusions and recommendations of the aforementioned final evaluation of security research under FP7.

To strengthen the role of end-users in security research, the new project proposal was going to adopt and adapt to the specific needs of the field of security research several of the open-source model principles and practices, which were in use in other domains such as ICT, but not yet in the field of European security research. Among these principles and practices are decentralization, open collaboration, peer-review production and iterative and incremental full-development life cycles.

To reduce the tendency for insights and tools produced within projects to be left behind as partners move on to new projects or other priorities, the new project proposal decided that the main goal of the project was going to be "to support LEA Technological Autonomy by building a sustainable, long-lasting community formed by LEAs, Researchers and Industry that will create (at little or no cost to LEAs), maintain and evolve a best of class tool set for the extraction, fusion, exchange and analysis of Big Data including cyber-offenses data for forensic investigation". The idea therefore was to create a sustainable and long-lasting "restricted" community composed by mutually trusted actors which was going to adapt and adopt open-source model principles and practices to conduct in a more efficient way European security research projects.

To appropriately manage the expectations of the LEA partners, the project's work plan was structured so that they were able to evaluate intermediate results several times before the end of the project, so that their feedback after each of the short full-development cycles could be used to re-adjust the scope and work plan of the subsequent ones.

In summary, based on their experience, the leaders of the new proposal designed the project under the hypothesis that a Consortium of LEA, Researchers and Industry, closely collaborating in a security research

[2] I.e., SAVASA, VALCRI, EPOOLICE, RECOBIA, VOXPOL, CAPER and VIRTUOSO.

project, following open-source model principles and practices, including iterative and incremental full development life cycles, and with the goal of building a sustainable and long-lasting restricted community was, on one hand, going to strengthen the role of end users in security research, it was on the other hand going to help market uptake of security research project results, and that it was also going to help setting better LEA expectations.

This chapter presents the H2020 ASGARD project, which is the project that was presented and that won the FCT-01-2015 topic, scoring 14.5 out of 15, that was funded with 12M Euro, and that started in September 2016 and is scheduled to end at the end of February 2020. This project has been identified by the European Commission as a success story that has built best practices which should be followed by future research projects [4, p. 24].

The rest of the chapter is structured as follows. In the "Related Work" section a brief state-of-the-art study and a brief description on how many, if not most, of the security research projects were executed at the time when the ASGARD project was being defined is presented. In the "Methods" section, the ASGARD project is presented as a case study. In the "Results" section, the findings of the case study are presented. Finally, in the "Discussion and Future Research" section, an analysis and explanation of the results of the research conducted, some of its limitations and some ideas for future research are presented.

1.2 Related Work

During Framework Programmes 6 (2002–2006), the participation of European law enforcement agencies in security research projects was small or rare that in general it could be considered as insignificant. The Framework Programme 7 (2007–2013) was a significant step forward in the recognition of the importance of this research field, and security became one of the key thematic areas of the programme. However, at the end of the Framework Programme 7, only a few European LEAs were participating in research projects. Out of the 320 projects listed in FP7 Projects section of the Horizon Dashboard[3] under the "SECURITY" thematic priority, the authors have only been able to identify 64 projects including at least one law enforcement agency or other relevant security

[3] https://webgate.ec.europa.eu/dashboard/sense/app/eaf1621c-67ce-4972-a07b-dddba31815c1

practitioners that are public legal entities. Based on these results, 80% of the projects under the "SECURITY" thematic priority were not including any relevant public security practitioners.

A 2011 study from the Harvard's Executive Session on Policing and Public Safety calls for "a shift in ownership of police science from the universities to police agencies" [5, p. 1]. This study states that such ownership would facilitate the implementation of evidence-based practices and policies in policing and would change the fundamental relationship between research and practice.

A 2014 study for the LIBE Committee of the European Parliament also revealed that technological tools and services cannot be developed without a thorough legal, social and political assessment, in order to determine their impact and effects, and it anticipated that funded security research in the future was mainly going to be put at the service of industry rather than society [6].

The role of LEAs participating in FP7 projects was mainly focused on requirements gathering phase and on participating on evaluations or demonstrations conducted at the end of the projects. In most cases of the 20% of the projects that included relevant public security practitioners, case apart from a few exceptions, the collaboration between research technology organisations, industry and LEAs was superficial, and the LEAs were not integrated into the project teams at the same level as the rest of their partners. The FP7 final evaluation report states that "End-users are thought to have constituted a significant minority of the organisations participating directly in FP7 Security Research projects, and are known to have also been engaged with the programme through other routes such as project advisory boards and dissemination events" [2, p. 118].

