
	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)		
	CORAL Methodology and Conformity Assessment Guidance		
	17.04.2023	Version 1.0	Page 1 de 24

CORAL Methodology and Conformity Assessment Guidance v1.0

A CORAL project deliverable

	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)		
	CORAL Methodology and Conformity Assessment Guidance		
	17.04.2023	Version 1.0	Page 2 de 24



Document working group

Name	Affiliation	Role
Dominique Kogue	LHC	Contributor
Gabriela Gheorghe	LHC	Contributor
Jean Lancrenon	ILNAS	Contributor
João Dos Santos	ILNAS	Contributor

Document history

Version	Date	Changes from previous
0.1	15/11/2022	Creation of this document, continuation of a previous document meant initially to serve as this deliverable.
1.0	17/04/2023	First version


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 Call¹. The contents of this publication are the sole responsibility of ILNAS and do not necessarily reflect the opinion of the European Union.


Acronyms

Acronym	Full meaning
ANEC GIE	<i>Groupement d'Intérêt Economique Agence pour la Normalisation et l'Economie de la Connaissance</i>
CAB	Conformity Assessment Body
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CORAL	cybersecurity Certification based On Risk evALuation and treatment

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


	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)		
	CORAL Methodology and Conformity Assessment Guidance		
	17.04.2023	Version 1.0	Page 3 de 24

CSA	Cybersecurity Act
CISA	Certified Information Systems Auditor
ECSF	European Cybersecurity Skills Framework
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUCC	European Cybersecurity Certification Scheme on Common Criteria
EUCS	European Certification Scheme for Cloud Services
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
ILNAS	<i>Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services</i>
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
LHC	Luxembourg House of Cybersecurity
NAB	National Accreditation Body
SME	Small and Medium Enterprise

	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)		
	CORAL Methodology and Conformity Assessment Guidance		
	17.04.2023	Version 1.0	Page 4 de 24

Contents

Document working group.....	2
Document history	2
European Union funding.....	2
Acronyms	2
1. Introduction	5
The CORAL project.....	5
Purpose and scope of this CORAL deliverable	5
Important disclaimer	6
Structure.....	6
2. The relation between the methodology, the questionnaires and the CSA's certification schemes.....	7
CSA schemes covering the 'basic' level of assurance	7
The particular case of the EUCS.....	7
3. Conformity assessment procedure integrating the CORAL methodology	8
Overview of conformity assessment in general at the assurance level 'basic' of the CSA	8
Description of the CORAL methodology	9
Placement of the CORAL methodology in the general conformity assessment process.....	13
4. The Fit4CSA tool and its scoring scale calculation	13
A description of the Fit4CSA tool.....	13
The scoring scale calculation	14
Limitations to the scoring approach	16
5. Auditor profile	16
Baseline profile source	17
Derived CORAL auditor profile.....	19
6. Conclusion	23

	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)		
	CORAL Methodology and Conformity Assessment Guidance		
	17.04.2023	Version 1.0	Page 5 de 24

1. Introduction

The CORAL project

The *cybersecurity Certification based On Risk evALuation and treatment (CORAL)* research project (Action no. 2020-LU-IA-0209, benefitting from EU funding under the 2020 CEF Telecom Call²) aims to elaborate a toolkit and methodology to speed up the certification process in line with the Regulation (EU) 2019/881 (Cybersecurity Act - CSA)³ in what concerns the conformity self-assessment and the basic level of assurance, as well as to enhance the exchange of good practices, collaboration and information sharing related to performing evaluations in line with this act. In particular, this project will develop a light, efficient and straightforward evaluation method in line with the technical objectives of Article 51 of the CSA and based on risk assessments, to achieve a basic assurance level. This evaluation method will apply to Small and Medium Enterprises (SMEs) that are in charge of Information and Communication Technology (ICT) products, services or processes, acting in any sector and in any EU country. This method will also be used for conformity self-assessments, also possible with the entry into force of the CSA. The project partners are:

- The Luxembourg House of Cybersecurity⁴ (LHC);
- The *Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)*⁵; and
- The *Agence pour la normalisation et l'économie de la connaissance (ANEC GIE)*⁶.

More information on the CORAL project and its partners can be found on the project website: <https://coral-project.org/>.

Purpose and scope of this CORAL deliverable

This deliverable describes two outputs of the CORAL project:

- A methodology to streamline the processes of certification, or issuance of an EU declaration of conformity, at the basic level of assurance. This methodology is aimed at providers that are SMEs, for whom it is particularly important to keep costs as low as possible, and complexity minimal. The methodology proposed consists essentially in the following 3 steps:
 - **A set of standards-based questionnaires.** Answering a multiple-choice questionnaire covering a range of cybersecurity topics that are applicable to the provider's product, service or process. CORAL has so far elaborated four such questionnaires applicable respectively to generic ICT products, generic ICT services, generic ICT processes, and web applications. These


² <https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2020-cybersecurity>

³ Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) <https://eur-lex.europa.eu/eli/reg/2019/881/oj>

⁴ <https://lhc.lu/>

⁵ <https://portail-qualite.public.lu/fr/acteurs/ilnas.html>

⁶ <https://portail-qualite.public.lu/fr/acteurs/gie-anec.html>

	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)		
	CORAL Methodology and Conformity Assessment Guidance		
	17.04.2023	Version 1.0	Page 6 de 24

are based on well-known international technical standards or recognized technical specifications, and the project considers that they are easy to align to current or future CSA certification schemes. For more details on the relation between the questionnaires and CSA schemes, see Section 0

- **Attribution of a maturity score and issuance of recommendations.** Based on the answers provided, a score is attributed (see Section 4 for details on this score), and depending on whether or not a certain threshold is attained, the provider is invited to either launch a certification process (or issue an EU declaration of conformity), or implement further recommendations suggested by the questions.
- **External audit conditioned by a minimum score and based on existing filled-in questionnaire.** CORAL envisages the placement of the above steps at the beginning of any CSA scheme's procedure for certification or issuance of EU declarations of conformity. In the certification case, the output of the CORAL method can be used by auditors as a base of the questions to further investigate. In the case of conformity self-assessment issuance, as soon as templates become available for EU declarations of conformity, the tool will integrate these in order to directly generate the complete declaration itself. (At the time of writing of this deliverable, no CSA scheme allows issuance of EU declarations of conformity.)

