CORAL

cybersecurity Certification based On Risk evALuation and treatment

Dr. Jean Lancrenon

Project officer - Cybersecurity – ILNAS

14th ECCG meeting, virtual, 09.06.2023

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

What CORAL is

A European project

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
- 3 partners, all in Luxembourg
- CORAL website: https://coral-project.org/
- 5 existing deliverables (not a big project, so not too many to sift through), all available on the website

What CORAL is

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)

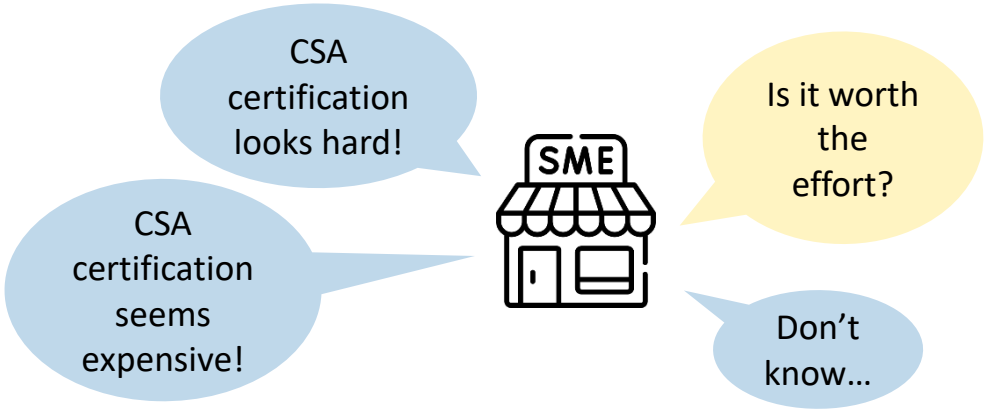
- *Groupement d'Intérêt Economique*
- Supports ILNAS in its legal missions as national standards body

What CORAL is

Project objectives

What it is, or aims to be

- Wish to address a gap: There appears to be no tool available yet to aid in bringing the CSA to the market, esp. market actors with less resources
- Wish to bridge this, starting with the most fundamental level: ‘basic’ assurance

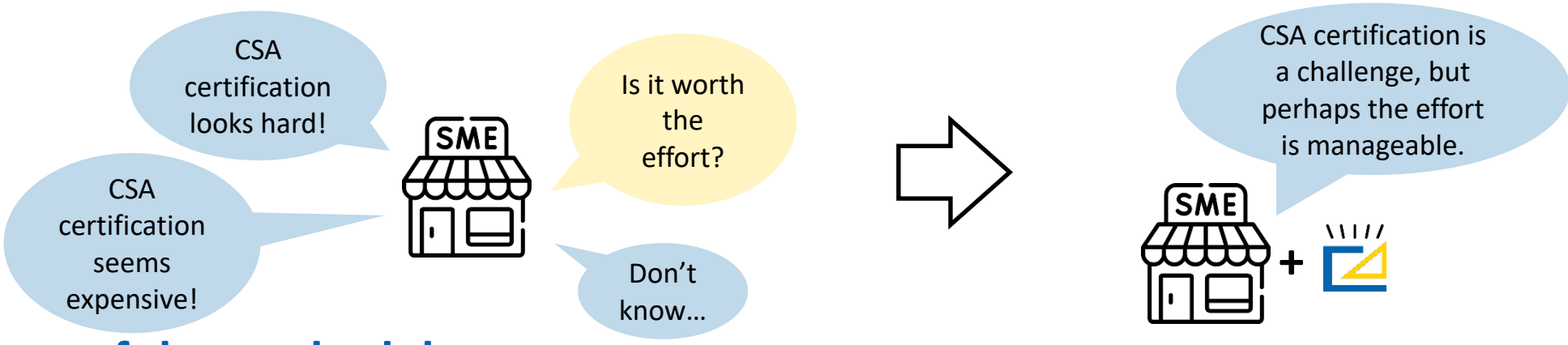


What CORAL is

Project objectives

What it is, or aims to be

- A methodology to streamline the procedures of CSA certification or issuance of EU declarations of conformity at assurance level ‘basic’
- Targeted at SMEs, in an effort to lower costs and simplify the process

