CORAL's contribution towards a common level of maturity in cybersecurity certification

A CORAL project milestone

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

Document working group

Name	Affiliation	Role
Gabriela Gheorghe	LHC	Contributor

Document history

Version	Date	Changes from previous
1.0	31/10/2023	Creation and finalisation of draft.

European Union funding

The CORAL project - of which this deliverable is a part - is Action no. 2020-LU-IA-0209, benefitting from European Union funding under the 2020 CEF Telecom Call[1].

The contents of this publication are the sole responsibility of ILNAS and the LHC and do not necessarily reflect the opinion of the European Union.

[1] https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2020-cybersecurity

Table of Contents

1. Introduction

The current document is part of the CORAL CEF Telecom project (2020-LU-IA-0209) and duplicates the content of the final report of the Action in what concerns the contribution of the CORAL project to supporting a common level of maturity in cybersecurity certification. The reason of the content duplication is the ease of sharing of this particular text with other members of the DG-CONNECT for the purposes of final project review.

Milestone 11 referred to the participation of a representative of the CORAL consortium in a May ECCG meeting, which was eventually delayed to June 9th. The participation was linked to a project presentation, the slides of which had been prepared sufficiently in advance to share with the HaDEA and organisers of the ECCG meeting as well. Therefore, the Milestone having been achieved in June, the current report wraps up the consortium's final thoughts on the positioning of the results of this Action with respect to the Call, and the reuse of the Action's achievements.

2. Alignment with Call text and CEF Telecom programme

Alignment with the CEF Telecom Work Programme.

Our action is aligned with the CEF Telecom Work Programme 2019 and 2020 in that it aims to support consumers and businesses (in particular SMEs) in their need of using or developing safer and more secure services at lower costs. Our action is proposing a possible structure and several building blocks of a potential public service, that could be operated at member state level or across neighbouring countries. This is because the CSA ecosystem should be encouraged to develop and expand across borders, especially for the countries like Luxembourg where the

reliance of the majority of local SMEs on supply chains from abroad is significantly higher than elsewhere. In this spirit, the approach taken by our action is not country-specific, is fully transparent towards the public and future-proof in that it can be adapted to any new official criteria activated at EU-level, for the basic level of assurance within the CSA context. The framework that CORAL proposes can enable a digital cross-border service of security assessment and certification. Businesses (SMEs in particular) are the main target of this service, as the purpose is to support them in achieving higher cybersecurity maturity and encourage them to frequently reiterate the assessment that we propose in this framework. In addition to businesses, other stakeholders part of our framework are:

- Auditors, whose role would be to perform the external review potentially leading to a certification, based on the answers provided by respondents but also on separately provided evidence;
- Conformity Assessment Bodies (CABs), who could inspect the result of the audit using the proposed tool, and contribute to the actual certification (or labelling) of a given ICT service/product/process at the basic level.

The action's outcomes are also completely country-agnostic with respect to these stakeholders.

With its proof of concept, our action can prove that cybersecurity assessment at the basic level of the CSA can be quickly turned into an operational public service, ready to be deployed and easily maintainable over time. Even though the action cannot yet claim alignment with official schemes for CSA certification (as none have yet been activated at EU-level and technical specifications for such schemes covering the basic level of assurance are yet to be finalized), the consortium maintains that the assessment criteria chosen are based on state-of-the-art best practices, and the tool provided serves at this point as a strong maturity assessment tool.

Alignment with the Call Text. Our action addressed Objective 4 of the CEF-TC-2020-2 Cybersecurity Call for Proposals (page 7), in particular it contributed to improving the "*cooperation of cybersecurity certification stakeholders"* aspect in line with the CSA. As the CORAL consortium consisted of one cybersecurity agency, one standardisation agency, and an NCCA in Luxembourg, the action has created common activities related to cybersecurity standardisation that did not exist before and that will live outside of the project lifetime. This is evidenced with two main examples:

- The newly developed standardisation page on the cybersecurity.lu portal, the development of which is work in progress between ILNAS and LHC. This common effort has already started in the second part of 2023, and its purpose is to bring the existing work in standardisation in cybersecurity closer to the cybersecurity community at large in Luxembourg.