The project has implemented this methodology in an open-source, online proof-of-concept tool named Fit4CSA that can be launched by following this link: <https://fit4csa.nc3.lu/survey/>. After the (selection and) completion of a given questionnaire, the tool automatically computes the score and generates a report complete with recommendations for those questions not optimally answered. It is recommended that the questionnaires be answered by a person or team with some familiarity in information security in their domain.

- **Proposal of an auditor profile.** Finally, the CORAL project also proposes a baseline profile for auditors in charge of assessing the conformity at the basic level of assurance. CORAL posits that this profile is, similarly to the questionnaires, easily adaptable to current or future CSA schemes.


Important disclaimer

The authors stress that merely adopting and following the methodology does not necessarily yield successful certification or a finalized and correct EU declaration of conformity. Only following the processes precisely defined by the schemes themselves can accomplish this. The objective is for the methodology to support in the achievement of these processes, not to guarantee their success.

Structure

This document

The rest of this deliverable is structured as follows. Section 0 details how the methodology and Fit4CSA tool relate to CSA certification schemes. Section 3 gives some context on conformity assessment in the CSA framework, explains the CORAL methodology, and then proceeds to explain where the CORAL methodology can play a role. A more involved description of the Fit4CSA online tool and the underlying

	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)		
	CORAL Methodology and Conformity Assessment Guidance		
	17.04.2023	Version 1.0	Page 7 de 24

scoring scale is in Section 4. Finally, Section 5 contains a baseline auditor profile corresponding to the CORAL methodology and Section 6 concludes the report.

2. The relation between the methodology, the questionnaires and the CSA's certification schemes

CSA schemes covering the 'basic' level of assurance

At the time of writing of this deliverable, only two CSA schemes are close to being available for the ICT market: the European Cybersecurity Certification Scheme on Common Criteria⁷ (EUCC) and the European Certification Scheme for Cloud Services⁸ (EUCS). The EUCC is targeted at general IT products, is based on the Common Criteria and Common Evaluation Methodology⁹ (also known as the ISO/IEC 15408 and ISO/IEC 18045 series of standards), and covers assurance levels 'substantial' and 'high'. The EUCS is aimed at cloud computing service provisioning, has its own tailored set of security requirements (contained in Annex A of the most recent available public draft from December 2020, and in the process of being standardized by CEN/CLC/JTC 13 Cybersecurity and Data Protection¹⁰), and covers levels 'basic', 'substantial', and 'high'. At level 'basic', the EUCS does not allow issuance of EU declarations of conformity.

CORAL's objective is to provide a methodology, including security requirements and recommendations, to aid in obtaining certification or issuance of EU declarations of conformity at level 'basic' for ICT products, services, and processes. Thus, there is no intersection with EUCC and there is a level of intersection with EUCS. Furthermore, it is certain that as the CSA framework matures and subsequent schemes are issued covering level 'basic', CORAL will intersect with those as well.

Yet, it is not the intention of the project to compete with these, which would make no sense in the overall CSA ecosystem. Rather, the project posits that:

- In the absence of a scheme covering a particular topic, users of the CORAL methodology will still end up both in a better security posture, and in a better position to eventually conform to such a scheme should one eventually be published; and
- Once a scheme on a particular topic is published, the CORAL methodology – in particular the questionnaires and scoring scales – can be easily adapted to the requirements of that scheme, thereby turning the intersection into an alignment.

The particular case of the EUCS


Since cloud services are certainly ICT services, the CORAL questionnaire was designed as a generalization of the EUCS' Annex A requirements. This way, it is easy to re-align completely once the need arises.

⁷ <https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1>

⁸ <https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme>

⁹ <https://www.commoncriteriaportal.org/>

¹⁰ https://standards.cencenelec.eu/dyn/www/?p=205:110:0:::FSP_PROJECT,FSP_LANG_ID:74247,25&cs=19E6889B88C3ECD7CB6C5AFAF4C31DA2C

	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)		
	CORAL Methodology and Conformity Assessment Guidance		
	17.04.2023	Version 1.0	Page 8 de 24

3. Conformity assessment procedure integrating the CORAL methodology

Overview of conformity assessment in general at the assurance level 'basic' of the CSA

Actors involved

The main actors involved in conformity assessment at the assurance level 'basic' or the CSA are the following:

- The manufacturer of the product/provider of the service/provider of the process. For the remainder of the deliverable, we shall simply use the terms 'provider' and 'object of evaluation' to designate the manufacturer/provider and product/service/process, respectively;
- The conformity assessment body (CAB), in case a certification is sought;
- The national cybersecurity certification authority (NCCA);
- The national accreditation body (NAB).

These four bodies are set on two different planes of governance:

- A lower plane that concerns itself with the provisioning of the object of evaluation and its cybersecurity assessment against a CSA scheme. Here intervene the provider and, in case certification is sought, the conformity assessment body (CAB);
- An upper plane that concerns the continuous monitoring of compliance of the object of evaluation against its certification or EU declaration of conformity, and of the overall certification process' conformance to the CSA. Here intervene the NCCA, CAB and NAB.

The methodology proposed by the project, including in particular the placement of the tool, is in the lower plane. The upper plane can be implemented without difficulty on top of the existing tool, should a CAB take on the CORAL approach and build on the source code of the existing tool.

Process of conformity assessment

The exact details of the processes of either issuance of an EU declaration of conformity or earning a certification at level basic are completely scheme-dependent, and at the time of writing of this deliverable not fully determined even for established schemes, such as the EUCS¹¹. However, in all cases, there is a phase in which the provider constructs, for the purpose of backing up claims of conformity, documentary evidence that the requirements specified in the scheme are met:

- In the case of an EU declaration of conformity, for the purpose of NCCA monitoring of compliance,

¹¹ Annex D of the December 22nd, 2020 version of the EUCS begins by stating that "some important templates [...] are missing".

- In the case of certification, for the CAB to be able to perform the audit. According to Article 52, Paragraph 5 of the CSA, it may even be the case that documentation review forms the full basis of the assessment. See Figure 1 for the case of a (very simplified) certification process.