A trust relationship is one of the basic elements of any efficient collaboration. Most likely due to the nature of their work, LEAs had the tendency to follow the security through obscurity paradigm, and therefore the exchange of information between them and their partners in security research projects was limited. This issue was even more exacerbated by the intrinsic characteristics of European research projects, which include heterogeneous partners from multiple countries.

In addition, legitimate interests but different from different types of partners were not managed in the most appropriate way possible. It was not rare that LEAs hoped that the research projects would provide them with operational solutions, if not during the execution of the project, at least at the end of the projects. The report on Final Evaluation of Security

Research under the Seventh Framework Programme for Research established the following conclusions about the forms of end-users involvement in projects: “the development of outputs that don’t always correspond to end-users’ needs and requirements, and so cannot be immediately deployed in operational environments” and “the only way for projects to deliver outputs that are fit for purpose, immediately deployable at operational level, and that can contribute to solving real-life needs, is to actively involve them throughout the entire process of the preparation, management and review/evaluation of the Security Research programme” [2, p. 124–125].

During the definition of the proposals for new projects, many LEAs were asking for solutions that they needed at that time, not considering the times and deadlines that the research and development cycle entails. A proposal takes months to be prepared, then the evaluation process takes a few more months, then, if your proposal has been successful, the grant preparation also takes a few extra months. Once the grant has been signed and the project starts, the duration can easily be of 3 or more years. And the end results of the project are normally at technology readiness levels of 5–7; these are prototypes tested and/or demonstrated in laboratories or in operational environments but not final products and services that can be commercialized straight away. The whole process could normally last 4–6 years, and by the time the projects were finished, the results were in most cases still not ready to be used by end-users in their real cases. The (in many cases unrealistic) expectations of LEAs were not being met, and their level of frustration and dissatisfaction started to grow.

On the other hand, many industrial partners were using the research projects as part of their overall technological research and development pipeline process, being the technology itself their main interest, and not the pursue of developing new products for the law enforcement agencies. The technological results of the security research projects could serve as foundations for developing products and services in other (more profitable) markets. Besides, the fragmentation of the security market and the existence of a few global providers, often non-European, discouraged SMEs’ investments oriented towards crossing the innovation “valley of death”.

And with regard to research and technology organisations, their main interest was in many cases focused on producing scientific results that go beyond the state of the art and publishing those results in scientific journals and conferences, as those are the things that boost the careers of successful researchers.

Therefore, in the twilight of the FP7 programme, there was a clear misalignment between the interests, and in consequently the efforts and focus, of the different types of partners. In the context of decentralised, distributed, multidisciplinary and collaborative actions such as the European security research projects, this misalignment was as lethal as a torpedo in the waterline of the project.

In the twilight of the FP7 programme, a group of project coordinators and other principals of several security projects met and agreed that they wanted to tackle those known problems. They agreed to jointly prepare a proposal for a new project which should aim at building trust among LEAs, research technology organisations and industry, should also build upon best practices and lessons learnt from those previous projects and should do its best to deliver results which could be valuable to LEAs as soon as possible.

1.3 Methods

The main paradigm followed has been constructivism, which proclaims that reality is not discovered, but that it is constructed [7]. In this way, it is not intended to measure or control the real world but to know about it and to rebuild it in the most reliable way possible. The authors understand that knowledge is socially constructed by the participants in the research process and the research itself is not alien to the values of the researcher. The authors, as understood in the constructivist paradigm, believe that there is no single and (pre)determined reality but constructions that respond to the individual perception of each participant in the phenomenon. Therefore, the different interpretations of the phenomenon studied by a representative sample of the individuals participating in it have been studied.

The questions that this chapter will try to answer are: "How was the ASGARD project designed, how has it been executed, and why is it considered a success story?"

To answer these questions, the method chosen was a case study. According to the following definition for a case study, "a case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident" [8, p. 13]. This research method was chosen because the authors deliberately believed that contextual conditions could be highly pertinent to the phenomenon of study and, therefore, they wanted to cover them.

To build trust among LEAs, research technology organisations and industry, to build upon best practices and lessons learnt from previous related projects, and to deliver results which were of value to LEAs as soon as possible, the project was designed following open-source model principles.

Framework Programme security research projects are decentralised, distributed and collaborative endeavours, by nature. Also, the members of the Consortia are heterogeneous. Under these conditions, the open-source model principles of open collaboration, peer production, decentralised and iterative and incremental full-development cycles fit nicely. These principles, and the associated best practices, methods and techniques, were already common practice in other domains (such as information and communications technology – ICT) by the time the ASGARD project was designed, but they were not being applied in European security research projects.

At operational level, the management structure of the project gives task and work package leaders a great deal of flexibility to organise and coordinate the work within their work packages. Project coordination focused mainly on inter-work packages dependencies and issues.