Following Luxembourg's national cybersecurity strategy, LHC's mission is to encourage the development of new, and the improvement of existing, capabilities in order to strengthen the local economy. One of the main information tools that LHC is offering to the local cybersecurity ecosystem is the cybersecurity.lu portal, currently being used by 364 entities (of which 311 private companies, 40 public entities and 13 clubs or associations). This portal contains a wealth of information and references to tools relevant for, and targeted to, the cybersecurity professionals in Luxembourg, for example: different types of events, professional education and job offers, support for start-ups, and resources (including best practices, publications, rules and laws). On this background, CORAL set the ground for promoting (1) European and international standards to the local cybersecurity community and (2) local representation in standardisation committees that take place nationally and abroad.

At this moment, LHC has started addressing point (1) above, in collaboration with ILNAS. The main intention of this initiative is to inform all cybersecurity professionals of the existence of different types of information security and privacy standards (e.g., depending on their main topic, issuing organisation but not only) that can be of use in their day-to-day operations (including certification, evaluation and auditing). In a follow-up effort, to address point 2) above, we intend to "take the pulse" in a quantitative and qualitative way of current interests of market players in the proposed standards, and then to aim to popularise the take-up of standards in cybersecurity practices for SMEs in Luxembourg.

- Organisation of joint ILNAS-LHC events such as this one on topics in relation with the CSA. CORAL has substantially strengthened the collaboration between the ILNAS and the LHC, and so we foresee similar joint events – either located in the premises of LHC or of ILNAS – on topics that are close to the missions of both ILNAS and LHC. This is because ILNAS intends to boost visibility on its missions including the role of NCCA hence address a wider cybersecurity community in Luxembourg. At the same time, as explained above the LHC aims to consolidate the cybersecurity ecosystem and provide it with tools to improve its cybersecurity posture. Therefore the collaboration between ILNAS and LHC can only benefit both sides.

In relation with the 3 types of activities mentioned in the Call for Proposals (at page 7), our action has contributed to the following activities:

- **"building up or enhancing internal capabilities**". Our action significantly contributed to the upskilling and development of specific internal capabilities for all project beneficiaries, in the following ways:
    - For ILNAS, in its role of NCCA, this action brought a clear improvement on internal expertise. The project required examining the CSA from an angle different than merely that of its supervision missions. ILNAS has had to

immediately plunge into scheme requirements in order to support the LHC in its formulation of the security questionnaires. Also, the action required ILNAS's standardisation department to closely pay attention to CSA-specific standardisation developments. This increase of internal expertise benefits ILNAS's missions, as they will be better prepared in their role, when they would need to perform official NCCA duties. In the meantime, this newly acquired expertise also contributed to the creation of training material, for instance for that given at the Digital Learning Hub by ILNAS.

- For ANEC G.I.E, the action triggered the acquisition of solid knowledge of CSA-related standards. ANEC G.I.E.'s missions related to standardisation are to support ILNAS' standardisation department in promoting the market's (1) usage of standards and (2) participation in the standardisation process. As a consequence to this action, ANEC G.I.E. is now well prepared to do this in particular for existing and upcoming CSA standards, as well as to answer any queries about cybersecurity standards from market actors.
- For LHC, in its role of cybersecurity agency for Luxembourg, the action led to a strong improvement on several areas: 1) on internal expertise related to cybersecurity standards of different issuers, on different technologies, 2) positioning of LHC as a centre of expertise in the cybersecurity certification ecosystem in Luxembourg (particularly supporting the assessment process), 3) investigating ways of becoming a Conformity Assessment Body (CAB) in the future in Luxembourg and already having not only a good understanding of but also active interactions with the NCCA in this space. Due to CORAL's Fit4CSA, LHC's Fit4* platform can propose an audit module that can be used by auditors and auditees alike; this is a feature that did not exist before but that can be used in the future in contexts related to certification at scale.

