

ICT Security Guide

CCN-STIC 2010

Cloud Product Evaluation Methodology (CICLON)



March 2026

Edited by:



© Spanish National Cryptologic Center, 2026
Edition date: march 2026



CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.04.24 11:49:41 +02'00'

LIMITATION OF LIABILITY

The present document is provided in accordance with the terms set forth herein, expressly rejecting any type of implied warranty related thereto. Under no circumstances shall the National Cryptologic Center be liable for any direct, indirect, incidental, or extraordinary damages arising from the use of the information and software provided herein, even if advised of such possibility.

LEGAL NOTICE

Without the written authorization of the National Cryptologic Center, the partial or total reproduction of this document by any means or procedure, including photocopying and computer processing, and the distribution of copies through public rental or loan, are strictly prohibited under the penalties established by the law.

Version Control

Version	Comment	Date
1.0	Initial Version	March 2026

INDEX

1. PURPOSE OF THE DOCUMENT	6
2. OBJECTIVE OF THE METHODOLOGY	7
3. ACTORS AND RESPONSABILITIES.	8
3.1 LIST OF ACTORS	8
3.2 RESPONSABILITIES.....	8
3.2.1 APPLICANT OR MANUFACTURER	8
3.2.2 EVALUATION LABORATORY	9
3.2.3 CCN	9
4. PREPARATION OF THE EVALUATION	10
4.1 MINIMUM REQUIRED EVIDENCE	10
4.1.1 SECURITY TARGET (ST).....	10
4.1.2 VALIDATION OF THE SECURITY TARGET	10
4.1.3 SERVICE ARCHITECTURE DOCUMENT (DAS)	10
4.1.4 LIBRARY FILE	11
4.2 PREPARATION PHASES	11
4.2.1 SELECTION OF AN EVALUATION LABORATORY	11
4.2.2 EVALUATION REQUEST.....	12
4.2.3 ANALYSIS OF THE EVALUATION REQUEST.....	12
5. EVALUATION PROCESS	13
5.1 GENERAL INFORMATION ABOUT THE EVALUATION PROCEDURE	13
5.2 EVALUATION PHASE	13
5.2.1 STAGE 1 – ANALYSIS OF THE SECURITY TARGET	14
5.2.2 STAGE 2 – ANALYSIS OF THE SERVICE ARCHITECTURE DOCUMENT	14
5.2.3 STAGE 3 – ACCESS AND CONFIGURATION OF THE TESTING ENVIRONMENT ...	15
5.2.4 STAGE 4 – FUNCTIONAL TESTS	15
5.2.5 STAGE 5 – CRYPTOGRAPHIC ANALYSIS OF COMMUNICATIONS	16
5.2.6 STAGE 6 – TOE PENETRATION TESTING	16
5.2.7 STAGE 7 – CALCULATION OF THE EVALUATION ASSURANCE SCORE	17
5.2.8 STAGE 8 – GENERATION OF THE TECHNICAL EVALUATION REPORT	17
5.3 MONITORING PHASE.....	17
5.3.1 STAGE 1 – THIRD-PARTY LIBRARY ANALYSIS	17

5.3.2	STAGE 2 – VERIFICATION OF INTEGRATED COMPONENTS.....	18
5.3.3	STAGE 3 - REVIEW OF CERTIFICATIONS APPLICABLE TO THE CLOUD PLATFORM PROVIDER.....	19
5.3.4	STAGE 4 – CALCULATION OF THE MONITORING ASSURANCE SCORE	19
5.3.5	STAGE 5 – CALCULATION OF THE COMPOSITE ASSURANCE SCORE	19
5.3.6	STAGE 6 - GENERATION OF THE TECHNICAL MONITORING REPORT.....	20
5.4	EVALUATION RESULT	20
6.	EFFORT CALCULATION.....	21
7.	GLOSSARY.....	22
8.	ACRONYMS.....	24
9.	REFERENCES.....	25

1. PURPOSE OF THE DOCUMENT

The National Cryptologic Centre (CCN) has developed the Cloud Product Evaluation Methodology (CICLON) in response to the need to evaluate products deployed in cloud environments for all threat levels established by the Cybersecurity Act (Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA).

This document defines the Cloud Product Evaluation Methodology (CICLON) for an Information and Communication Technology (ICT) security product, including the definition of the actors involved, the different input elements of the evaluation process, the phases that comprise it, and the specific characteristics that distinguish it.

