Table of Contents

[Table of Contents I](#_Toc57741961)

[Chapter 1 Introduction 2](#_Toc57741962)

[Chapter 2 Internal and external recommendations 3](#_Toc57741963)

[Chapter 3 Modular governance framework 4](#_Toc57741964)

[3.1 CCN structure 4](#_Toc57741965)

[3.2 Transversal activities [INOV] 4](#_Toc57741966)

[3.2.1 Partnership instrument [CNR] 5](#_Toc57741967)

[3.2.2 Cybersecurity training and awareness [BUT] 6](#_Toc57741968)

[3.2.3 Sustainable exploitation and IPR [SMILE] 6](#_Toc57741969)

[3.2.4 Certification organization and support [CETIC] 7](#_Toc57741970)

[3.2.5 Dissemination and communication [INOV] 7](#_Toc57741971)

[Chapter 4 Lessons learnt 8](#_Toc57741972)

[Chapter 5 Conclusions and perspectives 9](#_Toc57741973)

# Introduction

# Internal and external recommendations

# Modular governance framework

## CCN structure

## Transversal activities [INOV]

SPARTA’s transversal activities include the community and exploitation activities. In this section we report on the key governance and management takeaways, with regards to the recommendations that were reported in deliverable *D1.2 Lessons learned from internally assessing a CCN pilot*, as well as to other initiatives that contributed to improving the activities and processes in scope.

As governance and management matured from the project bootstrap year (Year1) to the intermediate year (Year2), the focus also turned decisively towards the future CCN setup and operation. In this vein, it is important to emphasize that the purpose of D1.2 was to assess the governance of the pilot, not that of the project.

The D1.2 recommendations that directly concern the community and exploitation activities are presented in the following table.

| **D1.2 reference** | **WP scope****(WP8-WP12)** | **Description (taken from D1.2)** |
| --- | --- | --- |
| GC\_I1 | WP8, WP11 | Technical Integration: Clarify the desirable and feasible level of integration between the technical components and results produced by WP4-WP7. Clarify the achievable level of alignment between the four technical programs on the one hand and both WP8 and WP11 on the other. |
| GC\_I4 | WP11 | Open Source: WP5 and WP6 may need support to engage with the Open Source spectrum in an active and sustainable manner. Could the scope of WP11 be extended by an activity targeting relevant Open Source communities? Are there individuals within the consortium or its group of associates who can and are would act as champions? |
| GC\_I6 | WP11 | Training: The data from the questionnaire and our technical analysis suggest a huge disconnect between WP11 and the technical programs. Is this indeed the case? Is this intentionally so? Would it be possible and desirable to establish trans-WP links? |
| GC\_A4 | WP8, WP9, WP10, WP11, WP12 | Risk Management: The T1.4 metrics for achieved objectives and the WP13 oriented metrics for the risk of not achieving them is very loosely coupled, if at all. In co-operation with partner INOV, T1.4 could be tasked to investigate whether there are industry-strength methods that offer better granularity, closer coupling, and an integrated view on progress vs. risk. Pilot governance may consider including those objectives that are currently incompletely covered in the list of managed risks.The D1.2 and D2.2 assessments could form the basis of future directory of SPARTA capabilities, supporting governance and stakeholders in building dedicated task forces. |
| GC\_M1 | WP8, WP11 | Four significant governance aspects are not fully covered yet. They all concern horizontal, co-operative and context-dependent activities:(a) Interaction with external entities and communities for validation and certification;(b) Potential joint activities with European agencies, external research programs and projects;(c) Roadmap updates to reflect new threats and cyber defence technologies;(d) Adjustments and extension of legal analysis to the (yet unknown) actual objectives of an ECCC / ECCN.It should be considered to track these four issues regularly and to include them in the list of risks to be managed. |

Table 1: Recommendations regarding community and exploitation activities (WP8, WP9, WP10, WP11, WP12).

The D1.2 recommendation concerning the coupling of risks to objectives (see Table 1, “GC\_A4” ) is analysed from the point of view of risk management, by identifying and reviewing risks that are not currently relevant. It is important to note that during the last risk assessment (Periodic Technical Report of October 2020), only 2 risks (out of a total of 28 risks managed for WP8-WP12) were assessed as being currently not relevant.

