

ICT Security Guide CCN-STIC 106

Procedure for the inclusion of ICT security products and services in the CPSTIC



October 2026

Published by:



Centro Criptológico Nacional, 2026



CCN

c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN

2026.10.08 13:00:36 +02'00'

Publication date: October 2026

LIMITATION OF LIABILITY

This document is provided in accordance with the terms set out herein, expressly disclaiming any implied warranty that may be related to it. Under no circumstances may the Centro Criptológico Nacional be held liable for any direct, indirect, incidental or extraordinary damage arising from the use of the information and software referred to herein, even when advised of such a possibility.

LEGAL NOTICE

Without the written authorisation of the Centro Criptológico Nacional, and subject to the penalties established by law, the partial or total reproduction of this document by any means or process, including reprography and computer processing, and the distribution of copies thereof by means of public rental or lending, are strictly prohibited.

CONTENTS

1. INTRODUCTION	3
2. PURPOSE AND SCOPE	5
3. TERMS AND DEFINITIONS	6
3.1 DEFINITIONS	6
3.2 STRUCTURE OF THE CPSTIC	6
3.3 INCLUSION PROCEDURE DOCUMENTS	7
4. PROCEDURE FOR INCLUSION IN THE LIST OF QUALIFIED PRODUCTS AND SERVICES (QUALIFICATION)	9
4.1 INITIAL QUALIFICATION	11
4.1.1. ON-PREMISE ICT SECURITY PRODUCTS	11
4.1.2. CLOUD-DEPLOYED ICT SECURITY PRODUCTS	13
4.2 RENEWAL OF THE QUALIFICATION	13
4.3 EXTENSION OF THE SCOPE OF THE QUALIFICATION (QUALIFICATION OF NEW SOFTWARE VERSIONS OR HARDWARE MODELS)	13
4.3.1. INCLUSION OF NEW VERSIONS	15
4.4 QUALIFICATION FILES AND TIME LIMITS	15
4.4.1. OPENING AND VALIDITY OF THE FILE	15
4.4.2. TIME LIMIT FOR RESOLVING THE PROCESS	15
4.4.3. EXTRAORDINARY EXTENSION	16
4.4.4. CLOSURE OF THE FILE AND NEW APPLICATION	16
4.5 PHASES OF THE PROCEDURE	16
4.5.1. APPLICATION FOR INCLUSION	16
4.5.2. REVIEW OF THE APPLICATION AND NOTIFICATION OF FILE OPENING	19
4.5.3. REVIEW OF THE PROPOSED SECURITY TARGET	20
4.5.4. REVIEW OF THE CERTIFICATION OR EVALUATION PROVIDED	20
4.5.5. PROVISIONAL INCLUSION AND SUBMISSION OF THE SECURE USE PROCEDURE	21
4.5.6. FINAL INCLUSION	22
4.5.7. RENEWAL OR EXTENSION OF SCOPE	22
5. PROCEDURE FOR INCLUSION IN THE COMPLIANCE AND GOVERNANCE LIST	23
5.1 APPLICATION FOR INCLUSION	23
5.2 GENERAL CONSIDERATIONS	23
5.3 REQUIRED EVIDENCE	24
5.4 DECISION AND PROVISIONAL INCLUSION	24
5.5 RENEWAL	25
5.6 SUMMARY OF EVIDENCE	25
6. VALIDITY AND EXCLUSION OF PRODUCTS	25
6.1 VALIDITY OF THE INCLUSION OF PRODUCTS IN THE CPSTIC	25
6.2 EXCEPTIONAL EXTENSION OF VALIDITY	26
6.3 EXCLUSION FROM THE CPSTIC	26
7. INCLUSION BADGES	27
7.1 CONDITIONS OF USE	27
7.2 QUALIFIED PRODUCT BADGE	27
7.3 QUALIFIED CLOUD-DEPLOYED SECURITY PRODUCT BADGE	28
7.4 COMPLIANCE AND GOVERNANCE BADGE	28
8. REFERENCES	29
9. ABBREVIATIONS	30

1. INTRODUCTION

The acquisition of an ICT security product or the procurement of an ICT security service that will handle national classified information or sensitive information must be preceded by a process verifying that the security mechanisms implemented in the product or service are adequate to protect that information.

The evaluation and certification of an ICT security product or service is the only objective means of assessing and attesting its ability to handle information securely. In Spain, this responsibility is assigned to the Centro Criptológico Nacional (National Cryptologic Centre, CCN) by Royal Decree 421/2004 of 12 March [1], in its articles 1 and 2.1, which establish that the Director of the CCN is the information and communications technology security certification authority and the cryptologic certification authority.