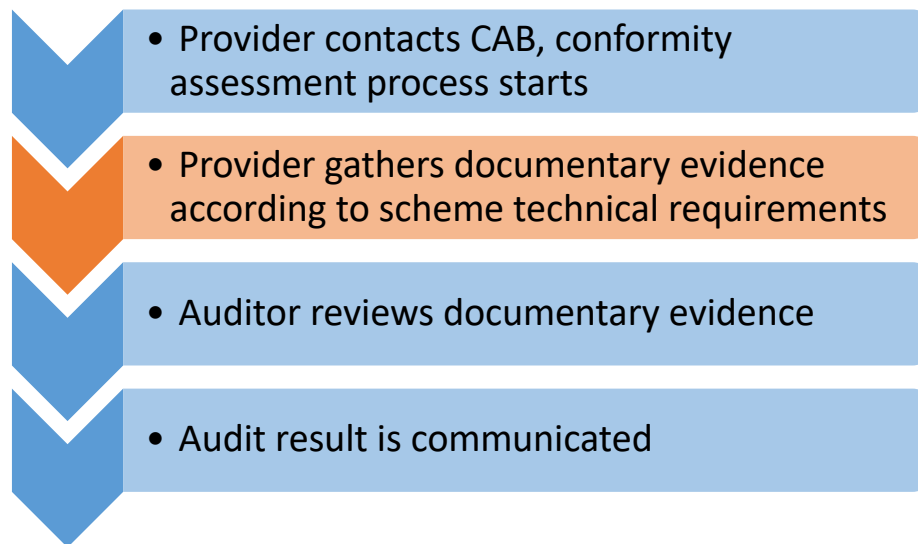


Figure 1: Placement (orange box) of documentary evidence provisioning in a typical simplified certification process

Description of the CORAL methodology

Main stages

CORAL proposes three main stages as part of the assessment process, see Figure 2.

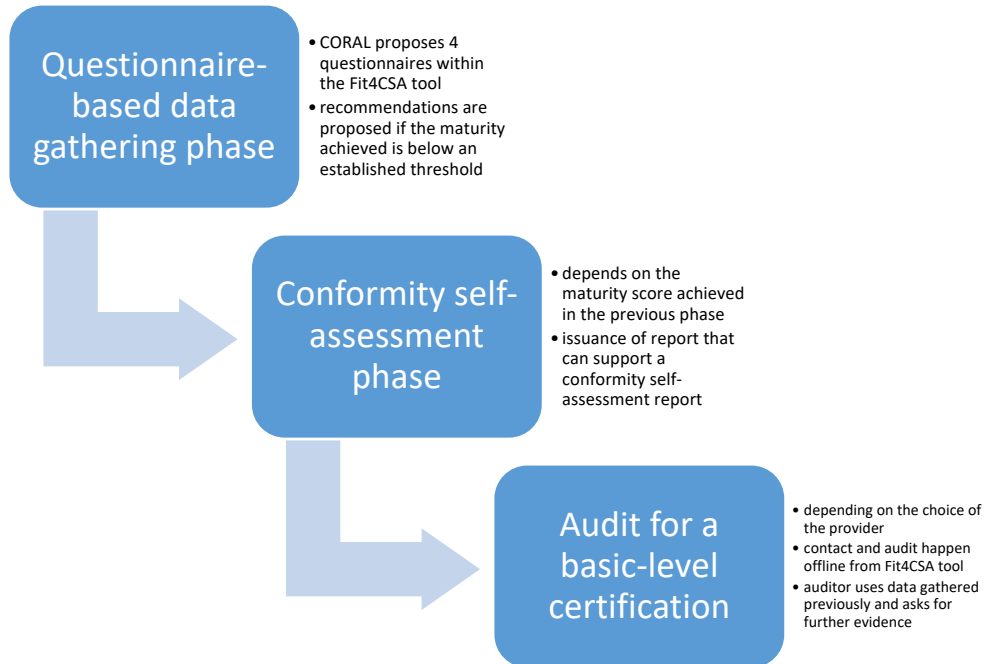



Figure 2: The CORAL assessment process

- The first stage, the so-called “Questionnaire-based data gathering” stage, is that of the filling-in of one of the CORAL questionnaires, based on what the object of the evaluation is (an ICT process, service or product). If the maturity is not satisfactory, the provider is given detailed recommendations to follow to improve its cybersecurity standing.
- The second stage is that of the conformity self-assessment, if the maturity achieved in the previous phase is satisfactory. As the template of an EU declaration of conformity is dependent on the scheme used, and due to lack of any readily-available conformity self-assessment template for any of the existing EU candidate schemes at the time of writing this report, the CORAL tool cannot be used to issue such a declaration until official templates come into existence, and the tool can be adapted. Therefore, CORAL can only claim that the report at this stage can serve as a basis for a conformity self-assessment, once scheme-dependent templates are available.
- The third stage is reached once the provider wishes to achieve a basic-level certification, in which case its details are registered on the platform, a document is generated for an auditor’s use, and, if the auditor’s evaluation is positive (based on an offline exchange of evidence with the provider), the details related to a new basic-level certification would be generated, recorded, and shared with the provider. We stress again that (see also the **Important disclaimer** in the Introduction of this deliverable) the mere usage of the CORAL methodology does not automatically yield a positive certification result. This remains strictly up to the CAB.

	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)		
	CORAL Methodology and Conformity Assessment Guidance		
	17.04.2023	Version 1.0	Page 11 de 24

Of course, it may very well be the choice of the provider to simply issue an EU declaration of conformity. In other words, there is no obligation to pursue with the third stage, unless a certification is what is wanted.

An iterative use of the Fit4CSA tool in the first phase

Fit4CSA is to be used in the first phase, on questionnaire-based data gathering. It is destined to be used in iterations, as follows (see also Figure 3):

1. The provider picks which is the type of object of evaluation (an ICT process, ICT service, or ICT product) that they wish to further assess within the CORAL methodology and tool;
2. The provider assesses its object of evaluation by answering the tool's questions;
3. At each question, the provider establishes which documentation, if any, supports its response, usually to justify the satisfaction of a control in place or requirement;
4. At the end of the questionnaire, the provider has a final score, a mapping of evidence for its responses, and a list of recommendations from the tool, usually to improve on unsatisfied requirements;
5. Depending on the final score obtained, the provider either:
 - a. concludes that its object of evaluation has sufficient cybersecurity maturity and supporting documented evidence to launch a certification procedure or issue an EU declaration of conformity or;
 - b. concludes that its object of evaluation is insufficiently mature, in which case it takes the tool's recommendations and improves its object of evaluation;
6. In case of 5.b, after putting into place the tool recommendations, the provider reassesses its object of evaluation through the tool, with the objective of arriving at a satisfying maturity level.