In the following sub-sections, a report is provided for each of the community and exploitation activities, detailing the pilot governance and execution improvements in Year 2.

### Partnership instrument [CNR]

<Please read the introduction of Section 3.2 carefully. You are free to follow any suitable approach for this report. The following suggestions are merely indicative –hope they help. Quality is more important than quantity, but regarding the expected page count: half-page to two-pages is OK.>

<Describe how the bootstrapping activities evolved and matured in Year 2, e.g. Community of Associates and Friends + Partners; Setup the SPARTA monthly workshops; Specify the JCCI - Joint Competence Centre Infrastructure; Support building relationships with all the relevant projects; Governance structures: Partnership Committee, Associates Council.>

<Analyse and report on how the recommendations in Table 1 applied to your WP in Year2, w.r.t. improvements of the activities and processes. Other governance and execution improvements in Year2 may also be relevant, if they contribute to increasing the overall governance maturity in SPARTA.>

<Topic to be developed: National Authorities in certification, NCCs>

<Comment on risks that materialized, and how they were addressed in Year2: e.g. WP8\_1 Lack of integration among the platforms; WP8\_2 Lack of integration of national ecosystems>

### Cybersecurity training and awareness [BUT]

<Please read the introduction of Section 3.2 carefully. You are free to follow any suitable approach for this report. The following suggestions are merely indicative –hope they help. Quality is more important than quantity, but regarding the expected page count: half-page to two-pages is OK.>

<Describe how the bootstrapping activities evolved and matured in Year2>

<Analyse and report on how the recommendations in Table 1 applied to your WP in Year2, w.r.t. improvements of the activities and processes. Other governance and execution improvements in Year2 may also be relevant, if they contribute to increasing the overall governance maturity in SPARTA.>

<Topic to be developed: contributions to cross-pilots workstreams>

<Topic to be developed: cooperation with ENISA>

<Comment on risks that materialized, and how they were addressed in Year2: e.g. Lack of cooperation from some WP9 partners>

### Sustainable exploitation and IPR [SMILE]

<Please read the introduction of Section 3.2 carefully. You are free to follow any suitable approach for this report. The following suggestions are merely indicative –hope they help. Quality is more important than quantity, but regarding the expected page count: half-page to two-pages is OK.>

<Describe how the bootstrapping activities evolved and matured in Year2>

<Analyse and report on how the recommendations in Table 1 applied to your WP in Year2, w.r.t. improvements of the activities and processes. Other governance and execution improvements in Year2 may also be relevant, if they contribute to increasing the overall governance maturity in SPARTA.>

<Topic to be developed: tools to collect/share exploitation-related information.>

<Comment on risks that are not relevant, and what is your suggestion for risk review, so that risks are related to SPARTA objectives: e.g. WP10\_1 Third party licensing obligations impacting project results exploitation>

### Certification organization and support [CETIC]

<Please read the introduction of Section 3.2 carefully. You are free to follow any suitable approach for this report. The following suggestions are merely indicative –hope they help. Quality is more important than quantity, but regarding the expected page count: half-page to two-pages is OK.>

<Describe how the bootstrapping activities evolved and matured in Year2>

In year 2 the certification activities have increased collaboration with the CAPE and HAIIT research programs, while initial contact have been established with T-SHARK and SAFAIR as shown in the figure below.



Figure Y: Status of cross-cutting certification activities

The above figure shows the evolution of cross-cutting certification activities with the research programs over the periods M1-M12, M12-24 and M24-M36. Certification activities within WP11 have focused on producing the WP11 deliverables with cross cutting activities in support. The main planned cross-cutting certification activities are with the CAPE research program in which several WP11 partners are involved. This has started at M1 with the topic of efficient certification processes and incremental certification that have been identified as a high priority research topics in T11.1 and T11.3. This has led to aligning the CAPE certification effort towards these goals by attempting to integrate incremental certification processes into cybersecurity assessment processes. The topic of certification of software development processes, as opposed to product-oriented certification, is the research topic of T11.4 and is being investigated as part of task T5.3 in the CAPE research program. Cross-cutting certification activities with the CAPE are planned until M36.