Likewise, article 19, *Acquisition of security products and procurement of security services*, of Royal Decree 311/2022 of 3 May, regulating the National Security Framework (Esquema Nacional de Seguridad, ENS) [2], provides as follows (unofficial translation):

- 1. In the acquisition of information and communications technology security products or the procurement of information and communications technology security services that are to be used in information systems within the scope of this royal decree, those whose security functionality related to the purpose of their acquisition is certified shall be used, in proportion to the category of the system and the security level determined.*
- 2. The Certification Body of the National Information Technology Security Evaluation and Certification Scheme of the Centro Criptológico Nacional, taking into account the national and international evaluation criteria and methodologies recognised by this body and depending on the intended use of the specific product or service within its competences, shall determine the following aspects:*
 - a) The security functional requirements and the certification assurance requirements.*
 - b) Other additional security certifications required by regulations.*
 - c) Exceptionally, the criterion to be followed in cases where no certified products or services exist.*
- 3. The procurement of security services shall be governed by the provisions of the preceding paragraphs and by article 16.*

In addition, the security measures set out in Annex II of the ENS for information systems of **MEDIUM and HIGH** category include the following (unofficial translation):

- **[op.pl.5.1]** The CCN Catalogue of Information and Communications Technology Security Products and Services (CPSTIC) shall be used to select the products or services supplied by a third party that form part of the security architecture of the system, as well as those expressly referred to in the measures of this royal decree.

Where there are no products or services in the CPSTIC that implement the required functionalities, certified products shall be used in accordance with article 19.

A Technical Security Instruction shall set out the criteria relating to the acquisition of security products.

– **[op.pl.5.2]** If the system provides a security service to a third party within the scope of the ENS, the product or products on which that service is based must undergo a qualification process and be included in the CPSTIC, or provide a certification that meets the security functional and assurance requirements in accordance with article 19.

By virtue of these competences, and in order to address the provisions of article 19 and measure [op.pl.5] of the ENS, the CCN publishes guide **CCN-STIC-105 — Catalogue of Information and Communications Technology Security Products and Services (CPSTIC)** [3].

2. PURPOSE AND SCOPE

The purpose of this guide is to define the procedure and the evaluations required to include a security product or service in the CPSTIC [3], both in the list of **Qualified Products and Services** and in the list of Products and Services for **Compliance and Governance**. Inclusion in the list of Approved Products is governed by CCN-STIC-102 [4] and falls outside the scope of this guide.

This guide contains three annexes:

- Annex A Requirements Justification (JR) Template,
- Annex B Differential Analysis Report (IAD) Template,
- Annex C Secure Use Procedure (PES) Template.

3. TERMS AND DEFINITIONS

3.1 DEFINITIONS

On-premise ICT security product: a set of software, firmware and/or hardware components that provide security functionality, designed for use in or incorporation into a defined system or operating environment, and which is deployed and operated on the organisation's own infrastructure.

Cloud-deployed ICT security product: a security product that is supplied and operated on a cloud infrastructure, in any of its models (SaaS, PaaS or IaaS).

ICT security service: for the purposes of this guide, the term "service" is equivalent to "cloud-deployed product".

Product or service for compliance and governance: one which, without forming part of the security architecture of the system, facilitates compliance with security regulations and the governance of the organisation. This term covers both on-premise products and cloud-deployed security products.

Fundamental Security Requirements (RFS): the minimum evaluation and/or certification requirements that a given product or service must meet in order to be included in the CPSTIC. These requirements are determined by various factors, such as the type of security product, the use case, or the classification level or ENS category for which qualification is requested. They are defined in guide CCN-STIC-140 Reference taxonomy for ICT security products [5].

3.2 STRUCTURE OF THE CPSTIC

The CPSTIC is structured into three (3) lists —Approved Products, Qualified Products and Services, and Compliance and Governance— defined as follows (see Table 1 and Figure 1):

- a) **Approved Products and Services:** products and services considered suitable for handling classified information of a given scope (national, International Organisations) and up to a maximum classification level specified for each product.
- b) **Qualified Products and Services:** security products and services that meet the security requirements set by the CCN for handling sensitive information under the ENS. As with approved products and services, the maximum system category for which each product or service is considered suitable (HIGH or MEDIUM) will be specified.
- c) **Products and Services for Compliance and Governance:** products or services which, without forming part of the security architecture of the system, facilitate compliance with security regulations and security governance.

