About the CORAL project and its results

18.10.2023

CORAL's purpose

- **Bring CSA's <u>assurance level basic & conformity self-assessments</u> closer to the market**
  - 2 reasons why level basic is so important: pervasiveness + consumer reliance
  - Momentum: market preparation while official schemes including level basic are in the "making"
- **Primary focus on SMEs without neglecting the CSA ecosystem**
- **Contribute to the adoption of cybersecurity certifications in general**

CSA certification looks hard!

CSA certification seems expensive!

Is it worth the effort?

Don't know…

CSA certification is a challenge, but perhaps the effort is manageable.

We could consider to achieve an even higher CSA certification level
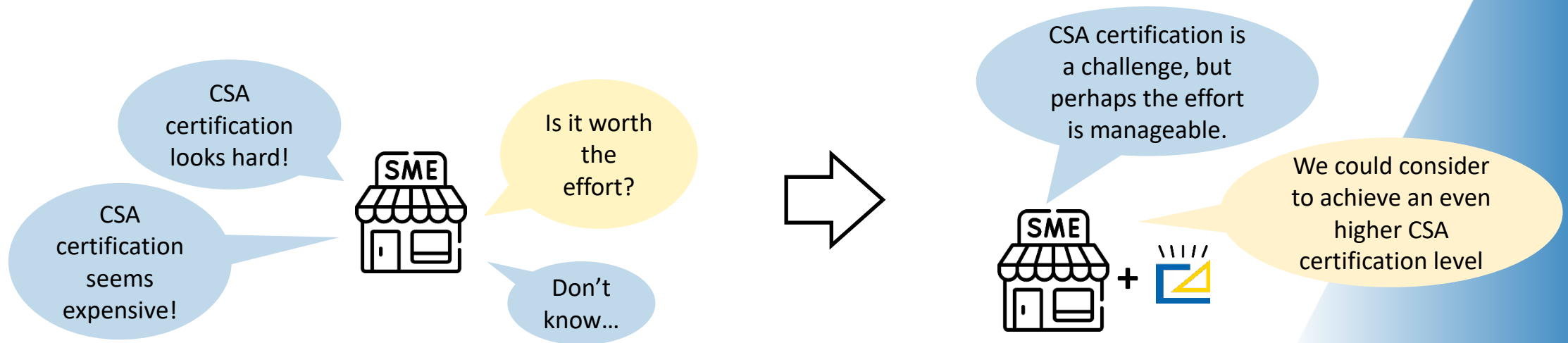
What CORAL is

Submission to a Connecting Europe Facility call in 2020

- 2020 CEF Telecom Call - Cybersecurity (CEF-TC-2020-2)
- Broad context: Support in implementing the Cybersecurity Act (CSA)

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

Some base information/resources

- Runs from September 2021 to October 2023
- CORAL website: https://coral-project.org/
- 3 Luxembourg partners

CORAL / Project partners

Luxembourg House of Cybersecurity (LHC, project lead)

- *Groupement d'Intérêt Economique*
- Mission to help improve cybersecurity posture of SMEs and public administrations in Luxembourg

Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS)

- Public administration under the Minister of the economy (Luxembourg)
- Multiple legal missions
- Luxembourg's NCCA (only supervision, not certification)

Agence pour la normalisation et l'économie de la connaissance (ANEC GIE)

- *Groupement d'Intérêt Economique*
- Supports ILNAS in its legal missions as national standards body