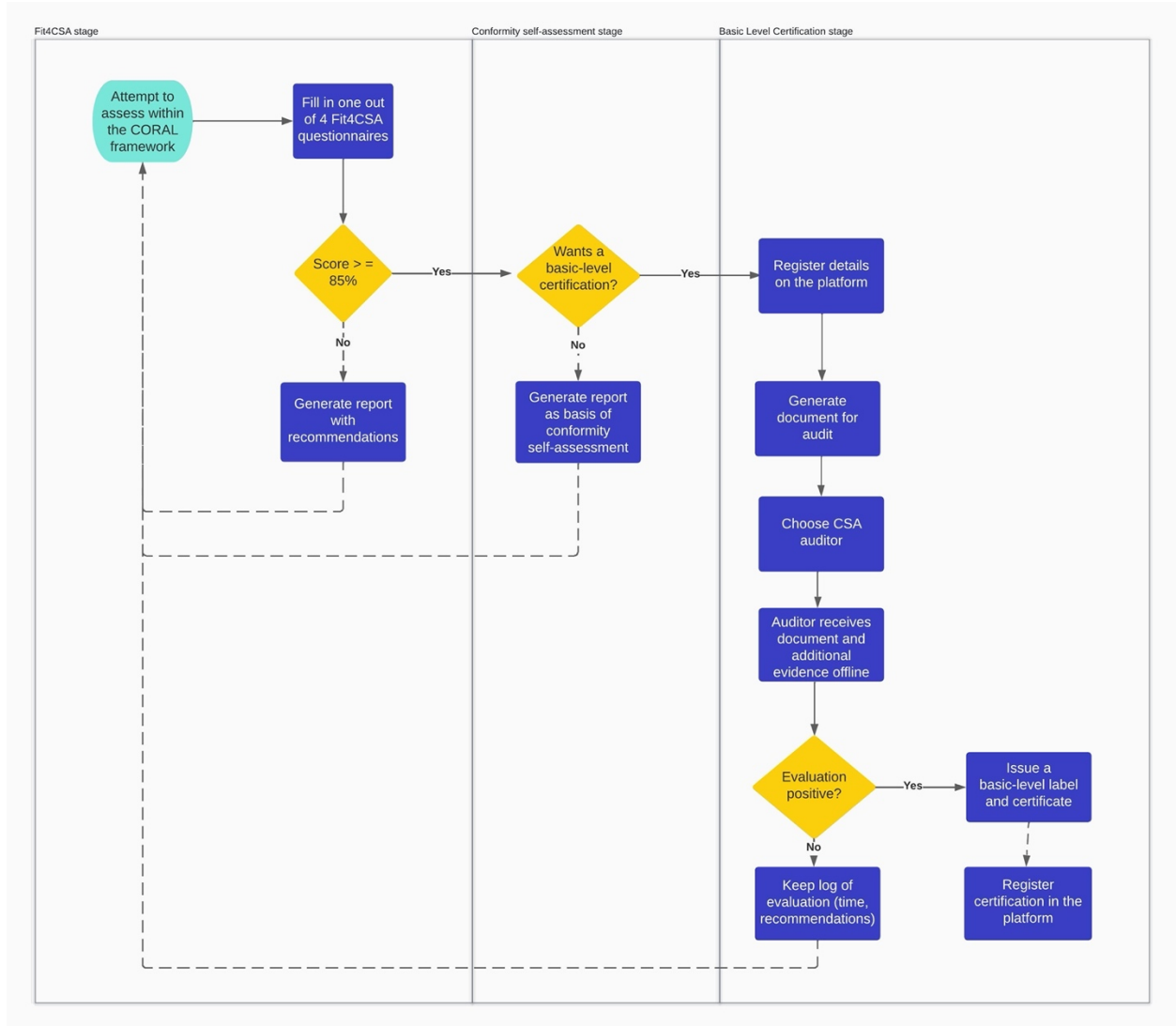



Figure 3: Iterations of uses of Fit4CSA

After using the tool, possibly in multiple iterations, the provider should have, following its last use of the tool, and as a final output:

1. An object of evaluation at an acceptable level of security for the assurance level 'basic';
2. A mapping giving a correspondence between desired security requirements and implemented controls, and documentation that serves as evidence that these are in place.

This final output can serve as the basis of technical evidence:

- For an auditor from a conformity assessment body in the context of a certification at level 'basic';

	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)		
	CORAL Methodology and Conformity Assessment Guidance		
	17.04.2023	Version 1.0	

- For anybody interested – in particular, an NCCA - in verifying the assurance level claimed in an EU declaration of conformity.

Placement of the CORAL methodology in the general conformity assessment process

The CORAL project methodology is destined first to aid in making the decision to actually go for a certification or a self-assessment, and second to support the particular step in the general process of gathering documentary evidence. Ideally, the provider would run the CORAL methodology prior to the certification/self-assessment process first as a maturity check, and second in preparation for the documentary evidence gathering.