The project's work plan was structured with a 3-month duration ramp-up phase, six full-development cycles of 6 months duration each and a final ramp-down phase of 3 months. This structure provides the flexibility needed as it allows adjusting the scope and the detailed plan of each of the stages as/if needed. Figure 1.1 below describes this agile approach. This flexibility in the design of the work plan allows keeping track of the evolution of the expectations from the relevant stakeholders (both internal and external to the Consortium) and making changes to the plan to try to meet them as much as possible whilst respecting the terms of the contractual agreement with the European Commission (EC).

But not only the expectations of relevant stakeholders are to be considered when thinking about changes to the plan of the subsequent project periods, it is also the continuous improvement of the processes of the project that matters. For this, it is important to conduct regular self-reflection of the project processes to identify, reduce and eliminate suboptimal processes and to strengthen those that are considered best practices.

In ASGARD, this was achieved by jointly conducting a lesson-learned exercise by all the project partners at the end of each of the project stages. This exercise aims at identifying what went right, what when wrong, which are the best practices that should be further implemented and improved,

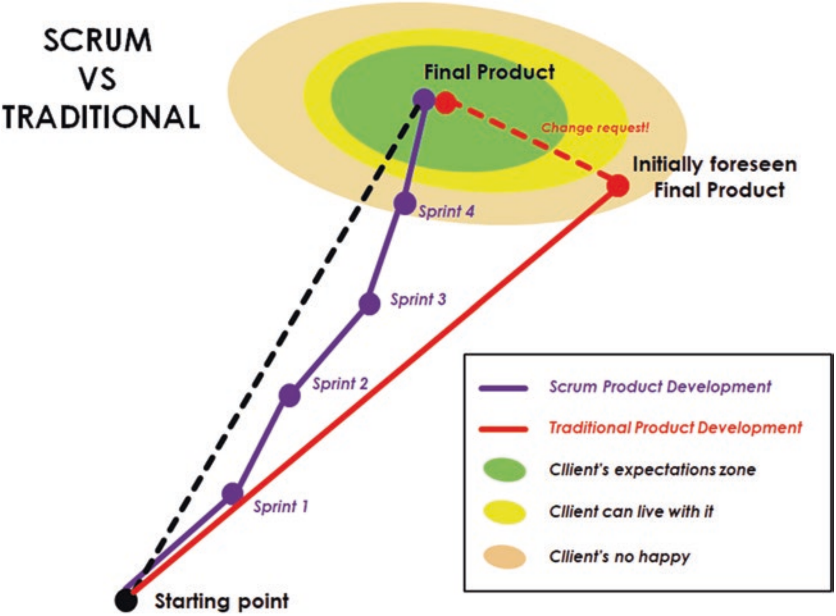


Fig. 1.1 How an agile approach allows adjusting the work plan to monitor and meet as much as possible the expectations of the stakeholders (source: "Scrum VS Traditional", Jorge Abad, http://www.lecciones-aprendidas.info/2016/07/Scrum-vs-traditional.html)

and which are the things that should be changed or avoided because they did not deliver the results that were desired.

Therefore, throughout the project, the Consortium can agree to adjust the scope and the detailed work plan for the subsequent periods based on the feedback that is collected and jointly assessed on regular basis (in the case of the ASGARD project, every 6 months).

The ramp-up phase served mainly to build the team, promptly launch requirements gathering and system specification and architecture design work streams, so that early drafts of all these deliverables could be produced to feed the first full-development cycle starting in month four of the project.

The first full-development cycle served to build the process, integrate several background technologies and allow conducting the first "hackathon" event on month nine of the project, at which these background technologies were evaluated jointly by all partners. The ASGARD "hackathons" were designed to be hands-on workshops for experimentation. These events team computer programmers, domain experts and users collaborate intensively. The ASGARD tools are presented and made available to set of multidisciplinary teams. Then a number of scenarios that are related to the project are presented to the teams so that they try to build a solution with the list of tools and datasets available to address those scenarios. The "hackathons" encourage participants to form ad hoc multidisciplinary teams, brainstorm ideas, implement and present a demo from which a winner is picked by popular vote. But most importantly, "hackathons" aid in team (trust) building, efficient peer collaboration and re-setting or adjusting project priorities and deadlines based on the feedback collected during the events.

At the end of each of the full-development cycles, self-assessment audits are conducted. These audits are based on anonymous feedback assessment by project partners. The purpose of the audits is team development and appraisal of project goals. They facilitate communication and team development within the consortium by providing feedback on partner performance. Furthermore, the process enables the partners to participate in goal setting and ensure they are married to the project goals, provide motivation to the consortium by demonstrating the participative nature of the project management process, provide clarity on the definition of project goals and most importantly make the communication and coordination processes of the project more effective and agile.