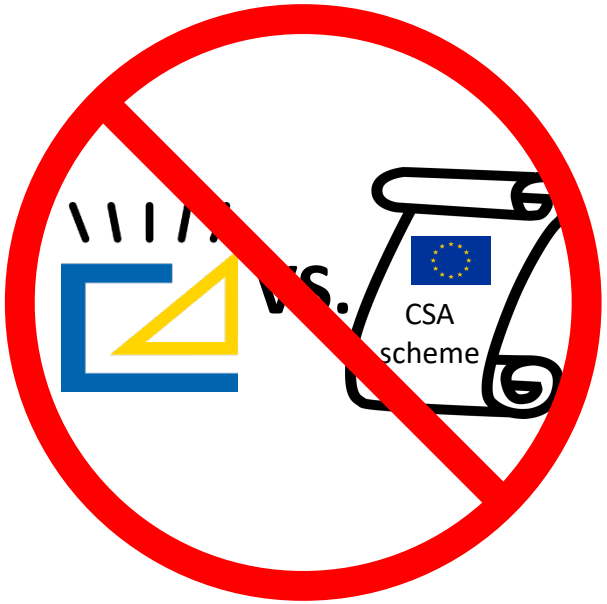


Steps of the methodology

- A set of standards-based questionnaires
- Maturity score and list of recommendations
- External audit conditioned by a minimum score and based on existing filled-in questionnaire
- Proposal of an auditor profile

…and what it is NOT

(perhaps more important)



CORAL is NOT a “competitor” to the EUCS, EUCC, or any other CSA scheme

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

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

What it is
in more detail

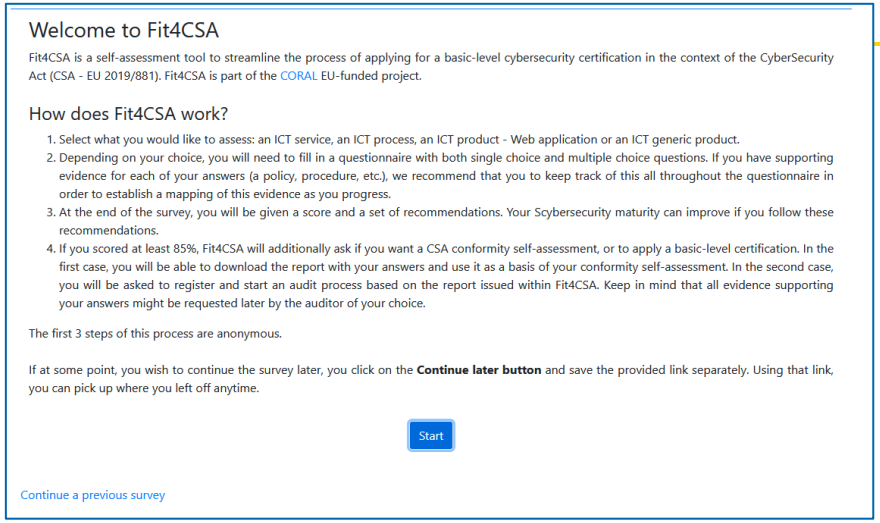
Overview

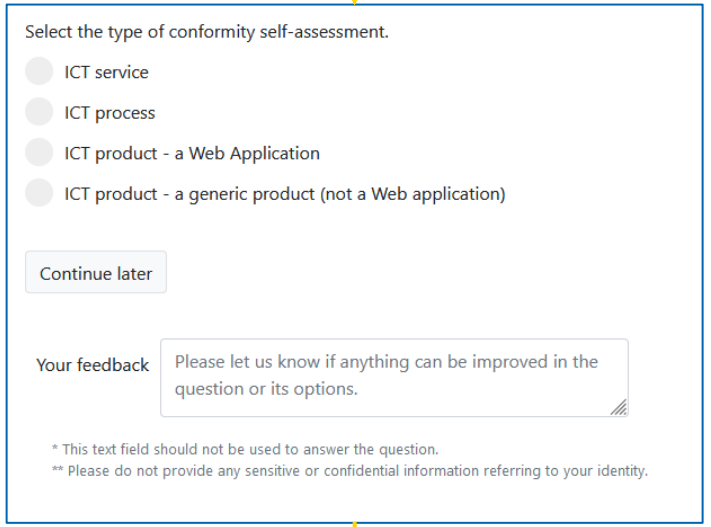
1. Provider has a product, process or service that it either wants a ‘basic’ certification for, or to issue an EU DoC
2. Provider goes through the online Fit4CSA tool, fills out a security questionnaire relevant to the “target”. The tool is open source software
3. At the end, the provider is issued a 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