- **"cross-border exchange of good practices and relevant information related to conformity assessment activities, and peer support."**

There are several contributions to the cross-border exchange of good practices that we can mention here. Two examples of cross-border exchange in the CORAL project came by virtue of *the design* of the project:

- The first one consisted in the presentation of the CORAL project and initial results at the ECCG meeting in June 2023. This particular CORAL presentation was the core of Milestone 11. In general, the ECCG meeting puts together CSA stakeholders (specifically, representatives from each Member State's NCCA) from multiple EU countries as well as ENISA. ECCG stands for "European Cybersecurity Certification Group" and its existence was established in the CSA, with the purpose to ensure the consistent implementation and application of the CSA in the EU member states. The

opportunity given to the CORAL project to be presented at the ECCG meeting allowed a considerable increase in visibility of the country's potential to contribute to the group. In addition to ENISA, multiple ECCG members welcomed the work and found it interesting.

- A second example is that the tool built throughout the project (Fit4CSA) is an open-source tool, which by design contributes to a cross-border exchange of practices and relevant information on cybersecurity assessment – as (1) it is not restricted to Luxembourg usage nor (2) is it restricted to country or region-specific schemas of certification, but based on EU-level or internationally agreed upon good practices.

Other examples materialised along the project as a consequence of the first two design choices:

A third example of cross-border exchange was a consequence of the initial presentation within the ECCG group. The CORAL consortium has had multiple interactions with ENISA's Open Source Software group, as the OSS team expressed interest in the CORAL tool and approach to performing assessments based on official schemes.

A fourth example of a meaningful cross-border exchange is that an ENISA representative has agreed to be a speaker at the CORAL end-of-project event and their presentation led to sharing relevant information with the Luxembourgish community. As there have been multiple requests to share the slides of the presentation given by the ENISA representative, we have posted the materials on the project website. One participant to the CORAL end-of-project event – an otherwise seasoned cybersecurity professional in Luxembourg – mentioned that it was "a privilege to be on the receiving end of a very informative session by ENISA".

Fifth, the consortium decided to add two more deliverables as part of the action, of which one in particular was distributed to the European CSIRT network by LHC's CIRCL team (and that CIRCL is part of). The topic of how does CSA-based certification impact computer emergency response teams (CSIRTs) was a topic that was on the CSIRT network discussion agenda, with CSIRT representatives from all over Europe having received this CORAL report.

- **"development and implementation of efficient evaluation methods"**

Due to its design, CORAL has developed and implemented an efficient evaluation method called Fit4CSA, whose proof of concept was the purpose of Activity 3 of the action. Fit4CSA addresses the problem of a lengthy process of assessment and improves the likelihood that the target of assessment succeeds in obtaining the certification. The tool and the process are domain agnostic and can be replicated or adapted to incoming official assessment schemes activated at EU level. The tool is easily accessible online, open source, and is usable free of charge and anonymously by any entity wishing to perform a self-assessment of its

product/service/process for as many iterations as it wishes. (The entity may choose to lift this anonymity if it opts to use the tool in the context of a CSA certification process, but there is no obligation to do so.)

3. Reuse of CORAL achievements by other European entities

Our action proposed an approach that can be tailored to individual contexts and that is fully reusable. As soon as official schemes for cybersecurity certification covering the basic assurance level would be activated, these can be easily plugged into the Fit4CSA tool. This is done by reworking the questionnaires (questions, answers, recommendations – all grouped into sections and categories that depend on the context, and the maturity threshold while reusing the tool's look and feel, scoring, and overall process from self-assessment to potential audit. The reporting features (result screen and the downloadable report) that the tool offers can also be customised with visuals that depend on anything from country/region/issuing authority.