CPSTIC list	Information handled
Approved Products	CLASSIFIED
Qualified Products and Services	SENSITIVE (ENS)
Compliance and Governance	Any type

Table 1. Lists that make up the CPSTIC

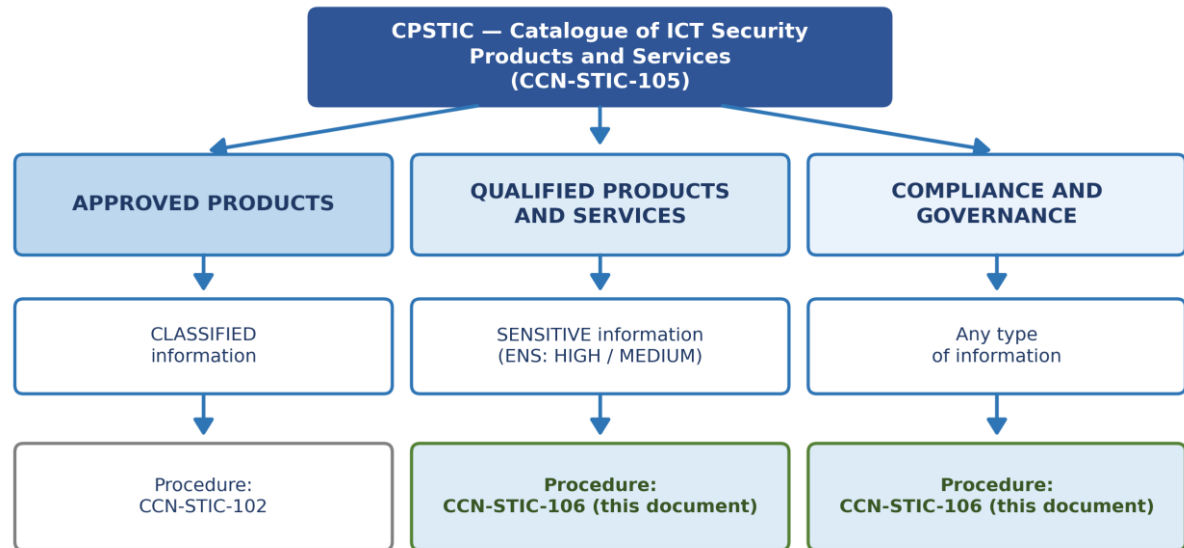


Figure 1. Structure of the CPSTIC and applicable procedure guides

The RFS applicable to qualified products, depending on the type of product, are set out in the annexes to guide **CCN-STIC-140** [5].

A product qualified by the CCN shall refer to a specific configuration defined in a Secure Use Procedure (PES), which will be published as a CCN-STIC guide and referenced in the information contained in the CPSTIC.

3.3 INCLUSION PROCEDURE DOCUMENTS

The documents involved in the inclusion process are listed in Table 2, which also indicates who prepares them and the source that defines their content.

Document	Prepared by	Content defined in
Application for inclusion (FOR-CPSTIC-02) and responsible statement (FOR-CPSTIC-01)	Applicant	Forms published on the CPSTIC website
Security Target (DS) — Common Criteria or LINCÉ	Applicant	Original certification methodology
Security Target (DS) — Complementary STIC Evaluation	Applicant	CCN-STIC-2003 [6]
Security Target (DS) and Service Architecture Document (DAS)	Applicant	Annexes A and B of CCN-STIC-2010 [7] [8]

Document	Prepared by	Content defined in
— cloud-deployed security products		
Requirements Justification (JR)	Applicant	Annex A of this guide [9]
Differential Analysis Report (IAD)	Applicant	Annex B of this guide [10]
Secure Use Procedure (PES)	Applicant	Annex C of this guide [11]
Penetration test report — Compliance and Governance	Laboratory accredited under the ENECSTI	CCN-STIC 2030
Responsible statement (DAS) — Cloud Compliance and Governance	Applicant	Annex B of CCN-STIC-2010
Evaluation plan	Laboratory	Validated by the CCN for each file
Evaluation reports (ITE, ITM)	Laboratory	CCN-STIC-2004 [12] (ITE) and CCN-STIC-2010 [13] (ITM)
COM-INI, RRPDS, ITI and RITI	CCN	Section 4.5

Table 2. Documents involved in the procedure

Figure 2 summarises, for each type of file, the processes allowed, the assurance required, the evidence required and the validity of the inclusion.