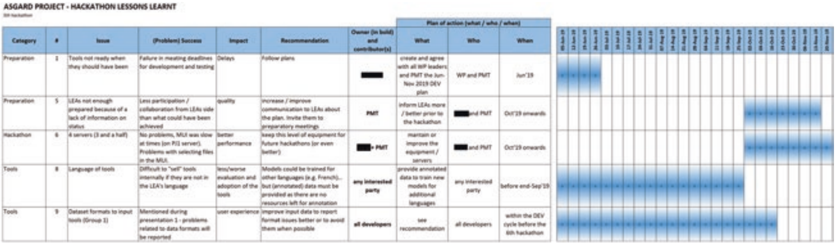
The audits are simple 360-degree feedback process in order to foster open and frank discussion on the progress of the project and performance of partners and project principals. The expected benefit of the processes is to formalize periods of reflection after distinct phases of the project life cycle so that inefficiencies and conflict can be identified and the appropriate measures adopted. The purpose of this review style is not intended to drive or maximize performance in the project but rather to ensure the expectations of partners and other stakeholders are reasonable and achievable to meet project goals. The audit's questionnaire is structured around the goals of the project period and the core values and ambitions of the project purpose. As a standing agenda item at project meetings, the governance body of the project assesses the results of these audits and takes appropriate action. As a consequence, a plan of action that addresses corrective actions, that re-inforces the strengths shown in the previous project period, and that works to remove the barriers identified to achieve the project goals is defined and implemented.

Face-to-face meetings, evaluation forms, and other means have been used to collect the feedback from other relevant project stakeholders such as European Commission officers or members of the project's Stakeholder Advisory Group (SAG).

1.4 Results

Up until now, six detailed project level (inter-work packages) work plans have been produced during the project, one for the ramp-up phase and one per each of the full-development cycles. These detailed work plans are discussed and agreed at the beginning of each of the periods, and they focus on the period at hand, maintaining the rest of the project periods at high level only. As described in Sect. 1.3, these detailed work plans were produced considering the overall project plan, the feedback collected and jointly discussed from the self-assessment audits and the outcome of the lesson-learned exercises conducted at the end of each of the stages. As an example, note how item #1 of the lesson-learned exercise conducted at the end of the fifth hackathon (Fig. 1.2) was included as part of the detailed plan of action for the subsequent period (Fig. 1.3) and even explicitly added to the plan as task #1.

As described in Sect. 1.3, the main tool to collect feedback from the members of the Consortium, and to measure their level of satisfaction and motivation, were the self-assessment audits. The audits consist on a set of 13 questions. All questions allow respondents to make comments, whilst questions 1–8 include in addition five-level Likert scale questions for specific statements. This is the meaning of each of the five level Likert questions:

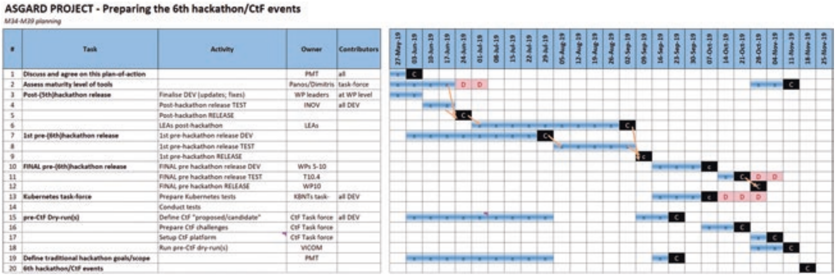


ASGARD PROJECT - HACKATHON LESSONS LEARNT

5th hackathon

							Plan of action (what / who / when)		
Category	#	Issue	(Problem) Success	Impact	Recommendation	Owner (in bold) and contributor(s)	What	Who	When
Preparation	1	Tools not ready when they should have been	Failure in meeting deadlines for development and testing	Delays	Follow plans	[redacted]	create and agree with all WP leaders and PMT the Jun-Nov 2019 DEV plan	WP and PMT	Jun'19
Preparation	5	LEAs not enough prepared because of a lack of information on status	Less participation / collaboration from LEAs side than what could have been achieved	quality	increase / improve communication to LEAs about the plan. Invite them to preparatory meetings	**PMT**	inform LEAs more / better prior to the hackathon	[redacted] and PMT	Oct'19 onwards
Hackathon	6	4 servers (3 and a half)	No problems, MLI was slow at times (on PII server). Problems with selecting files in the MLI.	better performance	keep this level of equipment for future hackathons (or even better)	[redacted] + PMT	maintain or improve the equipment / servers	[redacted] and PMT	Oct'19 onwards
Tools	8	Language of tools	Difficult to "sell" tools internally if they are not in the LEA's language	less/worse evaluation and adoption of the tools	Models could be trained for other languages (e.g. French)... but (annotated) data must be provided as there are no resources left for annotation	**any interested party**	provide annotated data to train new models for additional languages	any interested party	before end-Sep'19
Tools	9	Dataset formats to input tools (Group 1)	Mentioned during presentation 1 - problems related to data formats will be reported	user experience	improve input data to report format issues better or to avoid them when possible	**all developers**	see recommendation	all developers	within the DEV cycle before the 6th hackathon