Following M12 review recommendations the certification cross-cutting activities with the other research programs has been investigated. In the period M12-M24 cross-cutting activities with the HAII-T have been started to understand potential links to certification. This has been implemented in the form of regular audio conferences with the individual HAII-T tasks to help them identify and understand some of the certification schemes identified in D11.1 as potentially relevant to SPARTA. It must be noted that WP11 partners are not involved in the HAII-T research program, which make it more difficult to implement the same type of experimental collaboration as with CAPE. However, some experimental activities are the topic of discussions especially in the area of privacy. Cross-cutting certification activities with the HAII-T are planned until M36.

Initial contacts with the T-SHARK and SAFAIR research programs have revealed little need for certification. However, contacts with the two research programs will be continued throughout the M24-M36 period.

Interaction with national cybersecurity authorities involved in SPARTA on the topic of certification is the topic of T11.2. Meetings are planned with the national cybersecurity authorities in the M24-M36 period and one of the topics of discussion will be results from cross-cutting certification activities. Topics of interest that will be discussed with national authorities include need for more efficient certification processes and incremental (product) certification and certification of software development processes.



Fig. Y: Conformity Assessment Bodies

The above figure shows the conformity assessment bodies as planned in the EU cyber act. It can be seen that members states designate national cybersecurity authorities that will supervise the conformity assessment bodies (CAB). CABs are in then accredited by the national accreditation bodies. CABs issue cybersecurity certificates upon prior approval of each certificate by the national cybersecurity authorities.

The Commission and ENISA are responsible for assessing the efficiency and use of adopted Cyber Act certification schemes (Evaluation and review of schemes – article 49-8, from voluntary to mandatory certification – article 56-3). If necessary, the Commission may ask ENISA to start a revision for a given scheme. Useful feedback on the application of certification schemes could certainly be provided by CABs and national cybersecurity certification authorities to the Commission and ENISA.

But beyond providing data directly related to certification schemes CABs could share innovations related to certification via workshops with the national certification authorities. For example the results of experiments on incremental product certification, or the comparison of process versus product certification could be shared in this manner. Also compilation of best practices with respect to certification such as in aviation safety [1] could be shared in a similar manner between CABS and national certification authorities.



Fig Y: network of evaluation facilities in the CCCN

Projecting this kind of collaboration between CABs and national certification authorities beyond the SPARTA project could give the following organisation described in figure Y in the context of the future CCCN. A European network of CABs could be created as a sub-goup within the CCCN community to share innovations related to certification. This idea will be detailed in D11.3. Sharing of more confidential data related to certification would be done on a national basis between CABs and their national certifications authorities, before being communicated to the European Commission.

<Analyse and report on how the recommendations in Table 1 applied to your WP in Year2, w.r.t. improvements of the activities and processes. Other governance and execution improvements in Year2 may also be relevant, if they contribute to increasing the overall governance maturity in SPARTA.>

GC\_I1: Collaboration between WP11 and CAPE is working well, collaboration between WP11 and HAII-T is progressing. And collaboration between WP11 and T-SHARK and SAFAIR is at an initial stage.

GC\_I4: the open source dimension is not being taken into account in certification.

GC\_I6: this is being addressed by the cross-cutting activities between WP11 and the research programs as reported above.

GC\_M1: most aspect of this requirement have not been analysed.

<Comment on risks that materialized, and how they were addressed in Year2: e.g. WP11\_1 Cybersecurity certification initiatives evolve during project duration -> ENISA EU Cybersecurity Act (CSA)>

The EU CyberAct is being closely monitored by WP11. Several WP11 partners are participating in ENISA ad hoc working groups on new certification schemes.

[1] Tobias Fiebig: How to stop crashing more than twice: A Clean-Slate Governance Approach to IT Security. EuroS&P Workshops 2020: 67-74.

### Dissemination and communication [INOV]

<Please read the introduction of Section 3.2 carefully. You are free to follow any suitable approach for this report. The following suggestions are merely indicative –hope they help. Quality is more important than quantity, but regarding the expected page count: half-page to two-pages is OK.>

<Describe how the bootstrapping activities evolved and matured in Year2>

<Analyse and report on how the recommendations in Table 1 applied to your WP in Year2, w.r.t. improvements of the activities and processes. Other governance and execution improvements in Year2 may also be relevant, if they contribute to increasing the overall governance maturity in SPARTA.>

# Lessons learnt

# Conclusions and perspectives