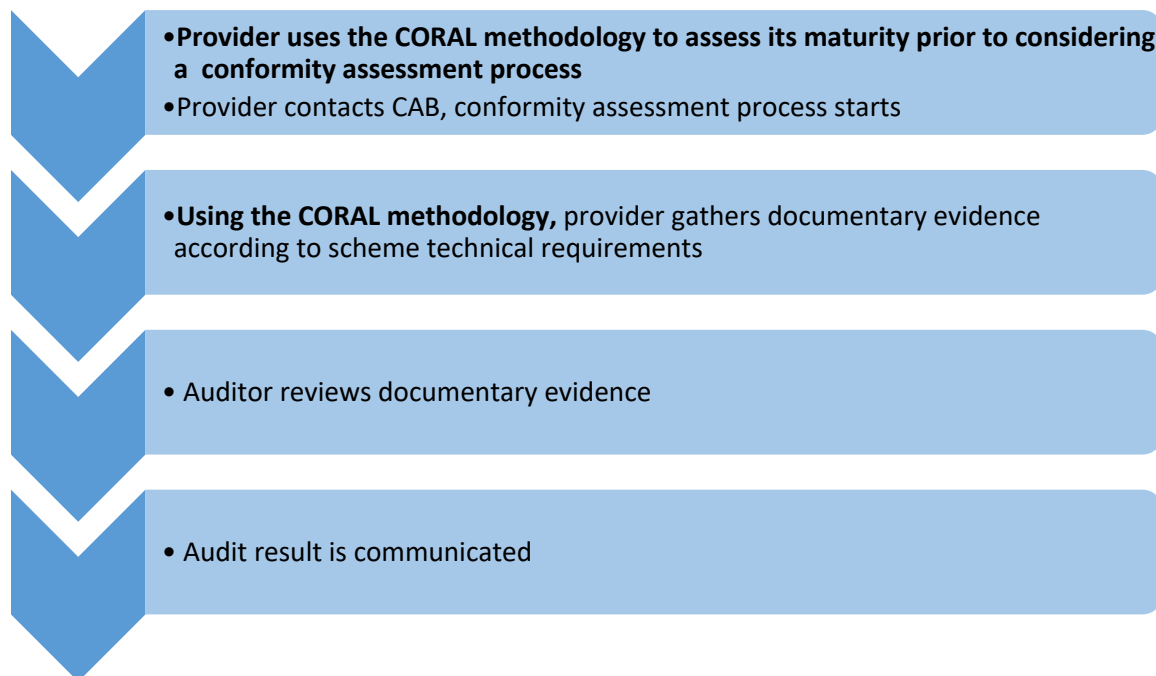


Figure 4: Placement of the CORAL methodology in the overall conformity assessment process

4. The Fit4CSA tool and its scoring scale calculation

A description of the Fit4CSA tool

Fit4CSA presents itself in the form of an online tool (<https://fit4csa.nc3.lu/survey/>) that proposes a set of questionnaires. Providers of products, processes or services answer the questionnaire the most suitable for their category of object of evaluation. Each question is assigned a maximum amount of points. Depending on how a given question is answered, a certain score out of the question's maximum is awarded. Once the questionnaire is completed, an overall score on a scale of 0 to 100 is calculated at the end for the entire questionnaire, as a percentage based on the ratio of points obtained out of the global possible maximum.

The final overall score approximates the maturity level of the object of evaluation in terms of cybersecurity, in particular attempting to “measure” how ready it is for a certification or an EU declaration of conformity, in accordance with Table 1 below.

Score	Conclusion
100	Ready to launch a certification process or to issue an EU declaration of conformity
85 to 99	Some changes required prior to launching a certification process or to issue an EU declaration of conformity
< 85	Many improvements required prior to launching a certification process or to issue an EU declaration of conformity

Table 1: Overall scoring result interpretation

The tool also generates a report that provides recommended actions to take whenever a question was not answered in an optimal manner. This allows providers of those objects of evaluation that did not score as desired to immediately take concrete steps towards amending that object of evaluation, with a view towards improving their posture from a cybersecurity certification maturity point-of-view.

The scoring scale calculation


Here we detail how the tool’s scoring scale is designed. There are, at the time of writing, four questionnaires each corresponding to one of the four categories below:

- IT products in general (these can be software, hardware or anything in between);
- Web applications;
- IT services in general;
- IT processes in general.

The project’s view is that a scoring scale on a set of questions that lead to recommendations and a risk assessment that assigns risk reduction to a certain pre-evaluated level of risk are not so different in nature. In particular, they both suffer from a more-or-less uncontrolled level of subjective choice. That is, no matter how refined the formulae one devises, there are always subjective inputs fed to give life to these formulae to obtain a final estimate. The main objective in any case is to try and find a way to refine the inputs to minimize this subjectivity to some extent.

In the particular case at hand, challenges encountered in coming up with a reasonable scoring scale resided mainly in the level of generality that is sought, in particular in the three general questionnaires, and finding adequate and explainable subcategories to aggregate to reach a given score for each question.

At the same time, the overall methodology in the CORAL project being aimed at the basic level of assurance implies that having a scoring method that is too intricate provides little additional value,

	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)		
	CORAL Methodology and Conformity Assessment Guidance		
	17.04.2023	Version 1.0	Page 15 de 24

especially since the end user of the tool is not necessarily interested in the details of these calculations. Thus, it was decided to limit these subcategories, or scoring dimensions, to no more than three.

In summary, for each questionnaire, three “dimensions” were selected in order to assign a maximum score to each question.

For the questionnaires on products and web applications, the three dimensions considered are the classic information security properties “**confidentiality**” (C), “**integrity**” (I), and “**availability**” (A). These are well suited for the case at hand because the controls underlying the questions that are asked are mostly relatable to these categories.

For the questionnaires on services and processes, the three dimensions considered are:

- **The scope** of the underlying control. We consider that the scope in the organization goes from 1 (a limited part of the organization), to 2 (a substantial part of the organization, e.g., a department), or 3 (a large part of the organization, or a core service);
- The control’s **applicability in terms of timing**. For timing, we consider it can have one of three values: 1 (activated only in case of exceptional circumstances), 2 (often, but at certain times, or a recurring event), and 3 (in affect at all times);
- Finally, an assessment of **whether the security provided by the measure is direct or indirect**. We consider that 1 is an indirect impact (because it relies on something else being enforced), or 2 (provides security immediately once in place).

These properties were chosen because traditional security properties like C-I-A cannot be applied for services and processes. Instead, they are inferred from the common feature of processes and services: the procedural / organizational aspect of instating security controls that ensure C-I-A.


Products

Each question is given:

- a weight C of 0, 1, 2, or 3 for relevance to confidentiality;
 - a weight I of 0, 1, 2, or 3 for relevance to integrity;
 - a weight A of 0, 1, 2, or 3 for relevance to availability;
1. These weights are added, to get a pre-score P of 0 to 9. In other words, $P = C+I+A$;
 2. The pre-score X is multiplied by 5 to get a max score M of 0 to 45. In other words, $M = 5 \cdot P$;
 3. Scores are linearly distributed between 0 and M per answer within a given question when there is only one possible answer. When multiple answers are possible, scores are added, but never exceed M.