Fig. 1.2 Sample extract of one of the lesson-learned exercises



ASGARD PROJECT - Preparing the 6th hackathon/CtF events

M34-M39 planning

#	Task	Activity	Owner	Contributors
1	Discuss and agree on this plan-of-action		PMT	all
2	Assess maturity level of tools		Panos/Dimitris	task-force
3	Post-(5th)hackathon release	Finalise DEV (updates; fixes)	WP leaders	at WP level
4		Post-hackathon release TEST	INOV	all DEV
5		Post-hackathon RELEASE		
6		LEAs post-hackathon	LEAs	
7	1st pre-(6th)hackathon release	1st pre-hackathon release DEV		
8		1st pre-hackathon release TEST		
9		1st pre-hackathon RELEASE		
10	FINAL pre-(6th)hackathon release	FINAL pre hackathon release DEV	WPs 5-10	
11		FINAL pre hackathon release TEST	T10.4	
12		FINAL pre hackathon RELEASE	WP10	
13	Kubernetes task-force	Prepare Kubernetes tests	KBNTs task-	all DEV
14		Conduct tests		
15	pre-CtF Dry-run(s)	Define CtF "proposed/candidate"	CtF Task force	all DEV
16		Prepare CtF challenges	CtF Task force	
17		Setup CtF platform	CtF Task force	
18		Run pre-CtF dry-run(s)	VICOM	
19	Define traditional hackathon goals/scope		PMT	
20	6th hackathon/CtF events			

Fig. 1.3 Sample extract of one of the detailed work plans

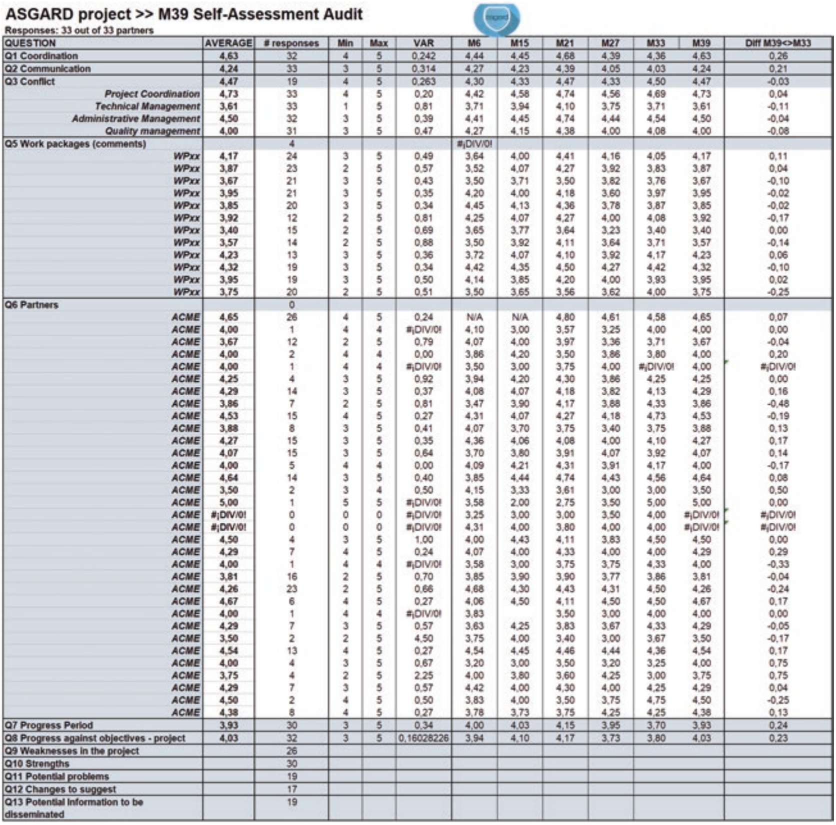
1. Insufficient
2. Barely sufficient
3. Sufficient
4. Good
5. Very good

Figure 1.4 presents an anonymized extract of the self-assessment summary corresponding to month 39 of the project. This extract excludes the comments, and it includes the average score obtained in questions 1–8 of the previous self-assessment audits.