What are CORAL's objectives

- A <u>lightweight and straightforward</u> methodology to streamline the procedures of CSA certification at assurance level basic & conformity self-assessments
- Full reliance on existing schemes / standards
- Applicable in relation with the provision of either an ICT product, service or process
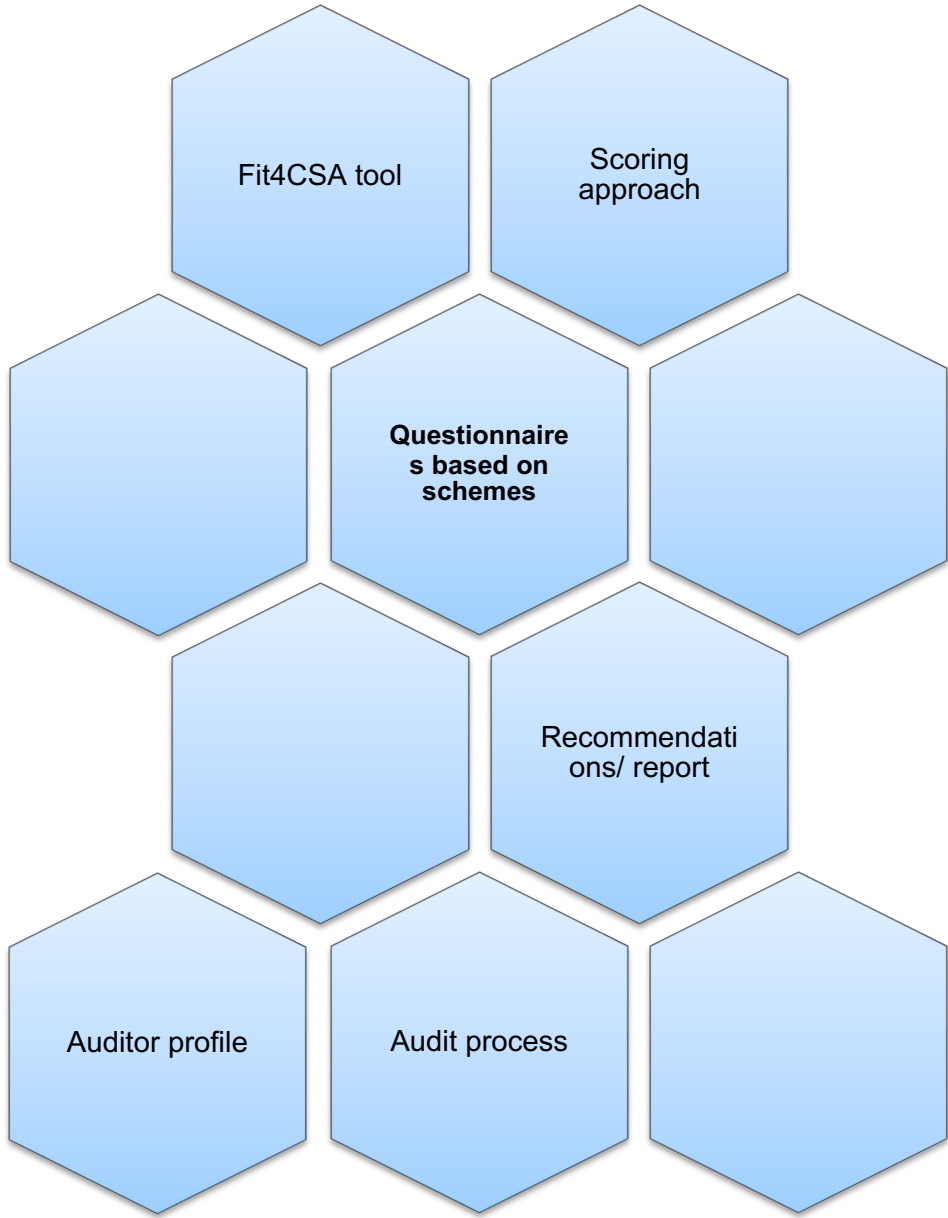
- Support for the auditor work related to the CSA certification al level basic
- An auditor profile adapted to perform this sort of assessment

- An open source tool for performing the assessment
- Terminology and report templates
- Promotion of process transparency and low cost evaluation with a view to achieve basic-level certification

The CORAL building blocks

Fit4CSA tool

Scoring approach

Questionnaires based on schemes

Recommendations/ report

Auditor profile

Audit process

The questionnaires and the standards landscape

The questionnaires

- How did the project "build" them?