The security evaluation of a cloud product is the only objective means of assessing its capability to handle information with the level of security stated by the manufacturer in its Security Target (ST).

This methodology defines the procedure required for a trusted and technically competent third party to carry out an ICT security evaluation.

The main characteristics of the evaluation are as follows:

- a) The evaluation process is composed of two clearly differentiated phases: an initial evaluation phase and a continuous monitoring phase of a periodic nature.
- b) The estimated effort required to perform the evaluation depends on the complexity of the product deployed in the cloud.
- c) The methodology allows the automation of activities associated with the evaluation process wherever applicable.
- d) The outcome of the evaluation is expressed as a Composite Assurance Score (PGC), which integrates the results obtained from both the evaluation and monitoring phases.
- e) The PGC value is subject to periodic updates as a result of successive iterations of the monitoring phase.

2. OBJECTIVE OF THE METHODOLOGY

The CICLON evaluation methodology has been developed to address the specific challenges associated with the evaluation of products deployed in cloud environments. Traditional evaluation methodologies —such as LINCE, Common Criteria (CC) or EUCC— are not suitable for these environments, as they generally require physical access to the evaluated product or the existence of a static and immutable version of the product throughout the entire evaluation period.

The evaluation is based on the verification of implemented security functions and on the execution of vulnerability analysis through functional testing and penetration testing.

The objective of the evaluation process is to enable a laboratory to verify whether the product conforms to its specification —by confirming the correct implementation of its security functions— as well as to perform a vulnerability analysis and a set of penetration tests to determine that the product is free from vulnerabilities with a given level of assurance. The results of this process are documented in the Evaluation Technical Report (ETR) and the Monitoring Technical Report (MTR).

For this purpose, the evaluation laboratory shall use as its documentary baseline the Security Target (ST), which defines the scope of the evaluation; the Service Architecture Document (DAS); the list of third-party libraries together with their corresponding versions; publicly available information related to the product; and access to the Target of Evaluation (TOE) itself.

In addition, the laboratory will use all publicly available information related to the TOE, including, but not limited to, documentation published by the manufacturer for the product under evaluation or equivalent products, publicly available information provided by third parties, and public vulnerability databases applicable to products deployed in the cloud.

3. ACTORS AND RESPONSABILITIES.

3.1 LIST OF ACTORS

The following actors participate in the evaluation process:

- a) **Applicant:** the entity responsible for formally submitting the evaluation request for the cloud-deployed product.
- b) **Manufacturer:** the entity responsible for the design, development and, where applicable, maintenance of the cloud-deployed product.
- c) **Evaluation Laboratory:** an entity accredited within the framework of the ENECSTI in accordance with ISO/IEC 17025 and authorized by the Certification Body to perform the product evaluation.
- d) **National Cryptologic Center (CCN):** the entity responsible for validating the evaluation report issued by the evaluation laboratory and the assurance percentage derived from the obtained results.

3.2 RESPONSABILITIES

3.2.1 APPLICANT OR MANUFACTURER

The applicant shall provide, at least, the following elements and evidence required to carry out the evaluation process:

- a) A formal evaluation request submitted to CCN, using the cloud-deployed product evaluation request form [FOR-CIC-001].
- b) The cloud-deployed product that is the subject of the evaluation.
- c) The documentation associated with the product.
- d) The Security Target (ST), of a public nature.
- e) The Service Architecture Document (DAS), of a private nature.
- f) A valid certification under the National Security Scheme (ENS) or another certification recognized within the ENECSTI framework.
- g) The list of third-party libraries used by the product, including their versions.
- h) The environment required for the security evaluation of the product. The applicant shall provide the evaluation laboratory with access to the TOE testing environment. This environment shall correspond to the described in the Security Target or be functionally and configurationally equivalent, allowing the validation of the implemented security functions and the execution of the planned evaluation activities.
- i) The managing of the execution of the evaluation with a CCN authorized laboratory and providing the necessary support during the entire process.
- j) The required evidences to perform the evaluation process.

Note: In certain cases, the manufacturer and the applicant for certification may be different entities. For simplicity, they are treated as a single role. In such cases, the applicant is generally responsible for financing the evaluation, while the manufacturer provides the technical support required to perform the evaluation process.

3.2.2 EVALUATION LABORATORY

Due to the high level of specialization required for the execution and validation of evaluation activities, as well as the complexity of the equipment required for certain tests, it is necessary to assure that evaluation laboratories possess the minimum technical capabilities and material resources needed to apply this methodology.