For example, in the case of question 1, it can be observed that there were 32 responses, scoring an average of 4.63. The minimum score obtained was 4 and the maximum 5, being the variance quite low (0.242). Also, in comparison to the previous audit (month M33), this question obtained a better score, 0.26 points higher. When looking to all the average scores obtained for question 1 in all previous audits, it can be observed that the minimum score obtained was precisely on the previous audit (month M33) and the maximum score was 4.68 in month M21; therefore, the variance obtained throughout all periods was also low (0.017).

For question 4, one of the key roles has got an average score across all the self-assessment audits in the range of 3.61–4.10, whilst another key role has got an average score in the range of 4.42–4.73.

In the case of question 5, one of the work packages has got an average score across all the self-assessment audits in the range of 3.23–3.77, whilst another work package has got average scores in the range of 4.27–4.50. The average score for all work packages and all audits is 3.93.



ASGARD project >> M39 Self-Assessment Audit

Responses: 33 out of 33 partners

QUESTION	AVERAGE	# responses	Min	Max	VAR	M6	M15	M21	M27	M33	M39	Diff M39<>M33
Q1 Coordination	4,63	32	4	5	0,242	4,44	4,45	4,68	4,39	4,36	4,63	0,26
Q2 Communication	4,24	33	3	5	0,314	4,27	4,23	4,39	4,05	4,03	4,24	0,21
Q3 Conflict	4,47	19	4	5	0,263	4,30	4,33	4,47	4,33	4,50	4,47	-0,03
Project Coordination	4,73	33	4	5	0,20	4,42	4,58	4,74	4,56	4,69	4,73	0,04
Technical Management	3,61	33	1	5	0,81	3,71	3,94	4,10	3,75	3,71	3,61	-0,11
Administrative Management	4,50	32	3	5	0,39	4,41	4,45	4,74	4,44	4,54	4,50	-0,04
Quality management	4,00	31	3	5	0,47	4,27	4,15	4,38	4,00	4,08	4,00	-0,08
Q5 Work packages (comments)		4				#¡DIV/0!						
WPxx	4,17	24	3	5	0,49	3,64	4,00	4,41	4,16	4,05	4,17	0,11
WPxx	3,87	23	2	5	0,57	3,52	4,07	4,27	3,92	3,83	3,87	0,04
WPxx	3,67	21	3	5	0,43	3,50	3,71	3,50	3,82	3,76	3,67	-0,10
WPxx	3,95	21	3	5	0,35	4,20	4,00	4,18	3,60	3,97	3,95	-0,02
WPxx	3,85	20	3	5	0,34	4,45	4,13	4,36	3,78	3,87	3,85	-0,02
WPxx	3,92	12	2	5	0,81	4,25	4,07	4,27	4,00	4,08	3,92	-0,17
WPxx	3,40	15	2	5	0,69	3,65	3,77	3,64	3,23	3,40	3,40	0,00
WPxx	3,57	14	2	5	0,88	3,50	3,92	4,11	3,64	3,71	3,57	-0,14
WPxx	4,23	13	3	5	0,36	3,72	4,07	4,10	3,92	4,17	4,23	0,06
WPxx	4,32	19	3	5	0,34	4,42	4,35	4,50	4,27	4,42	4,32	-0,10
WPxx	3,95	19	3	5	0,50	4,14	3,85	4,20	4,00	3,93	3,95	0,02
WPxx	3,75	20	2	5	0,51	3,50	3,65	3,56	3,62	4,00	3,75	-0,25
Q6 Partners		0										
ACME	4,65	26	4	5	0,24	N/A	N/A	4,80	4,61	4,58	4,65	0,07
ACME	4,00	1	4	4	#¡DIV/0!	4,10	3,00	3,57	3,25	4,00	4,00	0,00
ACME	3,67	12	2	5	0,79	4,07	4,00	3,97	3,36	3,71	3,67	-0,04
ACME	4,00	2	4	4	0,00	3,86	4,20	3,50	3,86	3,80	4,00	0,20
ACME	4,00	1	4	4	#¡DIV/0!	3,50	3,00	3,75	4,00	#¡DIV/0!	4,00	#¡DIV/0!
ACME	4,25	4	3	5	0,92	3,94	4,20	4,30	3,86	4,25	4,25	0,00
ACME	4,29	14	3	5	0,37	4,08	4,07	4,18	3,82	4,13	4,29	0,16
ACME	3,86	7	2	5	0,81	3,47	3,90	4,17	3,88	4,33	3,86	-0,48
ACME	4,53	15	4	5	0,27	4,31	4,07	4,27	4,18	4,73	4,53	-0,19
ACME	3,88	8	3	5	0,41	4,07	3,70	3,75	3,40	3,75	3,88	0,13
ACME	4,27	15	3	5	0,35	4,36	4,06	4,08	4,00	4,10	4,27	0,17
ACME	4,07	15	3	5	0,64	3,70	3,80	3,91	4,07	3,92	4,07	0,14
ACME	4,00	5	4	4	0,00	4,09	4,21	4,31	3,91	4,17	4,00	-0,17
ACME	4,64	14	3	5	0,40	3,85	4,44	4,74	4,43	4,56	4,64	0,08
ACME	3,50	2	3	4	0,50	4,15	3,33	3,61	3,00	3,00	3,50	0,50
ACME	5,00	1	5	5	#¡DIV/0!	3,58	2,00	2,75	3,50	5,00	5,00	0,00
ACME	#¡DIV/0!	0	0	0	#¡DIV/0!	3,25	3,00	3,00	3,50	4,00	#¡DIV/0!	#¡DIV/0!
ACME	#¡DIV/0!	0	0	0	#¡DIV/0!	4,31	4,00	3,80	4,00	4,00	#¡DIV/0!	#¡DIV/0!
ACME	4,50	4	3	5	1,00	4,00	4,43	4,11	3,83	4,50	4,50	0,00
ACME	4,29	7	4	5	0,24	4,07	4,00	4,33	4,00	4,00	4,29	0,29
ACME	4,00	1	4	4	#¡DIV/0!	3,58	3,00	3,75	3,75	4,33	4,00	-0,33
ACME	3,81	16	2	5	0,70	3,85	3,90	3,90	3,77	3,86	3,81	-0,04
ACME	4,26	23	2	5	0,66	4,68	4,30	4,43	4,31	4,50	4,26	-0,24
ACME	4,67	6	4	5	0,27	4,06	4,50	4,11	4,50	4,50	4,67	0,17
ACME	4,00	1	4	4	#¡DIV/0!	3,83		3,50	3,00	4,00	4,00	0,00
ACME	4,29	7	3	5	0,57	3,63	4,25	3,83	3,67	4,33	4,29	-0,05
ACME	3,50	2	2	5	4,50	3,75	4,00	3,40	3,00	3,67	3,50	-0,17
ACME	4,54	13	4	5	0,27	4,54	4,45	4,46	4,44	4,36	4,54	0,17
ACME	4,00	4	3	5	0,67	3,20	3,00	3,50	3,20	3,25	4,00	0,75
ACME	3,75	4	2	5	2,25	4,00	3,80	3,60	4,25	3,00	3,75	0,75
ACME	4,29	7	3	5	0,57	4,42	4,00	4,30	4,00	4,25	4,29	0,04
ACME	4,50	2	4	5	0,50	3,83	4,00	3,50	3,75	4,75	4,50	-0,25
ACME	4,38	8	4	5	0,27	3,78	3,73	3,75	4,25	4,25	4,38	0,13
Q7 Progress Period	3,93	30	3	5	0,34	4,00	4,03	4,15	3,95	3,70	3,93	0,24
Q8 Progress against objectives - project	4,03	32	3	5	0,16028226	3,94	4,10	4,17	3,73	3,80	4,03	0,23
Q9 Weaknesses in the project		26										
Q10 Strengths		30										
Q11 Potential problems		19										
Q12 Changes to suggest		17										
Q13 Potential Information to be disseminated		19										