State of the Art	⇒	Yielded multiple sub-categories, not always generic	⇒	Settled as a starting point on generic products, services, and processes + web applications

- Standards, specifications, best practices
- Took an ECSO* document as a baseline already-existing survey
- Added a few things
- Had a view towards making the questionnaires as generic as possible

- Lots of IoT
- Web applications
- Not much generic
- A lot more products than services or processes
- Added AI as a category

- Part of the stated project objectives to cover all three CSA categories 'products', 'services', 'processes'
- Multiplicity of large sub-categories cannot be ignored
- If the tool has uptake, will add more questionnaires as appropriate
- Could even cover 'managed security services' in the future…

The questionnaires and the standards landscape (2)

The questionnaires

- What they are

Products	Services	Processes

Products
- **Two** questionnaires
  - Generic (inspired by ISO/IEC 15408 *Evaluation criteria for IT security*)
  - Web applications (inspired by the OWASP *Application Security Verification Standard*)

Services
- Generic
- Inspired by EUCS Annex A
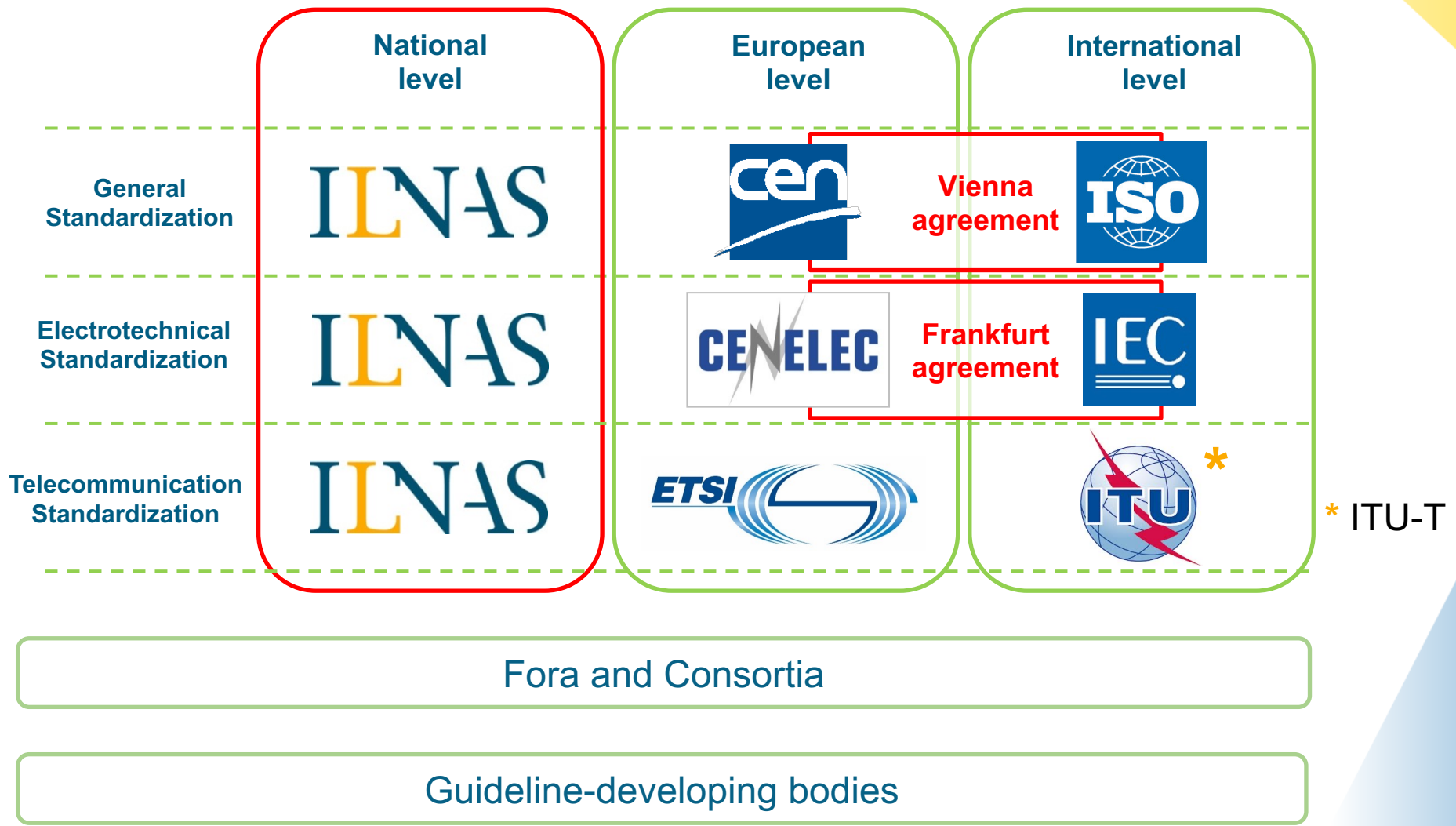- Aims to be a generalization of it