Web applications

1. Each question is given:
 - a weight of 0, 1, or 2 for relevance to confidentiality;
 - a weight of 0, 1, or 2 for relevance to integrity;

	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)		
	CORAL Methodology and Conformity Assessment Guidance		
	17.04.2023	Version 1.0	Page 16 de 24

- a weight of 0, 1, or 2 for relevance to availability;
2. These weights are added, to get a pre-score P of 0 to 6. In other words, $P = C+I+A$;
 3. The pre-score X is multiplied by 5 to get a max score M of 0 to 30. In other words, $M = 5 * P$;
 4. Scores are linearly distributed between 0 and M per answer within a given question when there is only one possible answer. When multiple answers are possible, scores are added, but never exceed M.

A note on the scoring philosophy difference between the case of products and the case of web applications

In the case of products, the “C-I-A” weight assigned to a given question ranges from 0 to 3, whereas in the case of web applications it ranges from 0 to 2. This is because in the “product” questionnaire, there are controls considered that are also more organizational in nature. Thus, there needed to be a way to force a level of C-I-A score onto them. The best way to do this appeared to be to give a bit more leeway in intermediate scoring values to better gauge the relevance of the control to the C-I-A.

Services and processes


1. Each question is given:
 - a weight of 1, 2, or 3 for scope of the control on the overall service;
 - a weight of 1, 2, or 3 for the timing of the control on the overall service;
 - a weight of 1 or 2 depending on whether the measure indirectly or directly affects security;
2. These weights are multiplied, to get a pre-score P of 1, 2, 3, 4, 6, 8, 9, 12 or 18;
3. The pre-score X is multiplied by 5 to get a max score M of 1, 10, 15, 20, 30, 40, 45, 60 or 90. In other words, $M = 5 * P$;
4. Scores are linearly distributed between 0 and M per answer within a given question when there is only one possible answer. When multiple answers are possible, scores are added, but the total never exceeds M.

Limitations to the scoring approach

The main limitation is that although there is a rationale behind the scoring justification, it remains quite subjective in nature. The project’s view is that it remains sufficient for the purpose of maturity estimation at a basic level of assurance. Anything more complex would be of limited additional value.

5. Auditor profile

In this section, we give a description of the profile that auditors ought to fit in order to evaluate the methodology’s output against a CSA scheme. Given that the project is focused on the basic level of assurance, and that the methodology and questionnaires will certainly evolve as new certification schemes are published, a single profile is presented to cover the whole methodology, and in particular all four existing questionnaires. Of course, this profile can also evolve; in particular, it can be made more specific depending on future scheme needs, such as those stemming from any specific requirements in conformity assessment methodologies.

	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)		
	CORAL Methodology and Conformity Assessment Guidance		
	17.04.2023	Version 1.0	Page 17 de 24

Baseline profile source

In the context of the general assessment of cybersecurity skills in Europe, ENISA has devised a European Cybersecurity Skills Framework (ECSF)¹², describing in particular a set of 12 different baseline profiles¹³ that are commonly needed in the field of cybersecurity transversally across the digital single market. One of these profiles is the 'cybersecurity auditor', found in Section 2.6 of the European Cybersecurity Skills Framework Role Profiles document.

By design, the ECSF also provides the necessary flexibility to alter these baseline profiles according to specific needs. Thus, this is the case for the 'cybersecurity auditor' profile as well, with the needs in question originating in CSA cybersecurity schemes.

Table 2 below simply recalls the baseline 'cybersecurity auditor' profile from the ECSF. For details on the chosen descriptors in the left-hand column, except for the last one, we invite the reader to consult the ECSF.

The descriptor in the last row – the e-Competence levelling – warrants a bit more explaining. It is a direct application of a scale defined in Annex A of the standard *EN 16234-1:2019 e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all sectors - Part 1: Framework*¹⁴. This scale measures the overall competence level of a given individual, on a scale of 1 to 5, with 1 being the lowest level of competence to 5 being the highest. Essentially, a level 1 individual is capable of performing pre-determined tasks in a structured and stable environment, while a level 5 individual is capable of determining overall strategy and providing leadership in highly fluid and unpredictable settings.


Subsequently, the table is adapted to describe a general profile to cover the CORAL methodology, see Table 3 and Table 4.

Profile Title	Cybersecurity Auditor
Alternative Title(s)	Information Security Auditor (IT or Legal Auditor) Governance Risk Compliance (GRC) Auditor Cybersecurity Audit Manager Cybersecurity Procedures and Processes Auditor Information Security Risk and Compliance Auditor Data Protection Assessment Analyst
Summary statement	Perform cybersecurity audits on the organization's ecosystem. Ensuring compliance with statutory, regulatory, policy information, security requirements, industry standards and best practices.
Mission	Conducts independent reviews to assess the effectiveness of processes and controls and the overall compliance with the organization's legal and regulatory frameworks policies. Evaluates, tests and verifies cybersecurity-


¹² <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf>

¹³ <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles>

¹⁴ https://standards.cencenelec.eu/dyn/www/f?p=205:110:0:::FSP_PROJECT:67073&cs=15E62ED24D608A5F10D6BEE8E6D50FA10