This flexibility is possible because reuse was an essential principle in the design of our work, both in the proof of concept and in our deliverables including the questionnaires and reports. In particular at play there were two main aspects:

- **Open source proof of concept of our action.** As LHC is committed to producing open-source software that is useful for the cybersecurity community in general, this was a design choice woven into this action. The Fit4CSA tool is part of the Fit4Cybersecurity platform. Anybody is free to obtain its source code over github and adapt the tool as desired, by respecting the GNU Affero GPL v3.
- **Deliverables and extra reports intended to be useful**. All our planned project deliverables are intended to be useful and used by the public (be it the wider public, or the CSA ecosystem in several cases). Notably:
    - The State-of-the-Art document (first item here) consists of a comprehensive listing of standards, literature, and guidelines related to requirements and recommendations for basic levels of cybersecurity.
    - The evaluation questionnaires (third item here) can be used to track the criteria and control objectives as they are now encoded in the tool, and how they link with known references (standards, best practices, etc).
    - The CORAL methodology and conformity assessment guidance (sixth item here) can be useful for any organisation that is part of a CSA ecosystem, to understand and reuse parts of the CORAL approach.

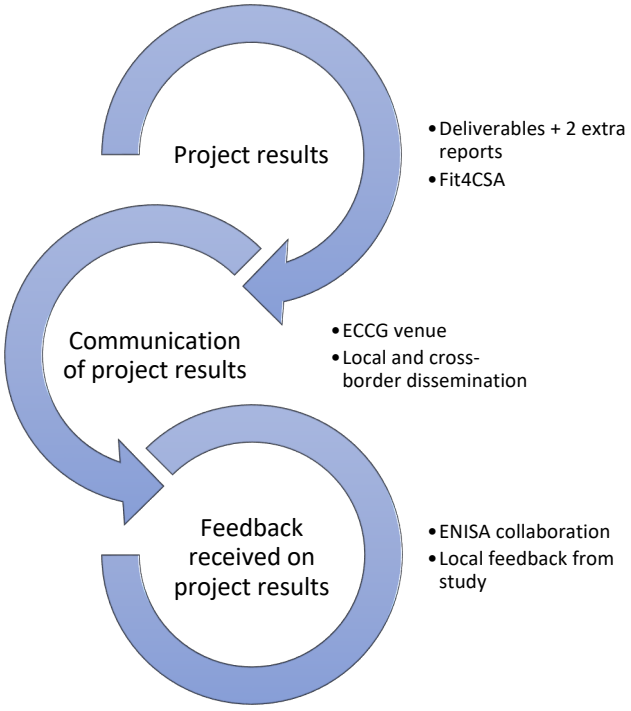
- The extra reports (items 7 and 8 here) are also intended to be used by an even wider community: computer incident response teams in Europe who might wonder on the impact of CSA over their functioning, as well as anybody who is interested or curious about cybersecurity certifications and asking themselves what is value of that in light of incoming regulations and directives in Europe regulating cybersecurity directly or indirectly.

To add to the reusability of our action's results, the consortium was delighted to receive strong interest from ENISA's OpenSource Software team and the certification team, related to the CORAL PoC and approach. The CORAL consortium has had several interactions with ENISA on this topic, of which one workshop describing technical parts of the CORAL tool and approach. From our understanding, ENISA considers re-using the CORAL approach in its future work.

4. Contribution to a common level of maturity in cybersecurity certification

In this previous sections we have addressed how our action was aligned with the CEF Telecom Work Programme 2019-2020 and with the call text from the CEF-TC-2020-2 Cybersecurity call for proposals. We have also presented how others can reuse the results of this action. On this compliance background, we will now describe how the action has contributed to support a common level of maturity in cybersecurity certification.

CORAL is based on an existing common set of maturity criteria (e.g., candidate schemes and accepted standards)**.** Firstly, the action has focused on proposing a solution (a process, a tool, terminology, an auditor profile, most notably) to ease the way an ICT product/process/service can reach a basic level cybersecurity certification in line with the CSA, based on common maturity criteria established at EU level. CORAL proposes no



new schemes or evaluation criteria of its own; instead, it relies entirely on activated official schemes, or, if none are available, those candidates schemes that cover CSA's basic level of assurance. For the areas outside of the current scope of candidate schemes (ICT process), CORAL bases itself on known standards for maturity assessment. Hence, commonly-agreed control requirements to assess cybersecurity maturity are at the heart of CORAL's design.