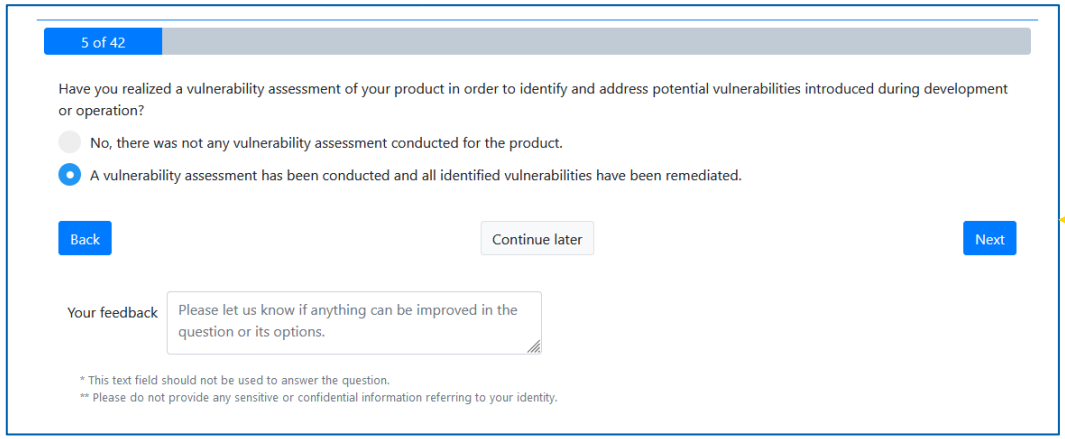
The process in detail is described in a deliverable on the website: “5. CORAL Methodology and Conformity Assessment Guidance v1.0”

What it is

in more detail (Fit4CSA tool: https://fit4csa.nc3.lu/)







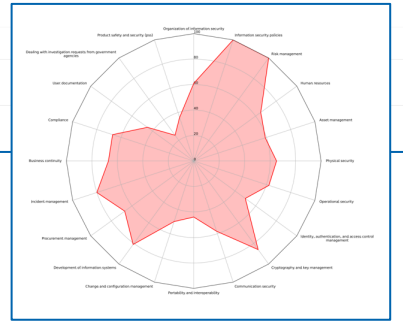
The survey can be filled in anonymously until the score is computed and the report issued, the possibility to register presents when the score is high enough

What it is

in more detail (Fit4CSA tool: https://fit4csa.nc3.lu/)

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**

Log in

99 /100
Report:
Download
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

What it is

in more detail (Fit4CSA tool: https://fit4csa.nc3.lu/)

Auditor module

Two roles can sign up and log in: auditees and auditors

- Auditors can start an audit based on an existing auditee request (offline) & survey that's of at least 85%;
- Auditees can link any survey of more than 85%, to an auditor (based on offline agreements), and can follow up with existing audits;

The auditee can have a view on the status of the audit (completion, pending points)

An audit facilitating tool

What it is

in more detail (Fit4CSA tool)

What it is
in more detail

Not a full certification service in itself, of course

- Provider contacts CAB, conformity assessment process starts
- Provider gathers documentary evidence according to scheme technical requirements
- Auditor reviews documentary evidence
- Audit result is communicated

High level view of what a conformity assessment process looks like

- **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, **auditor module can support**
- Audit result is communicated

How CORAL can fit into this process, **IN THEORY**

What it is
in more detail

The questionnaires

- What they are

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®*

The questionnaires in detail (and the recommendations) are part of the deliverables on the website: “3. Evaluation Questionnaire for ICT Services, ICT Processes, and ICT Products”.

What it is
in more detail

The questionnaires

- How did the project “build” them?

SotA	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 SotA is a deliverable on the website: “1. State of the Art”

*State of the Art Syllabus Overview of existing Cybersecurity standards and certification schemes v2, ECSO, December 2017

What it is
in more detail

The questionnaires

- Sample questions from “generic products”

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

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 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

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.

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.

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

What it is
in more detail

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.

What it is

Its 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

• Two questionnaires
  • Generic (inspired by ISO/IEC 15408)
  • Web applications (inspired by OWASP)
	• Generic
	• Inspired by EUCS Annex A
	• Aims to be a generalization of it
		• Generic
		• Inspired by ISO/IEC 21827

• 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	• 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	• No issue (yet)

What it is

Its 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”

- The project’s view today:

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

    - If that fails, the tool remains 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

CORAL in practice

Feedback from 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 security team, or if not possible, the IT team
  - “Can we be CORAL-certified?” → Need to keep pushing the message that this is a tool for CSA certification, not something standalone. A key message for future dissemination

A proposed auditor profile

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:

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

A proposed auditor profile

that fits CORAL as is looks today

Baseline profile directly rooted in an ENISA framework

- Simply edited 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"

A proposed auditor profile

that fits CORAL as is looks today

Takeaways and outlook

- Aim is to have a tool that aids in making the CSA practicable for the market, esp. at level ‘basic’
- Could be a stepping stone towards similar tools for other assurance levels
- If the ECCG or its members have opinions or thoughts on this aim, or how else they see the project might serve the CSA, we welcome the feedback

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

Luxembourg House of Cybersecurity

ILNAS

ANEC
AGENCE POUR LA NORMALISATION ET L'ÉCONOMIE DE LA CONNAISSANCE

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”