Fig. 1.4 Extract from the month 39 self-assessment audit summary

In the case of question 6, one of the partners has got an average score across all the self-assessment audits in the range of 3.00 and 4.00 (an average across all audits of 3.23), whilst another partner got average scores in the range of 4.58–4.80 (an average across all audits of 4.63). The average score for all partners and all audits is 3.94.

Note that for certain questions, the number of responses obtained could be none or low; thus, the score/result obtained should be interpreted accordingly. The detailed results for the rest of the questions can be found in Fig. 1.4.

An analysis of the results obtained after each of the audits allows identifying potential issues, weak areas and conflicts. The comments provided by the respondents, after being anonymized, are shared with the whole group, allowing also joint discussions around conflicts, issues, risks and barriers, but also around suggested improvements. In addition, each partner, key management roles and work package leaders can also see what the rest of the partners comment and think about their participation in the project.

Except for the second period review meeting, the feedback from the EC was consistently positive throughout the project. During the second period review meeting, there was a complaint about not having provided a draft of the technical report prior to the review meeting. Apart from this, communication with the project officer(s) from the EC was fluid and in general terms provided positive feedback on the progress made by the project. It is also important to note that in multiple occasions this fluid communication helped finding the most appropriate way forward to tackle specific issues or unexpected situations. An example of this is when the project coordinator requested clarification to the EC on how to proceed with the protection of the European Union classified information (EUCI) of the project. The project includes 16 deliverables that have been classified, and several of them required frequent access by most or all the partners. It was very important to find a prompt and efficient implementation of the EUCI handling guidelines, and this was successfully achieved thanks to the support provided by the EC.

