CORAL project, Act. 4.5

Feasibility study of basic-level certification following the CORAL framework v1.0

Market assimilation of CSA basic assurance certification

A CORAL project deliverable

Luxembourg House of Cybersecurity

Co-financed by the Connecting Europe Facility of the European Union

Document history

Version	Date	Changes	Editors
0.1	01/05/2023	Creation of the document, introduction and context	Gabriela Gheorghe
0.2	28/07/2023	Addition of section summarizing the feedback received section	Gabriela Gheorghe
0.3	31/07/2023	Internal review	Jean Lancrenon
1.0	31/07/2023	Internal follow-up to address comments, Website publication	Gabriela Gheorghe

Table of Contents

1 Introduction

1.1 Context in the project

Activity 4 in the CORAL project aims to propose a concrete process to evaluate basic-level conformity (against official schemes, or best practices) in line with the Cybersecurity Act (CSA) for any ICT process, service or product that is the target of assessment. While sub-activities 4.1 to 4.4 concentrate on defining the basic steps and actors in the certification process, the terminology to be used, a scoring approach and the proposal of an auditor profile to be involved in the assessment process, activity 4.5 proposes a study to evaluate the reaction of an initial user base to the overall approach and proposed usage of the tool.

1.2 Objectives of this document

This document presents the first outcomes of the feasibility study that was conducted on a small user base, in a short period of time during the project, covering a diverse audience in terms of either role (MSc students, SME representatives or CEOs, standardization workgroup delegates) or location (Luxembourg, Germany, Belgium, Sweden). The questions asked revolved mostly around comprehension of using the tool but also the overall approach.

2 Feedback study methodology

Process. A feedback form was created and uploaded on the project website, including several questions related to the following aspects:

- The choice of the questionnaire that the respondent made,
- Overall comprehension of the questions and recommendations in the chosen questionnaire,
- The existence of blind spots or aspects not investigated that should be of interest to the respondent,
- A quantitative score over the usefulness of a self-assessment tool to ease the way towards certification in the CSA context,
- Feedback on the price that a solution provider such as the respondent would be willing to consider for obtaining a basic-level certification in the scope of the CSA,
- Any further remarks or comments on the current approach.

A link to this feedback form was propagated to a range of respondents in the following step.

Timeline. Our feasibility study lasted from the 22nd of March until the 30th of April.

Outreach. An estimated number of 40 individuals were contacted, directly or via mailing lists, including both individuals and companies. During our feasibility study, we reached out to the following categories of respondents:

- the external companies that supported the project proposal (based in Luxembourg and Germany),
- members of Luxembourg standardization committees related to CSA (Luxembourg),
- MTECH Master students where ILNAS is a partner institution (Luxembourg),
- Several LHC contacts representing small and medium size organizations in Luxembourg,
- Two companies external to Luxembourg (namely, a Swedish one and a Belgium one).

Aside from unofficial feedback, we received 6 feedback forms duly filled in.

3 Feedback received

Choice of questionnaire. In terms of which questionnaires were chosen by responders:

- ICT services: 30% of respondents chose this option,
- ICT product (Web application): 50% of respondents chose this option,
- ICT process: 20% of respondents chose this option.

Usefulness quantification. On a scale of 1 (not useful) to 5 (useful), the average score obtained was 3.75. All respondents found the CORAL self-assessment for certification approach useful, but one respondent whose comments pointed out a comprehension challenge[1] towards the wider public of the Fit4CSA tool. One participant specifically confirmed that the score result received is correlated with the level of maturity of their organization in terms of cyber security readiness.

Other remarks received.

- Wording improvements. Almost all respondents pointed out wording improvements (e.g., either acronyms that should be explained (e.g., "SSRF" from the "Web application" questionnaire), or minor wording issues that can make the responder hesitate among the answers to choose).
- Addition of references (links) or definitions.
- Additional questions. One respondent suggested the addition of questions related to security architectures and engineering "going beyond encryption and segmentation", as well as questions from OWASP A09:2021 – Security Logging and monitoring failures. Another respondent suggested adding a question about a responsible disclosure process and the accessibility of the contact details of the data protection officer in relation with a Web application.
- Themes in navigation. One respondent suggested to make the navigation structure more visible so that it would be possible to see the themes of the questions. Also, the same person suggested availability of the current tool in other languages.[2]
- Bug about recommendations. It was also several times that a bug was reported, that recommendations are given in the end despite the answer having been optimal. The bug was fixed immediately (in this case, it was related to password changes by users).

[1] The remark was on the terminology used in the questionnaires, which could be perceived as too technical for the general IT public in an SME. While the way CORAL questions were formulated was meant to simplify as much as possible some formulations present in the control objectives of official schemes and best practices, the position of the project with respect to this point is that a company aiming to achieve a cybersecurity certification should have a good understanding of the terminology in official related schemes and good practices.

[2] While the consortium analyzed this activity as possible during the lifetime of the project, it was decided not to translate in other languages as long as the schemes that Fit4CSA is based on (in particular EUCS) are not yet official.

Remarks about pricing the external assessment towards an external auditor.

- Duration of basic-level certification audit based on CORAL. One respondent suggests two days of work to be adapted to this task.
- Pricing estimations vary among EUR 3,000 and 5,000 for SMEs, and under EUR 2,500 for very small enterprises, with a suggestion to make recertification a recurring process priced to around EUR 400.
- One respondent mentioned that it is important that any certification should expire after maximum 5 years.

4 Conclusion

This document's aim was to present the feasibility study that was performed throughout the project, delivering the first feedback and reaction of an initial user base towards the tool and the CORAL approach. The comments received are in the process of being addressed (where possible, the Fit4CSA is adapted to account for the changes). With the final dissemination stage, the project is asking for more feedback about the tool and approach from a much larger audience both in Luxembourg and abroad. At this point we are also waiting for more detailed feedback from the ENISA workgroup on cybersecurity certification, who have given us a very positive first reaction about the overall approach and process.