	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)		
	CORAL Methodology and Conformity Assessment Guidance		
	17.04.2023	Version 1.0	Page 18 de 24

	related products (systems, hardware, software and services), functions and policies ensuring, compliance with guidelines, standards and regulations.
Deliverable(s)	<ul style="list-style-type: none"> • Cybersecurity Audit Plan • Cybersecurity Audit Report
Main task(s)	<ul style="list-style-type: none"> • Develop the organization's auditing policy, procedures, standards and guidelines • Establish the methodologies and practices used for systems auditing • Establish the target environment and manage auditing activities • Define audit scope, objectives and criteria to audit against • Develop an audit plan describing the frameworks, standards, methodology, procedures and auditing tests • Review target of evaluation, security objectives and requirements based on the risk profile • Audit compliance with cybersecurity-related applicable laws and regulations • Audit conformity with cybersecurity-related applicable standards • Execute the audit plan and collect evidence and measurements • Maintain and protect the integrity of audit records • Develop and communicate conformity assessment, assurance, audit, certification and maintenance reports • Monitor risk remediation activities
Key skill(s)	<ul style="list-style-type: none"> • Organize and work in a systematic and deterministic way based on evidence • Follow and practice auditing frameworks, standards and methodologies • Apply auditing tools and techniques • Analyze business processes, assess and review software or hardware security, as well as technical and organizational controls • Decompose and analyze systems to identify weaknesses and ineffective controls • Communicate, explain and adapt legal and regulatory requirements and business needs • Collect, evaluate, maintain and protect auditing information • Audit with integrity, being impartial and independent
Key knowledge	<ul style="list-style-type: none"> • Cybersecurity controls and solutions • Legal, regulatory and legislative compliance requirements, recommendations and best practices • Monitoring, testing and evaluating cybersecurity controls' effectiveness • Conformity assessment standards, methodologies and frameworks • Auditing standards, methodologies and frameworks

	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)		
	CORAL Methodology and Conformity Assessment Guidance		
	17.04.2023	Version 1.0	Page 19 de 24

	<ul style="list-style-type: none"> • Cybersecurity standards, methodologies and frameworks • Auditing-related certification • Cybersecurity-related certifications
e-Competences (from e-CF)	<ul style="list-style-type: none"> • B.3. Testing (Level 4) • B.5. Documentation Production (Level 3) • E.3. Risk Management (Level 4) • E.6 ICT Quality Management (Level 4)

Table 2: ECSF 'Cybersecurity Auditor' role profile


Derived CORAL auditor profile

Since the audit is essentially a review of technical documentation, there are *à priori* no activities related to testing. Furthermore, the basic level of assurance should generally be achieved in a framework that is stable and well understood. Hence, the e-Competence levelling was generally brought down to 2¹⁵. The technical documentation can include documentation not just on the product, service or process itself, but also on the provider's own processes. While the questionnaire is applicable in general, it is required that the evaluator have a good understanding of the technology area of the product, service, or process and its domain of application. The auditor shall also have solid knowledge of the CSA in general, and the relevant specific CSA scheme(s).


For ease of comparison, in Table 3 text in *purple italics* designates CORAL-specific additions or modifications to the baseline ECSF profile. Deletions of ECSF text are indicated using *struck-through-red italics*. Finally, for better readability, Table 4 contains a clean version of the CORAL profile table.

Profile Title	<i>CORAL</i> Cybersecurity Auditor
Alternative Title(s)	Information Security Auditor (IT or Legal Auditor) Governance Risk Compliance (GRC) Auditor Cybersecurity Audit Manager Cybersecurity Procedures and Processes Auditor Information Security Risk and Compliance Auditor Data Protection Assessment Analyst
Summary statement	Perform cybersecurity audits on the organization's <i>proposed product, service or process ecosystem</i> . Ensuring compliance with statutory, regulatory, policy information , <i>CSA scheme</i> security requirements <i>at the basic level of assurance</i> , industry standards and best practices .
Mission	Conducts independent reviews to assess the effectiveness of processes and controls and the overall compliance with <i>CSA scheme security requirements at level 'basic'</i> the organization's legal and regulatory frameworks policies .

¹⁵ According to Annex A of EN 16234-1:2019 e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all sectors - Part 1: Framework, level 2 corresponds to: "Operates with capability and independence in specified boundaries and may supervise others in this environment; conceptual and abstract model building using creative thinking; uses theoretical knowledge and practical skills to solve complex problems within a predictable and sometimes unpredictable context."

	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)		
	CORAL Methodology and Conformity Assessment Guidance		
	17.04.2023	Version 1.0	


	Evaluates, tests and verifies cybersecurity-related products (systems, hardware, software and services), functions and policies ensuring compliance with guidelines, standards and regulations properties of a product, service, process, or organization.
Deliverable(s)	<ul style="list-style-type: none"> • Cybersecurity Audit Plan • Cybersecurity Audit Report
Main task(s)	<ul style="list-style-type: none"> • Develop the organization's auditing policy, procedures, standards and guidelines • Establish the methodologies and practices used for <i>product, service, or process systems</i> auditing <i>according to the CSA scheme</i> • Establish the target environment and manage auditing activities • Define audit scope, objectives and criteria to audit against • Develop an audit plan <i>following the CSA scheme</i> describing the frameworks, standards, methodology, <i>and</i> procedures and auditing tests • Review target <i>product, service or process of evaluation</i>, security objectives and requirements based on the <i>CSA scheme risk profile</i> • Audit compliance with cybersecurity related applicable laws and regulations • Audit conformity with cybersecurity-related applicable standards • Execute the audit plan and collect evidence and measurements • Maintain and protect the integrity of audit records • Develop and communicate conformity assessment, assurance, audit, certification and maintenance reports • Monitor risk remediation activities
Key skill(s)	<ul style="list-style-type: none"> • Organize and work in a systematic and deterministic way based on evidence • Follow and practice auditing frameworks, standards and methodologies • Apply auditing tools and techniques <i>following the CSA scheme</i> • Analyze business processes, assess and review software or hardware security, as well as technical and organizational controls • Decompose and analyze <i>the product, service or process systems</i> to identify weaknesses and ineffective controls • <i>Performing documentation analysis</i> • Communicate, explain and adapt legal and regulatory requirements and business needs • Collect, evaluate, maintain and protect auditing information • Audit with integrity, being impartial and independent
Key knowledge	<ul style="list-style-type: none"> • Cybersecurity controls and solutions • <i>The overall CSA certification framework</i>

	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)		
	CORAL Methodology and Conformity Assessment Guidance		
	17.04.2023	Version 1.0	