Processes
- Generic
- Inspired by ISO/IEC 21827 *Systems Security Engineering — Capability Maturity Model®*

More information in the deliverable:

The questionnaires and the standards landscape (3)

The CORAL approach to \<getting closer to\> CSA level basic

The self-assessment approach

1. Provider has a product, process or service that it either wants a 'basic' certification for, or to issue an EU DoC
2. Provider goes through the online Fit4CSA tool, fills out a security questionnaire relevant to the "target"
3. At the end, the provider is issued a score out of 100
4. For questions with non-optimal answers, recommendations are proposed (automatic report produced by the tool)
5. If the score is at least 85, the provider can consider launching a certification process or issuing an EU DoC

The process in detail is described in a deliverable on the website: "5. CORAL Methodology and Conformity Assessment Guidance v1.0"

The CORAL approach to <getting closer to> CSA level basic (2)

High level view of a conformity assessment process

- Provider contacts CAB, conformity assessment process starts
- Provider gathers documentary evidence according to scheme technical requirements
- Auditor reviews documentary evidence
- Audit result is communicated
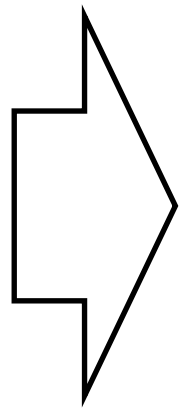
How CORAL could fit into this process

- **Provider uses the CORAL methodology to assess its maturity prior to considering a conformity assessment process**
- Provider contacts CAB, conformity assessment process starts
- **Using the CORAL methodology,** provider gathers documentary evidence according to scheme technical requirements
- Auditor reviews documentary evidence
- Audit result is communicated

The CORAL approach is not a full certification service in itself

The Fit4CSA Tool (1)

Welcome to Fit4CSA

Fit4CSA is a self-assessment tool to streamline the process of applying for a basic-level cybersecurity certification in the context of the CyberSecurity Act (CSA - EU 2019/881). Fit4CSA is part of the CORAL EU-funded project.

How does Fit4CSA work?

1. Select what you would like to assess: an ICT service, an ICT process, an ICT product - Web application or an ICT generic product.
2. Depending on your choice, you will need to fill in a questionnaire with both single choice and multiple choice questions. If you have supporting evidence for each of your answers (a policy, procedure, etc.), we recommend that you to keep track of this all throughout the questionnaire in order to establish a mapping of this evidence as you progress.
3. At the end of the survey, you will be given a score and a set of recommendations. Your Scybersecurity maturity can improve if you follow these recommendations.
4. If you scored at least 85%, Fit4CSA will additionally ask if you want a CSA conformity self-assessment, or to apply a basic-level certification. In the first case, you will be able to download the report with your answers and use it as a basis of your conformity self-assessment. In the second case, you will be asked to register and start an audit process based on the report issued within Fit4CSA. Keep in mind that all evidence supporting your answers might be requested later by the auditor of your choice.

The first 3 steps of this process are anonymous.

If at some point, you wish to continue the survey later, you click on the **Continue later button** and save the provided link separately. Using that link, you can pick up where you left off anytime.

Start

Continue a previous survey

Select the type of conformity self-assessment.

- ICT service
- ICT process
- ICT product - a Web Application
- ICT product - a generic product (not a Web application)

Continue later

Your feedback: Please let us know if anything can be improved in the question or its options.

* This text field should not be used to answer the question.
** Please do not provide any sensitive or confidential information referring to your identity.

5 of 42

Have you realized a vulnerability assessment of your product in order to identify and address potential vulnerabilities introduced during development or operation?