QUALIFICATION FILE · On-premise ICT security product Section 4	
Processes	Initial qualification · Renewal · Extension of scope (series and versions)
Assurance required	HIGH: Common Criteria, or LINCE under the conditions of section 4.1.1.2 MEDIUM: LINCE, as a minimum RFS not covered: Complementary STIC Evaluation (section 4.1.1.1)
Evidence	CC/LINCE certification and DS (or proposed DS) · JR · versioning policy IAD for extensions of scope
Validity	File: up to 5 years from the date of the certification Qualification: 2 years or until end of security support, whichever is earlier

QUALIFICATION FILE · Cloud-deployed security product Section 4	
Processes	Initial qualification · Renewal Extension of scope not allowed: CICLON does not use versioning (4.3.1)
Assurance required	CICLON evaluation (CCN-STIC-2010) covering the RFS of the family and category Verdict: Composite Assurance Percentage (PGC = PGE + PGM)
Evidence	DS and DAS (Annexes A and B of CCN-STIC-2010) · JR
Validity	File: coincides with the qualification (2 years) Qualification: 2 years · renewal requires a new full application

COMPLIANCE AND GOVERNANCE FILE Section 5	
Processes	Inclusion · Renewal
Assurance required	Penetration testing in accordance with CCN-STIC 2030, carried out by a laboratory accredited under the ENECSTI
Evidence	Penetration test report In the cloud, also: responsible statement (DAS) of valid ENS certification
Validity	Inclusion: 2 years · renewal requires a new full application

Figure 2. Types of file and conditions applicable to each list

4. PROCEDURE FOR INCLUSION IN THE LIST OF QUALIFIED PRODUCTS AND SERVICES (QUALIFICATION)

This section describes the procedure for inclusion in the CPSTIC list of **Qualified Products and Services**, applicable both to *on-premise* ICT security products and to cloud-deployed security products. Figure 3 illustrates *the* procedure.