	<ul style="list-style-type: none"> • <i>The relevant CSA certification scheme</i> • Legal, regulatory and legislative compliance requirements, recommendations and best practices <i>relevant to the CSA certification scheme</i> • Monitoring, testing and evaluating cybersecurity controls' effectiveness • Conformity assessment standards, methodologies and frameworks, <i>in particular the ISO/IEC 27000 series of standards related to ISMS and the ISO/IEC 21827 standard on</i> • Auditing standards, methodologies and frameworks, <i>such as those from ISACA's CISA</i> • Cybersecurity standards, methodologies and frameworks • Auditing-related certification • Cybersecurity-related certifications • <i>The technical area of the product, service or process</i> <ul style="list-style-type: none"> ○ <i>Intended or typical use</i> ○ <i>Intended or typical application domain</i> ○ <i>Development lifecycle</i> ○ <i>Design and architecture</i> • <i>The product, service, or process' specificities related to information security:</i> <ul style="list-style-type: none"> ○ <i>Notions of security functions (such as authentication; encryption; access control and rights, including for administrators; event logging and monitoring; clock accuracy; secure failure; backup and redundancy; key management; etc.)</i> ○ <i>Notions of vulnerability assessment, and being able to identify public vulnerability databases</i> ○ <i>Knowledge of typical threats to that product, service or process in its intended or typical application domain</i>
e-Competences (from e-CF)	<ul style="list-style-type: none"> • B.3. Testing (Level 4) • B.5. Documentation Production (Level 2 3) • E.3. Risk Management (Level 2 4) • E.6 ICT Quality Management (Level 2 4)

Table 3: CORAL auditor profile, with differences with base ECSF highlighted

Profile Title	CORAL Cybersecurity Auditor
Alternative Title(s)	-
Summary statement	Perform cybersecurity audits on the organization's proposed product, service or process. Ensuring compliance with CSA scheme security requirements at the basic level of assurance.
Mission	Conducts independent reviews to assess the effectiveness of processes and

	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)		
	CORAL Methodology and Conformity Assessment Guidance		
	17.04.2023	Version 1.0	

	controls and the overall compliance with CSA scheme security requirements at level 'basic'. Evaluates and verifies cybersecurity-related properties of a product, service, process, or organization.
Deliverable(s)	<ul style="list-style-type: none"> • Cybersecurity Audit Plan • Cybersecurity Audit Report
Main task(s)	<ul style="list-style-type: none"> • Establish the methodologies and practices used for product, service, or process auditing according to the CSA scheme • Establish the target environment and manage auditing activities • Define audit scope, objectives and criteria to audit against • Develop an audit plan following the CSA scheme describing the frameworks, standards, methodology, and procedures • Review target product, service or process, security objectives and requirements based on the CSA scheme • Audit conformity with cybersecurity-related applicable standards • Execute the audit plan and collect evidence and measurements • Maintain and protect the integrity of audit records • Develop and communicate conformity assessment, assurance, audit, certification and maintenance reports • Monitor risk remediation activities
Key skill(s)	<ul style="list-style-type: none"> • Organize and work in a systematic and deterministic way based on evidence • Follow and practice auditing frameworks, standards and methodologies • Apply auditing tools and techniques following the CSA scheme • Analyze business processes, assess and review software or hardware security, as well as technical and organizational controls • Decompose and analyze the product, service or process to identify weaknesses and ineffective controls • Performing documentation analysis • Collect, evaluate, maintain and protect auditing information • Audit with integrity, being impartial and independent
Key knowledge	<ul style="list-style-type: none"> • Cybersecurity controls and solutions • The overall CSA certification framework • The relevant CSA certification scheme • Legal, regulatory and legislative compliance requirements, recommendations and best practices relevant to the CSA certification scheme • Monitoring and evaluating cybersecurity controls' effectiveness • Conformity assessment standards, methodologies and frameworks, in particular the ISO/IEC 27000 series of standards related to ISMS and the ISO/IEC 21827 standard on

	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)		
	CORAL Methodology and Conformity Assessment Guidance		
	17.04.2023	Version 1.0	

	<ul style="list-style-type: none"> • Auditing standards, methodologies and frameworks, such as those from ISACA's CISA • Cybersecurity standards, methodologies and frameworks • Auditing-related certification • Cybersecurity-related certifications • The technical area of the product, service or process <ul style="list-style-type: none"> ○ Intended or typical use ○ Intended or typical application domain ○ Development lifecycle ○ Design and architecture • The product, service, or process' specificities related to information security: <ul style="list-style-type: none"> ○ Notions of security functions (such as authentication; encryption; access control and rights, including for administrators; event logging and monitoring; clock accuracy; secure failure; backup and redundancy; key management; etc.) ○ Notions of vulnerability assessment, and being able to identify public vulnerability databases ○ Knowledge of typical threats to that product, service or process in its intended or typical application domain
e-Competences (from e-CF)	<ul style="list-style-type: none"> • B.5. Documentation Production (Level 2) • E.3. Risk Management (Level 2) • E.6 ICT Quality Management (Level 2)

Table 4: CORAL auditor profile


6. Conclusion

This deliverable details the main output of the CORAL project: a methodology to streamline the processes of either obtaining a certification at level 'basic' or issuing an EU declaration of conformity in the context of the European Union's Cybersecurity Act.

The methodology can be essentially plugged into any conformity assessment process defined by a CSA certification scheme, and is destined for use by SMEs in order to keep costs at a minimum.

It is technically supported by an online tool named Fit4CSA (which can be launched as this link: <https://fit4csa.nc3.lu/survey/>), which is open-source and anonymized as much as possible¹⁶. This tool is based on questionnaires that a provider may answer in order to evaluate one's security posture on a product, service or process. Following completion of the questionnaire, a report complete with

¹⁶ More specifically, the tool requires identification only in case one wishes to register through it in order to be put into contact with potential auditors. All steps prior to this, including the issuance of the questionnaire report and recommendations, are anonymous.

	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)		
	CORAL Methodology and Conformity Assessment Guidance		
	17.04.2023	Version 1.0	

recommendations is issued. CORAL recommends that the questionnaire be answered by individuals with some information security familiarity in their domain or industry. The report itself could potentially serve as evidence in the context of a conformity assessment, or – once official appropriate templates are available and the tool is adapted to them – as a complete EU declaration of conformity.

The underlying questionnaires are malleable enough to be adapted to CSA schemes as these become progressively available.

The CORAL project welcomes anyone interested to try out the tool and provide feedback to the project partners: <https://coral-project.org/community/2023/03/17/feasibility-study-started.html>.