The feedback from the SAG members was mainly obtained via evaluation forms that the SAG members attending the project events filled in. The satisfaction level was high among them, and there were also a few constructive criticisms (which SAG members were explicitly requested to provide as part of the continuous improvement process established in the project). It is also worth mentioning that multiple SAG members requested access to the ASGARD results and/or ad hoc demonstrations, which is a clear symptom of the interest that the project arose among them.

1.5 Discussion and Future Research

In this chapter we have presented the results of an exploratory study that lays the ground for future studies which could determine if what has been observed might be explained by an emerging theory.

The results presented in Sect. 1.4 show that the management structure of the project has been successful. The two different levels of operational management, one at project (inter work package) level and the other at work package level, have provided sufficient flexibility to the needs and characteristics of each of the work packages whilst offering the space to discuss and jointly agree on the solutions to put in place to tackle the issues and dependencies that affect multiple or all work packages. It is also worth mentioning that not all work packages have received the same type and level of coordination, and the satisfaction of the affected partners reflect that as well.

The feedback about the tools delivered in each of the full-development cycles was used to re-adjust the development plans in the technical work packages. But it was also not rare to identify new things not initially foreseen which were necessary or convenient. In many of these occasions, the Consortium discussed and agreed to add a new task or a new piece of work to the original plan. A couple of illustrative examples are the decision to design and proof-test a privacy engine on one hand and the decision to design and implement a tool maturity evaluation model on the other hand. This level of flexibility is, in opinion of the authors, another very important success factor of the project, as it provides space for creativity and innovation within the project boundaries.

The self-assessment audits are a very valuable project management tool. In line with a continuous improvement spirit, this tool provides the process and the framework for individual and joint self-reflection, allowing prompt identification and managing of negative trends, issues and conflicts. In addition, the tool also allows providing valuable feedback and constructive criticism.

The experience of the ASGARD project seems to indicate that applying open-source model principles and practices, including iterative and incremental full-development life cycles, and with the goal of building a sustainable and long-lasting restricted community, does strengthen the role of end-users in security research, it helps market uptake of security research project results, and it helps setting better LEA expectations.

However, at the time of writing this chapter, November 2019, the ASGARD project is still ongoing, so no final conclusions should be established. Based on the results obtained so far and considering the feedback got both from internal Consortium partners as well as from the external stakeholders of the project, it can be assumed that the initial hypothesis seems to be correct. In any case, though the results of this study could probably be transferable to similar projects, generalizing them should be avoided, as one case cannot represent all similar cases or situations. Further causal or explanatory research would be needed to confirm or deny the conclusions of this study and to test the cause-and-effect relationship between the methods followed in the ASGARD project and the positive impacts that have been identified on it.

In addition, there is still much to learn about which is the most appropriate role of the end-users in security research projects, the role that adds the greater value to them and to the rest of stakeholders that participate on such research projects (i.e. research technology organisations and industry). For example, how does the internal organisational structure of the end-users and the role of their project team members affect in their contribution to the benefits gathering of the research project? Or which methodologies, processes and techniques are the most appropriate to implement in security research projects to maximize the value added by the participation of end-users?

And there is also much to learn about which are the factors that help maximizing the market uptake of the results from security research projects. For example, which is the best combination of type of research actions or instruments that promote market uptake and that minimizes the risk of reducing the tendency for insights and tools produced within projects to be left behind?

Acknowledgements

Results incorporated in this chapter received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700381

References

1. Moravec, L. (2014). Research market gap in law enforcement technology: Lessons from Czech security research funding programmes. *Central European Journal of Public Policy, 8*(2), 28–49.
2. *Final evaluation of security research under the seventh framework programme for research, technological development and demonstration*. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/security/reference-documents/docs/fp7_security_research_final_report_en.pdf. Accessed 10 Dec 2019.
3. *Security Research Event 2019* – https://www.sre2019.eu/. Accessed 12 Dec 2019.
4. *Horizon 2020 – Work Programme 2018–2020, Secure societies – Protecting freedom and security of Europe and its citizens (European Commission Decision C(2019)4575 of 2 July 2019)*, p. 24. https://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-security_en.pdf. Accessed 10 Dec 2019.
5. Weisburd, D., & Neyroud, P. (2011). *Police science: Toward a new paradigm*. Washington DC: National Institute of Justice.
6. Bigo, D., Jeandesboz, J., Martin-Maze, M., & Ragazzi, F. (2014). *Review of security measures in the 7th research framework programme FP7 2007–2013*. Brussels: Committee on Civil Liberties, Justice, and Home Affairs.
7. Burr, V. (2003). *Social constructionism* (2nd ed.). Hove: Routledge.
8. Yin, R. K. (2014). *Case study research design and methods* (5th ed., p. 282). Thousand Oaks: Sage.