The document [PO-CIC-010] establishes the requirements and procedures that laboratories must meet to be authorized by the CCN to perform cloud product evaluations under the CICLON methodology.

The responsibilities of the evaluation laboratory are the following:

- a) Maintaining technical competence to perform evaluations in accordance with the CICLON methodology.
- b) Applying the procedures, guides and documentation required to perform the evaluation, including at least:
 - a. Cloud product certification procedure [PO-CIC-005].
 - b. Laboratory accreditation procedure [PO-006].
 - c. Laboratory authorization procedure for CICLON evaluations [PO-CIC-010].
- c) Verifying that the access to the TOE testing environment provided by the applicant is adequate and allows the complete execution of the required evaluation activities.

3.2.3 CCN

The responsibilities of the certification body include the following:

- a) Elaborate the evaluation criteria and methodology applicable to cloud-deployed products. CCN may require the application of specific evaluation methods depending on the characteristics of the product under evaluation.
- b) Develop the procedures, forms, guides and documentation necessary for the correct implementation of the evaluation process, including:
 - a. Cloud product certification procedure [PO-CIC-005].
 - b. Laboratory accreditation procedure [PO-006].
 - c. Laboratory authorization procedure for CICLON evaluations [PO-CIC-010].
- c) Check and verify that the laboratories meet the criteria established in the laboratory accreditation procedure [PO-006].
- d) Review laboratory authorization requests and granting or revoking the status of CCN authorized laboratory.
- e) Review evaluation requests and authorize or deny the initiation of the evaluation process.

4. PREPARATION OF THE EVALUATION

4.1 MINIMUM REQUIRED EVIDENCE

4.1.1 SECURITY TARGET (ST)

The Security Target (ST) is used to specify the security problem of the cloud-deployed product that will be subject to evaluation, as well as to describe the relations between the product and its operational environment.

This security problem defines:

- a) The assets to be protected.
- b) The threats to which those assets may be exposed.
- c) The assumptions regarding the operational environment that apply to the TOE.
- d) The security functional requirements that mitigate the identified threats and that are subject to evaluation.

In addition, the ST shall unambiguously identify both the TOE and the environment in which the evaluation will be carried out, specifying whether the evaluation corresponds to a production environment or a pre-production environment.

For each security function subject to evaluation, the ST shall indicate the verification method by which it will be assessed, according to the following criteria:

- a) **Indirect Verification (IV):** applicable when the laboratory cannot directly test the security function.
- b) **Direct Verification (DV):** applicable when the laboratory can perform the security function tests on the TOE, including functional and penetration testing.
- c) **Integration (Int.):** applicable when the security function is covered by a component defined in the operational environment as an integrated element and has been configured by the manufacturer.

The Security Target shall conform to the Security Target Template defined in [Annex A CCN-STIC-2010].

4.1.2 VALIDATION OF THE SECURITY TARGET

The validation of the security target shall be performed initially by the team responsible for the CCN Catalogue of ICT Products and Services (CPSTIC).

The document resulting from this validation shall serve as formal evidence of the initiation of the evaluation process, together with the Security Target (ST) itself.

4.1.3 SERVICE ARCHITECTURE DOCUMENT (DAS)

This document constitutes a signed declaration of responsibility and shall include the following information:

- a) The structure of the TOE and its operational environment: in terms of subsystems and interfaces.

- b) A description of the information flows: declared between service components.
- c) The data jurisdiction of the cloud-deployed product.
- d) Transparency clauses.
- e) Authorization for direct access to the cloud-deployed product if WAF.
- f) Certification of conformity with ENS or EUCS.
- g) Information regarding cryptographic mechanisms and algorithms used, as well as encryption services.

The DAS shall conform to the Template of the Cloud Form defined in [Annex B CCN STIC 2010].

4.1.4 LIBRARY FILE

The Library File shall be provided in the form of a Software Bill of Materials (SBOM), compliant with the CycloneDX standard, in order to provide full traceability of all third-party dependencies used by the TOE.

The SBOM documents and organizes the software composition of the product, allowing the verification of versions, provenance and risks associated with each component.

The SBOM shall include the following elements:

- a) **General identification:** version, generation date, tool used and unique identifier (UUID).
- b) **TOE information:** identification data of the evaluated product.
- c) **Third-party libraries inventory:** exhaustive list of libraries, including name, version, type, supplier, licenses, hash values, standardized identifiers (purl, CPE), transitive dependencies and usage context.
- d) **Relationships between components:** dependency relationships such as “depends-on” and “includes” between the different software elements.
- e) **Integrity metadata:** digital signature, hash values and origin of each component, for verification and non-repudiation purposes.