- No, there was not any vulnerability assessment conducted for the product.
- A vulnerability assessment has been conducted and all identified vulnerabilities have been remediated.

Back   Continue later   Next

Your feedback: Please let us know if anything can be improved in the question or its options.

* This text field should not be used to answer the question.
** Please do not provide any sensitive or confidential information referring to your identity.

The survey can be filled in anonymously until the score is computed and the report issued, the possibility to register presents when the score is high enough
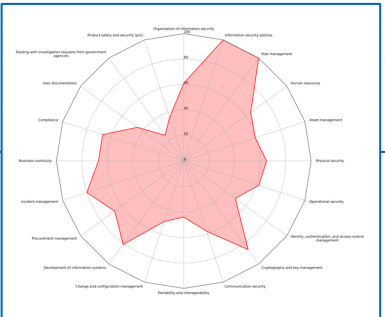
13

The Fit4CSA Tool (2)

CORAL
Cybersecurity certification based on risk evaluation and treatment

Table of contents

Summary:

Based on the answers selected for your category of self-assessment (an ICT service, an ICT process, an ICT Web application or an ICT generic product), please find here the following elements:

- the score you have achieved as a percentage of correctly answered questions,
- a list of recommendations that can be used to further improve the state of cybersecurity of your service/process/application/generic product,
- the report summarising and detailing the maturity of your service/process/application/generic product.

Congratulations, you have achieved a score of at least 85%! You can now move on to the next step: log in or create an account, in order to be able to manage your audit requests. Please save the below questionnaire ID to your filled-in survey, that you can use in the next steps: **4bdb6855-c95e-439f-843f-a2c0689d96d4**

99 /100
Report:

Download

Log in

Log in

Welcome to the Audit Module Fit4CSA
Audits

Name	Self-assessment id	Type of conformity	Audit company	Status	Actions
JeanTEST	4bdb6855-c95e-439f-843f-a2c0689d96d4	ICT product - a generic product (not a Web application)		Ongoing	

Add an audit

The audit module can be used to follow-up with an audit procedure, and see the auditor's verdict on each point

14

The Fit4CSA Tool (3)

Auditor module

Two role

- Audi
  of at
- Audi
  agre

The aud

An au

A proposed auditor profile (1)
that fits CORAL as is looks today

Baseline profile directly rooted in an ENISA framework

- European Cybersecurity Skills Framework: *"[...] an open European tool to build a common understanding of the cybersecurity professional role profiles and common mappings with the appropriate skills and competences required."* – website

- European Cybersecurity Skills Framework Role Profiles: Lists 12 typical cybersecurity profiles that are prevalent in the IT world today

- ...one of which is:

Cybersecurity Auditor

Chief Information Security Officer (CISO)

Cyber Incident Responder

Cyber Legal, Policy and Compliance Officer

Cyber Threat Intelligence Specialist

Cybersecurity Architect

Cybersecurity Auditor

Cybersecurity Educator

Cybersecurity Implementer

Cybersecurity Researcher

Cybersecurity Risk Manager

Digital Forensics Investigator

Penetration Tester

Image from the European Cybersecurity skills framework role profiles document, page 4

16

A proposed auditor profile (2)
that fits CORAL as is looks today

Baseline profile directly rooted in an ENISA framework

- Annotated the baseline profile
- Some key additions:
  - Knowledge of the CSA certification framework and relevant schemes
  - Knowledge of relevant standards, frameworks
  - The technical area of the product, service or process (Intended or typical use, Intended or typical application domain, Development lifecycle, Design and architecture)
  - The product, service, or process' specificities related to information security (notions of security functions, 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)

The profile, and its differences with the baseline, are described in a [deliverable on the website](#): "5. CORAL Methodology and Conformity Assessment Guidance v1.0"