Local and cross-border knowledge sharing and awareness about CSA certification and cybersecurity standards. Within our action we were aware of the need to communicate about its results, and also because knowledge about CSA and cybersecurity standards was isolated to certain communities in Luxembourg. Proposing something for the public good would have no value if nobody would know about it. By the design of the project, Activity 5 was foreseen as a solid dissemination effort, covering not only local but also cross-border venues. We have used the opportunity of having an "open door" to the ECCG group so that we would talk about CORAL and its reusability. As a consequence, we have received strong interest from ENISA (as demonstrated by the attached support letter dated 15/12/2023), whose overarching mission is towards common tools and requirements. Moreover, our end-of-project event hosted a wide group of diverse stakeholders who have showed interest in the results of the project and the topics addressed, so we are confident that awareness has increased with the collaboration brought about by CORAL, between ILNAS, ANEC G.I.E. and LHC.

Country-independent framework that can be adapted to future official schemes. As our output is not country nor context specific, our results are entirely transferable and freely reusable, which also speaks for the public value of our results. All the output of the project (tool and deliverables) were steered towards a public goal: turning state-of-the-art security maturity requirements into a set of building blocks that, when put together, could enhance the certification process and make it more understandable and cost-effective for SMEs to deploy security controls that abide by standard requirements.

Engagement with EU certification stakeholders. The consortium used the ECCG group meeting opportunity of Milestone 11 as a springboard for discussions with other NCCAs and EU's cybersecurity agency related to tools enabling basic assurance certification. Our interactions with ENISA and the feedback we have received locally from the study as well as from our events spoke for the value that CORAL has in supporting a common process to assess cybersecurity maturity. We have insofar received very encouraging feedback about the CORAL approach and ENISA's support letter of CORAL, dated 15/12/2023 and attached to this report, is a proof of that feedback.

Bootstrapping a feedback loop around certification tools and needs with SMEs. With the initial feasibility foreseen in our project, we have started a communication thread around the needs and expectations that the public (SMEs, primarily) would have when it comes to a tool for cybersecurity self-assessment. We have received interesting feedback that could be useful for certification bodies or ENISA in their design of future candidate schemes, or in the update of the

existing ones. We believe that real-world experience and open communication about challenges related to the assessment process and the assessment criteria are key to the common understanding of such mechanisms that benefit the common level of cybersecurity maturity in Europe. What we need to work more on, in this sense, is a way to propagate the feedback received, in a systematic way, to the stakeholders involved in the drafting of next or existing schemes. CORAL's experience opened up several reflections in this sense.

5. Final remarks

While the CORAL toolset is primarily destined to support SMEs in preparing for, and obtaining, basic-assurance-level certification against a CSA scheme for a developed product, process, or service (or alternatively, if permitted, the issuance of an EU declaration of conformity), a key point is that this is through an iterative process, in particular involving multiple repetitions of the usage of Fit4CSA to gradually build up and improve the security posture of said product, process or service. Thus, the added value of the tool is exactly that of the CSA itself: to improve cybersecurity in the Union.

In addition to the above, in its CORAL acknowledgement letter dated 15/12/2023 and shared with HaDEA, ENISA "took note of the development and demonstrated capability of operation of the online tool related to CORAL". ENISA acknowledged that such approach and tool falls within the scope of the European Cybersecurity Certification Framework, as "it provides guidance to specific stakeholders or use cases, some of which with hands on effect", being fully in line with CEF TELECOM call 2020 CEF-TC-2020-2:*"Cybersecurity for Objective 4: Support to cooperation and capacity building for cybersecurity certification in line with the Cybersecurity Act".*