Where applicable, container layers, runtimes and base systems on which the TOE operates shall also be documented.

4.2 PREPARATION PHASES

4.2.1 SELECTION OF AN EVALUATION LABORATORY

Before submitting the evaluation request, the applicant shall contact an evaluation laboratory accredited within ENECSTI and authorized by CCN.

The applicant and the laboratory shall agree on:

- a) The scope of the evaluation, based on the Security Target (ST), the Service Architecture Document (DAS) and the third-party library file provided.
- b) The estimated effort required for the evaluation, taking into account the following factors:

- a. Technological complexity of the TOE.
- b. Diversity of evaluated configurations.
- c. Number of interfaces and protocols used.
- d. Presence of proprietary modules or recent vulnerabilities.

The evaluation shall always comply with the minimum testing requirements defined by CCN for the methodology, and therefore with the minimum execution time associated.

4.2.2 EVALUATION REQUEST

Before formally submitting an evaluation request, the applicant shall:

- a) Elaborate the Security Target (ST) in accordance with the Template for the Security Target of Cloud Products Evaluation (CICLON) defined in [Annex A CCN-STIC-2010].
- b) Elaborate the Service Architecture Document (DAS) in accordance with the Template for the Service Architecture Document of Cloud Products Evaluation (CICLON), defined in [Annex B CCN-STIC-2010].
- c) Contract an authorized evaluation laboratory to perform the evaluation tests.
- d) Prepare the environment required to perform the evaluation tests.
- e) Prepare the third-party library file in SBOM format, in accordance with the present methodology.

To formalize the evaluation request, the applicant shall submit the above documentation together with:

- a) A completed evaluation request [FOR-CIC-001].
- b) A valid certification of the National Security Scheme (ENS) or, where applicable, another certification recognized within ENECSTI.
- c) A favorable result from the Security Target review report issued by the CPSTIC team.

4.2.3 ANALYSIS OF THE EVALUATION REQUEST

CCN shall analyze the evaluation request, the Security Target, the Service Architecture Document and the third-party library file.

An evaluation request may be rejected by CCN and may be subject to correction in the following cases:

- a) Incomplete request.
- b) Incomplete documentation or documentation not compliant with the defined requirements.

Once the evaluation request has been accepted by CCN, the evaluation project shall be registered and all participants shall be informed of its acceptance.

5. EVALUATION PROCESS

5.1 GENERAL INFORMATION ABOUT THE EVALUATION PROCEDURE

The evaluation must be carried out by a laboratory accredited by the ENECSTI and authorized by CCN, in order to guarantee the homogeneity and comparability of the results between the different authorized laboratories.

CCN may decide to close the evaluation file in the circumstances described in [PO-CIC-005] regardless of the contractual obligations that may exist between the applicant and the laboratory.

The evaluation process includes the following phases:

- a) Evaluation phase:
 - a. Analysis of the Security Target (ST).
 - b. Analysis of the Service Architecture Document (DAS).
 - c. Access and configuration of the test environment.
 - d. Execution of functional tests.
 - e. Cryptographic analysis.
 - f. Execution of penetration tests on the TOE, in accordance with [CCN-ITC-003].
- b) Monitoring phase:
 - a. Analysis of the third-party library file (SBOM).
 - b. Verification of components integrated into the operational environment.
 - c. Review of certifications applicable to the execution environment.

The results will be presented in two technical reports:

- a) Evaluation Technical Report (ETR).
- b) Monitoring Technical Report (MTR).

The evaluation process is carried out iteratively:

- a) In the first iteration, the Evaluation Phase will be carried out together with the Monitoring Phase, obtaining an initial Composite Assurance Score (PGC).
- b) In subsequent iterations, only the Monitoring Phase will be carried out, which will update the value of said PGC.

The evaluation laboratory may convene work sessions with the manufacturer and/or the applicant in order to deepen the knowledge of the TOE and optimize the development of the evaluation process.

Likewise, the manufacturer must facilitate access to the TOE prior to the start of the evaluation and provide the necessary technical support during the evaluation.

5.2 EVALUATION PHASE

The laboratory must begin with this phase in the first iteration of the process.

The result of this phase will be an Evaluation Assurance Score (PGE) of the product deployed in the cloud and will be reflected in the Evaluation Technical Report (ETR),

defined in the Cloud Product Evaluation Technical Report Template (CICLON) [Annex C CCN-STIC 2010].