Feedback and lessons learnt
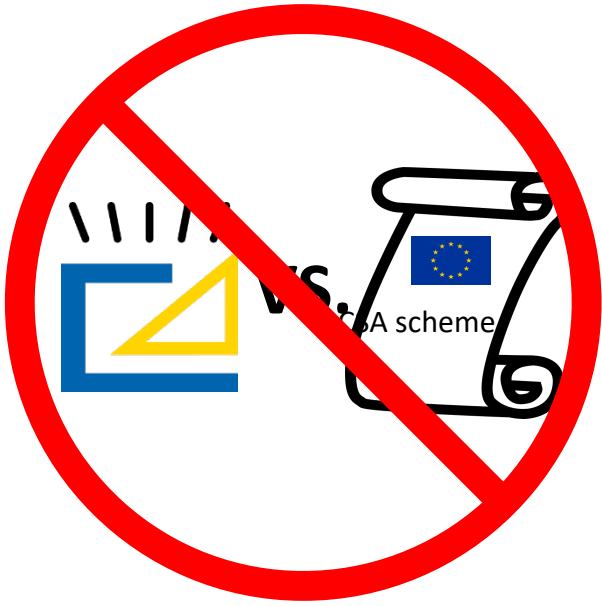
CORAL is **NOT** a "competitor" to the EUCS, EUCC, or any other CSA scheme

vs. CSA scheme

CORAL is **NOT** a national certification scheme in operation in, or proposed for, Luxembourg

CORAL-certified!

CORAL is **NOT** a guarantee of successful certification or good declaration of conformity

We used CORAL.

You don't even need an audit, then

Feedback and lessons learnt
The feasibility study

Feasibility study in numbers

- March 17th, 2023 to April 30th, 2023
- Contacted 41 people/entities
- Received 6 answers → Not enough, but overall positive feedback
- Would welcome – need - more testing/user feedback

Notable feedback received

- Editorial (wording to improve; double negations to avoid)
- Minor technical (add links to definitions; some questions are too "nothing or all", with nothing in between)
- Major technical
  - The questionnaires are too complex, and would be best suited to be used by an external consultant → Would like to avoid this precisely to keep costs down. However, CSA certification remains non-trivial, so some complexity cannot be avoided. CORAL recommends the questionnaire be filled out by the target's IT team
  - "Can we be CORAL-certified?" → Need to keep pushing the message that this is a tool for CSA certification, not something standalone.

Final remarks / Key take-aways

Observation on CSA positioning

- It is essential that the CORAL questionnaires align to existing and future official CSA schemes
- Any official visual design and template could be supported, when available

The Fit4CSA tool as of now

- The questionnaires and tool are flexible enough to be aligned to future schemes

- Is based on solid, well-established standards/best practices, and any market actor can use it as a simple, basic-level, security check to improve or measure their product/service/process' security posture

The overall CORAL approach

- Auditors, CABs and NCCAs can get inspiration from the process proposed

Project website:
https://coral-project.org/

Test Fit4CSA:
https://fit4csa.nc3.lu/survey/

Contacts:
General: coral@lhc.lu
Dr. Gabriela Gheorghe (LHC): gabriela.gheorghe@lhc.lu
Ms. Natalia Vinogradova (ANEC GIE): natalia.cassagnes@ilnas.etat.lu
Dr. Jean Lancrenon (ILNAS): jean.lancrenon@ilnas.etat.lu

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

Annex

In more detail

The questionnaire scoring scale

- Some details on how scores are attributed in Fit4CSA
  - Each question gets a potential max score based on perceived impact
  - Answers are evenly distributed in terms of scoring (worst gets "0", best gets "max", and intermediates get evenly spread intermediate values)
  - How to attribute a "max" depends on the questionnaire
  - Final score is just a re-scale to get a percentage

Products	Services and processes

- Based on the C-I-A triad for generic and for web applications: each question gets potential max score based on estimated impact of the measure in terms of C, I, and A

- Based on an estimate of a measure's impact in terms of
  - the scope of the underlying measure
  - the timing of a measure's applicability
  - whether it provides security directly or indirectly

The scoring scale is explained in detail in the deliverable "5. CORAL Methodology and Conformity Assessment Guidance v1.0"

Annex

- Sample questions from "generic products"

Topics include logging, authentication, cryptography, security during development,...

As part of your product design, is there any specification of security features that is understandable and available to users?
a) There is nothing
b) There is a specification and we have invested effort into making it understandable for most users.

Are there controls implemented to log all types of access to the product?
a) There is no control to log all types of access to the product.
b) The product has a log function that logs all types of access to the product.

Have you realized a vulnerability assessment of your product in order to identify and address potential vulnerabilities introduced during development or operation?
a) No, there was not any vulnerability assessment conducted for the product.
b) A vulnerability assessment has been conducted and all identified vulnerabilities have been remediated.

Have you implemented an access control mechanism that requires users to authenticate before any other action is allowed?
a) Users can perform certain actions without being authenticated.
b Users do not need to authenticate, in order to do any action with the product.
c) Users can only perform any given action or activity if only they are authenticated and authorized.
d) N/A

Is there a cryptographic key management function implemented in your product?
a) There is no cryptographic key management function implemented.
b) Cryptographic key generation function is implemented.
c) Cryptographic key distribution function is implemented.
d) Cryptographic key access function is implemented.
e) Cryptographic key destruction function is implemented.
f) N/A

Annex

The questionnaires

- Sample questions from "generic services"

Topics include organizational security, operational security, cryptography, change management, user support,…

To what extend does your organisation manage security roles and responsibilities?
a) Such roles and responsibilities are not defined, but team leads are expected to handle by default any information security tasks.
b) Such roles and responsibilities are only defined for top management.
c) Such roles and responsibilities are clearly defined throughout the organization, and each person is made aware of their roles and management expectations. Do you encrypt all sensitive data at rest?
a) No, there is no data encryption at rest implemented.
b) All sensitive data stored in our databases are encrypted to ensure their confidentiality.

Do you encrypt all sensitive data at rest?
a) No, there is no data encryption at rest implemented.
b) All sensitive data stored in our databases are encrypted to ensure their confidentiality.

How does your organisation manage malware? Check all that apply.
a) the IT or security team manages malware on an ad-hoc basis.
b) there is anti-malware software deployed on some devices.
c) there is anti-malware software deployed on all devices.
d) the deployment of anti-malware is formally managed (e.g., it is updated regularly)
e) there is a malware management policy or procedure, but it is not kept up up to date with new practices
f) the malware management procedure or policy is regularly updated, and its application is audited.

Before and after being released to the production environment, changes to your systems and applications are:
a) not always tested, and not always approved by management.
b) systematically tested, but not always approved by management.
c) not tested in all cases, but always approved by management.
d) always tested and also approved by management, but not always reviewed post-production.
e) always tested and approved by management, also reviewed post-production.

How do you help your clients with the secure configuration, installation, deployment, operation, and maintenance of the service provided?
a) The majority of required guidelines and recommendations are available online.
b) We offer on-call or online personalised support to our clients related to these points.
c) Some specific guidelines and recommendations are sent to them.
d) All of the above.

Annex
CORAL positioning with respect to the CSA

What it will take for CORAL to TRULY fit in the CSA?

- The questionnaires need to align to existing and future CSA schemes
- Absolutely essential, as this is not supposed to "scheme competition"
- A few misconceptions to address

Products	Services	Processes

Products
- Two questionnaires
  - Generic (inspired by ISO/IEC 15408)
  - Web applications (inspired by OWASP)

- Not trying to actually implement the full 15408 methodology (this is EUCC's job, and not even for 'basic')
- Just a very complete, useful set of categories of requirements to take inspiration from
- Not in competition with EUCC

Services
- Generic
- Inspired by EUCS Annex A
- Aims to be a generalization of it

- No choice but to align to EUCS "as much as possible", as a cloud service is an ICT service
- Can be turned into an EUCS-certification enabling tool
- Not in competition with EUCS

Processes
- Generic
- Inspired by ISO/IEC 21827

- No issue (yet)

Changing world & adapting to changes

eIDAS directive
2014
eIDAS

GDPR + NIS directive
2016 GDPR

Digital services Act + EU Cybersecurity Strategy
2020

Data Governance Act + Cyber Resilience Act
2022
DGA

2013
EU Cybersecurity strategy

2015
Digital Single Market

CYBERSECURITY ACT 2019
Cybersecurity Act

2021
Health Tech Assessment Regulation + AI Act

NIS2 DIRECTIVE 2023
NIS2 Directive