Next, the stages and **tasks to be carried out by the evaluator** are defined.

5.2.1 STAGE 1 – ANALYSIS OF THE SECURITY TARGET

Task 1. Check that the Security Target contains the elements described in [Annex A CCN-STIC-2010].

Task 2. Check that the name of the TOE is provided.

Task 3. Check that the Security Target (ST) has been validated by team responsible for the CPSTIC.

Task 4. Check that the description of the TOE is not confusing and that it describes at least the minimum functionality for which it is designed.

Task 5. Check that there is a correct delimitation of the parts that belong to the TOE and the parts that belong to the operational environment, as well as an adequate description of how the operational environment supports the execution of the TOE.

Task 6. Check the coherence of the security problem (Assets, Assumptions, Threats and Security Functions).

Task 7. Check that the security functions are described in sufficient detail to allow the evaluator to understand how they have been implemented in the TOE.

Task 8. Check that the security functions delegated to the operational environment are described in sufficient detail to allow the evaluator to understand how they are provided by the operational environment.

Task 9. Check that there are no non-conformities in relation to the analysis of the ST.

Task 10. Calculate the Assurance Score corresponding to this stage using the following formula.

$$PGE_1 = 1 - k_{CI} \frac{IV}{R}$$

Where:

$k_{CI} \rightarrow$ Scaling factor that allows adjusting the slope of the curve associated with the requirements satisfied through Indirect Verification (IV).

$IV \rightarrow$ Number of requirements satisfied by the manufacturer through Indirect Verification (IV).

$R \rightarrow$ Total amount of security requirements defined in the ST.

5.2.2 STAGE 2 – ANALYSIS OF THE SERVICE ARCHITECTURE DOCUMENT

Task 1. Check that the Service Architecture Document (DAS) is complete and corresponds to the evaluated TOE.

Task 2. Check that the Service Architecture Document defines the possibility of access to the TOE avoiding the WAF.

Task 3. Check that there is a correct delimitation of the parts that belong to the TOE and the parts that belong to the operational environment, as well as an adequate description of how the operational environment supports the execution of the TOE.

Task 4. Check that there are no non-conformities in relation to the Service Architecture Document.

5.2.3 STAGE 3 – ACCESS AND CONFIGURATION OF THE TESTING ENVIRONMENT

Task 1. Verify that the applicant has provided access to the testing environment required to perform testing on the product.

Task 2. Verify that it is possible to configure the product according to the configuration or configurations described in the Security Target. If the product allows several configuration modes, the identification of this mode must be indicated in the Security Target.

Task 3. Check that there are no non-conformities in the access and configuration of the test environment.

Task 4. Calculate the Assurance Score corresponding to this stage using the following formula.

$$PGE_3 = \begin{cases} 1 - W, & \text{Production environment} \\ P - W, & \text{Equivalent preproduction environment} \end{cases}$$

Where:

P → Value associated with the use of an equivalent pre-production environment.

W → Represents access to the TOE through the WAF in the evaluation environment.

A production environment is defined as one in which the environment used for evaluation is the same as the one that will later be provided to the end user of the TOE.

On the other hand, it is considered a pre-production environment when the evaluation environment has similar characteristics to the one that will be provided to the end user of the TOE, but without being the same.

5.2.4 STAGE 4 – FUNCTIONAL TESTS

Task 1. The evaluator must execute, for all the security functions defined in the Security Target (ST) and marked as Direct Verification (DV), the following tests:

- a) **Standard test.** The evaluator must verify that the security function described in the corresponding requirement is correctly implemented in the TOE.
- b) **Tampering/bypassing test.** The evaluator, taking as a reference the security mechanism implemented by the TOE, must try to:
 - a. Subvert the behavior of the security mechanism through alterations or modifications to the corresponding interface (**tampering**).

- b. Prevent the application of the security mechanism by exploiting weaknesses in the logic of its implementation (*bypassing*).

Task 2. The evaluator must perform the following tests for all security functions defined in the Security Target (ST) and marked as Indirect Verification (IV):

- a) Verify that the evidence provided has been signed by the manufacturer and covers the declared security requirement. For this purpose, only the following will be considered valid evidence, provided they are applicable to the requirement being verified:
 - a. Product manuals.
 - b. Source code.
 - c. Image or video captures of the specific function of the TOE.
 - d. Online or in-person sessions where the manufacturer demonstrates the implementation of the security function to the evaluator.
- b) Verify that the evidence provided is complete, consistent, and technically adequate to justify compliance with the security function.

5.2.5 STAGE 5 – CRYPTOGRAPHIC ANALYSIS OF COMMUNICATIONS

Task 1. The evaluator must verify that all external and internal communication channels related to the TOE are clearly defined and identified in the Security Target.

Task 2. The evaluator must verify that the information in the Security Target is consistent with the information in the Service Architecture Document.

Task 3. The evaluator must verify that there are no non-conformities related to the cryptographic characteristics of the communication channels.

Task 4. The evaluator must calculate the Assurance Score for this stage (PGE_5) using the following formula.

$$PGE_5 = e^{-(w_L \cdot L + w_{NR} \cdot NR)}$$

Where:

- $w_L \rightarrow$ Impact of Legacy cryptography on the assurance score.
- $w_{NR} \rightarrow$ Impact of Not Recommended cryptography on the assurance score.
- $L \rightarrow$ Number of cryptographic mechanisms used by the TOE that are considered Legacy as of the date of the evaluation.
- $NR \rightarrow$ Number of cryptographic mechanisms used by the TOE that are considered Not Recommended as of the date of the evaluation.

5.2.6 STAGE 6 – TOE PENETRATION TESTING

Task 1. The evaluator must perform, at a minimum, the set of tests described in the Technical Instruction for Security Evaluation in Web and Cloud Environments [CCN-ITC-003], in accordance with the Template for Cloud Product Evaluation Technical Report (CICLON), included in [Annex C CCN-STIC 2010].

Task 2. The evaluator must ensure that there are no non-conformities due to successful attacks.

5.2.7 STAGE 7 – CALCULATION OF THE EVALUATION ASSURANCE SCORE

Task 1. The evaluator must calculate the Evaluation Assurance Score (PGE) of the product cloud-deployed based on the results of the previous stages using the following formula:

$$PGE = e^{-(w_1(1-PGE_1)+w_3(1-PGE_3)+w_5(1-PGE_5))}$$

Where:

w_1 → Weight of PGE_1 in the PGE calculation.

w_3 → Weight of PGE_3 in the PGE calculation.

w_5 → Weight of PGE_5 in the PGE calculation.

PGE_1 → Assurance Score for Stage 1 of the Evaluation Phase.

PGE_3 → Assurance Score for Stage 3 of the Evaluation Phase.

PGE_5 → Assurance Score for Stage 5 of the Evaluation Phase.

Task 2. The evaluator must record the different Partial Assurance Scores (PGE_1 , PGE_3 , PGE_5) and the Evaluation Assurance Score (PGE) in the Technical Evaluation Report, in accordance with the provisions of [Annex C CCN-STIC 2010].

5.2.8 STAGE 8 – GENERATION OF THE TECHNICAL EVALUATION REPORT

Task 1. The evaluator must issue a Evaluation Technical Report (ETR) that contains and presents the results of the evaluation phase. This report must contain the information required in the template [Annex C CCN-STIC-2010].

5.3 MONITORING PHASE

The product deployed in the cloud must undergo the Monitoring Phase after passing through the Evaluation Phase.

During the evaluation period, this phase will be repeated iteratively.

The result of this phase will be an Assurance Score for the cloud-deployed product and will be recorded in the Cloud Product Monitoring Technical Report Template (CICLON) [Annex D CCN-STIC 2010].

Next, the stages and **tasks to be performed by the evaluator** are defined below.

5.3.1 STAGE 1 – THIRD-PARTY LIBRARY ANALYSIS

Task 1. The evaluator must process the Library File (SBOM) provided by the vendor to search for known public vulnerabilities.

Task 2. The evaluator must categorize the severity (critical, high, medium, low) of each public vulnerability found. Severity is defined by the following CVSS v4.0 ranges:

- a) **Critical:** From 9.0 to 10.0
- b) **High:** From 7.0 to 8.9
- c) **Medium:** From 4.0 to 6.9
- d) **Low:** From 0.1 to 3.9

Task 3. The evaluator must calculate the Percentage of Score (PGM_1) for this stage using the following formula:

$$PGM_1 = C \cdot e^{-\left(w_H \cdot H + \frac{w_M \cdot M}{T} + \frac{w_L \cdot L}{T}\right)}$$

Where:

- $w_H \rightarrow$ Impact of high-severity vulnerabilities on the assurance score.
- $w_M \rightarrow$ Impact of medium-severity vulnerabilities on the assurance score.
- $w_L \rightarrow$ Impact of low-severity vulnerabilities on the assurance score.
- $C \rightarrow$ Value 0 if any critical vulnerability exists and 1 otherwise.
- $H \rightarrow$ Number of high-severity vulnerabilities.
- $M \rightarrow$ Number of medium-severity vulnerabilities.
- $L \rightarrow$ Number of low-severity vulnerabilities.
- $T \rightarrow$ Total number of third-party libraries declared by the applicant in the Security Target (ST).

5.3.2 STAGE 2 – VERIFICATION OF INTEGRATED COMPONENTS

Task 1. The evaluator must verify that the integrated components declared in the Security Target are evaluated using the CICLON Methodology.

Task 2. The evaluator must calculate the Assurance Score corresponding to this stage (PGM_2) using the following formula:

$$PGM_2 = \sum_0^n (PGC_{COMPn} \cdot \frac{RFS_{COMPn}}{R})$$

Where:

- $PGC_{COMPn} \rightarrow$ Composite Assurance Score (PGC) of component n.
- $RFS_{COMPn} \rightarrow$ Number of fundamental security requirements implemented by component n.
- $R \rightarrow$ Total number of requirements defined in the Security Target.
- $n \rightarrow$ Number of external components that contribute to implementing security functionality.

5.3.3 STAGE 3 - REVIEW OF CERTIFICATIONS APPLICABLE TO THE CLOUD PLATFORM PROVIDER

Task 1. The evaluator must verify the validity of the various applicable certificates provided by the manufacturer.

Task 2. The evaluator must calculate the Assurance Score corresponding to this stage (PGM_3) using the following formula:

$$PGM_3 = \prod_{1}^n C_n$$

Where:

C → Certification of compliance with the National Security Scheme (ENS) or equivalent. Value 1 if the certification is valid and 0 otherwise.

5.3.4 STAGE 4 – CALCULATION OF THE MONITORING ASSURANCE SCORE

Task 1. The evaluator must calculate the Monitoring Assurance Score (PGM) of the cloud-deployed product based on the results of the previous stages using the following formula:

$$PGM = PGM_3 \cdot e^{-(w_1(1-PGM_1)+w_2(1-PGM_2))}$$

Where:

w₁ → Weight of PGM_1 in the PGM calculation.

w₂ → Weight of PGM_2 in the PGM calculation.

PGM₁ → Assurance score for Stage 1 of the Monitoring Phase.

PGM₂ → Assurance score for Stage 2 of the Monitoring Phase.

PGM₃ → Assurance score for Stage 3 of the Monitoring Phase.

Task 2. The evaluator must record the different Partial Assurance Scores (PGM_1 , PGM_2 , PGM_3) and the Monitoring Assurance Score (PGM) in the Technical Monitoring Report in accordance with the provisions of [Annex D CCN-STIC 2010].

5.3.5 STAGE 5 – CALCULATION OF THE COMPOSITE ASSURANCE SCORE

Task 1. The evaluator must calculate the Composite Assurance Score (PGC) of the cloud-deployed product based on the results of the Evaluation Assurance Score (PGE) and the Monitoring Assurance Score (PGM) using the following formula:

$$PGC = (w_e \cdot PGE + (1 - w_e) \cdot PGM) \cdot 100$$

Donde:

PGE → This is the Evaluation Assurance Score (PGE).

PGM → This is the Monitoring Assurance Score (PGM).

w_e → Weight of the PGE in the PGC calculation.

5.3.6 STAGE 6 - GENERATION OF THE TECHNICAL MONITORING REPORT

Task 1. The evaluator must issue a Monitoring Technical Report (MTR) that contains and presents the results of the monitoring phase. This report must contain the information required in the template [Annex D CCN-STIC-2010].

5.4 EVALUATION RESULT

The evaluation verdict will be a Composite Assurance Score (PGC) which will take into account evaluation factors and ongoing monitoring.

If non-conformities are found during the Evaluation Process, the evaluation verdict will be **FAIL and, therefore, the Composite Assurance Score will be 0.**

6. EFFORT CALCULATION

For guidance purposes, the following factors shall be considered when estimating the effort required to perform an evaluation. Elements marked with **[R]** are expected to reduce the required effort, whereas elements marked with **[A]** are expected to augment it:

- [A]** If a large number of fundamental security requirements are defined in the Security Target (ST).
- [A]** If the technology employed by the TOE is complex.
- [A]** If the operational environment is complex.
- [A]** If there are multiple evaluated configurations.
- [A]** If the TOE utilizes multiple communication protocols.
- [A]** If the TOE has multiple interfaces.
- [A]** If the TOE makes use of proprietary modules to which a potential attacker has direct access.
- [A]** If there have been recent security publications that may present new attack vectors for the type of TOE being evaluated.
- [R]** If the laboratory has test suites available for the protocols used by the TOE.
- [R]** If the laboratory has previous experience in evaluations similar to the TOE.
- [R]** If the laboratory has automated tools that facilitate the evaluation of security functions implemented by the TOE.

For standardization purposes, the effort calculation shall be understood as being carried out by an experienced evaluator with extensive knowledge of both the methodology and the evaluated technology. Consequently, if the evaluation is performed by an evaluator who does not meet this standard, the laboratory shall adjust the effort estimation accordingly.

7. GLOSSARY

Actors	Roles involved in the evaluation: applicant, manufacturer, laboratory and CCN.
Asset	Element of the TOE or of the environment that must be protected against threats.
Threats	Elements of the security problem that describe possible actions that may compromise the TOE assets.
Communication Channel	Information flow between internal or external TOE components whose security must be analyzed.
Direct Verification	Evaluation method in which the laboratory can directly test the security requirement.
Indirect Verification	Evaluation method based on evidence provided by the manufacturer.
Integrated Component	Element external to the TOE that provides part of the declared security functionality.
Security Target (ST)	Document that defines the security problem, scope, threats, assets and requirements of the TOE.
Service Architecture Document (DAS)	Document that describes the service architecture, cloud provider and service conformity.
Pre-Production Environment	Environment similar to the production environment but not identical.
Production Environment	Real environment used by the final user.
Operational Environment	Components external to the TOE that support its operation.
Security Function	Technical mechanism implemented by the TOE to mitigate threats and protect assets.

Library File	List of third-party libraries used by the TOE, including their versions.
Assumptions	Conditions assumed to be true in the TOE environment.
Evaluation Technical Report (ETR)	Document that records the results of the evaluation phase.
Monitoring Technical Report (MTR)	Document that records the results of the monitoring phase.
Non- Conformity	Non-compliance detected during the evaluation or monitoring process that invalidates the result.
Composite Assurance Score	Final assurance value of the TOE, periodically updated.
Evaluation Assurance Score	Result of the initial evaluation phase.
Monitoring Assurance Score	Result of the monitoring phase.
Penetration Testing	Controlled attacks intended to identify exploitable vulnerabilities.
Functional Testing	Tests intended to verify the correct implementation of security requirements.
Applicant	Entity that requests the product evaluation.
Vulnerability	Weakness of the TOE or its libraries that may be exploited through an attack.

8. ACRONYMS

CCN	National Cryptologic Center
DV	Direct Verification
IV	Indirect Verification
CICLON	National Iterative CLOud Certification
CPSTIC	Catalogue of ICT Products and Services
DAS	Service Architecture Document
DIAS	Service Architecture Diagram
ST	Security Target
ENS	National Security Scheme
ENECSTI	National Scheme for ICT Security Evaluation and Certification
ETR	Evaluation Technical Report
EUCC	European Cybersecurity Certification Scheme
ITC	Technical Instruction
MTR	Monitoring Technical Report
PGC	Composite Assurance Score
PGE	Evaluation Assurance Score
PGM	Monitoring Assurance Score
SBOM	Software Bill of Materials
STIC	Information and Communication Technology Service
TOE	Target of Evaluation
WAF	Web Application Firewall

9. REFERENCES

Annex A [CCN-STIC-2010]	Template for the Security Target of Cloud Products Evaluation (CICLON)
Annex B [CCN-STIC-2010]	Template for the Service Architecture Document of Cloud Products Evaluation (CICLON)
Annex C [CCN-STIC-2010]	Cloud Product Evaluation Technical Report Template (CICLON)
Annex D [CCN-STIC-2010]	Cloud Product Monitoring Technical Report Template (CICLON)
CCN-ITC-003	Technical Instruction for Security Evaluation in Web and Cloud Environments
FOR-CIC-001	Cloud Product Evaluation Request Form (CICLON)
PO-006	Laboratory Accreditation Procedure
PO-CIC-005	Cloud Product Certification Procedure.
PO-CIC-010	Laboratory Authorization Procedure for CICLON Evaluations.
SBOM CycloneDX	Software Composition Standard.