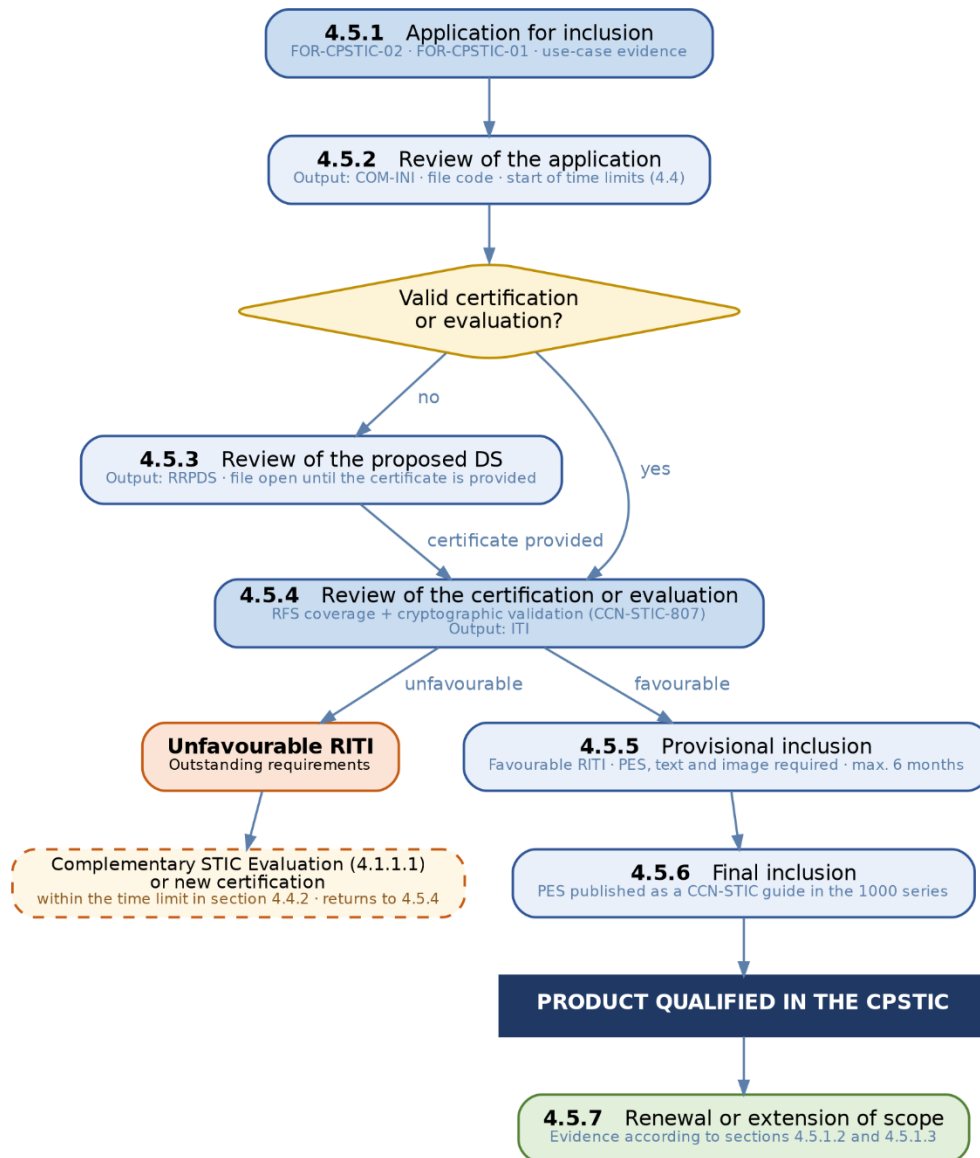


Figure 3. Procedure for inclusion in the list of Qualified Products and Services

In the qualification application, the applicant shall indicate the family or families into which the product or service fits, in accordance with the taxonomy established in guide CCN-STIC-140 [5], since the applicable RFS and the associated evidence depend on them.

If the product or service does not fit into any of the families covered by the taxonomy, the applicant shall state this in the application by indicating the family "Other tools". The CCN will study such applications individually and determine, on a case-by-case basis, which security requirements the product or service must implement and certify.

The CCN reserves the right to:

- a) Request additional information to verify that all the RFS of the family have been evaluated in applications that provide certifications.

- b) Reject the application if qualification of the main functionality of the product is not requested.
- c) Request additional information from the applicant on the security functionalities implemented by the product.
- d) Revoke the qualification of multi-function products where the applicant makes misleading claims about the qualified functionalities.

Three types of process are distinguished within this procedure:

- a) Initial qualification.
- b) Renewal of the qualification.
- c) Extension of the scope of the qualification (qualification of new software versions or hardware models).

4.1 INITIAL QUALIFICATION

Initial qualification, or inclusion in the list of Qualified Products and Services, requires evidence of a certification or an evaluation recognised by the CCN. This section defines the general requirements applicable to each type of product.

4.1.1. ON-PREMISE ICT SECURITY PRODUCTS

As a general rule, for a product to be qualified for ENS **HIGH** category it must meet one of these two conditions:

- a) Hold a certification under the Common Criteria methodology that includes the RFS defined for that product family or families.
- b) Hold a National Essential Security Certification (LINCE) [14] that includes the RFS defined for that product family or families, provided that the additional conditions described in section 4.1.1.2 are met.

For MEDIUM category, the product must hold, as a minimum, a **LINCE** certification [14].

If, in either case, the certification provided does not include all the RFS defined for that product family, the process must be completed by carrying out a **Complementary STIC Evaluation** as described in section 4.1.1.1.

4.1.1.1. COMPLEMENTARY STIC EVALUATION

The Complementary STIC Evaluation shall cover the security requirements not included in the initial certification and must be carried out in one of the laboratories accredited under the National Information Technology Security Evaluation and Certification Scheme (ENECSTI).

The evaluation procedure shall be based on the LINCE methodology (CCN-STIC-2001 [14] and CCN-STIC-2002 [15]), with the following modifications:

- a) There shall be no time restrictions.

- b) The vulnerability analysis shall focus on the requirements included in the DS and on public vulnerabilities disclosed after certification.
- c) Penetration testing of the target of evaluation (TOE) shall last a minimum of **five working days**.

To carry out the Complementary STIC Evaluation, the manufacturer must provide, as a minimum:

- a) Security Target (DS).
- b) The TOE operation and installation guides.
- c) The execution environment.

The DS shall be prepared in accordance with CCN-STIC 2003 [6] and must be validated by the CCN before the evaluation begins. It shall specify the security functionalities to be evaluated —those not covered by the original certification—, their mapping to the outstanding RFS and the assumptions about the environment, which by default shall be those of the certification.

The result shall be recorded in the Evaluation Technical Report (ITE), prepared in accordance with the CCN-STIC-2004 template [12].

4.1.1.2. QUALIFICATION FOR ENS HIGH BASED ON A LINCE CERTIFICATION

Products may be qualified for **ENS HIGH on the basis of a valid LINCE certification**, provided that they meet the following requirements:

- a) The LINCE certification is valid and covers the requirements for MEDIUM category.
- b) The cryptography implemented and required in the RFS meets the requirements for HIGH category.
- c) Where the set of requirements for HIGH category is larger than for MEDIUM category, a Complementary STIC Evaluation (section 4.1.1.1) shall be carried out, taking the LINCE certification as the original certification.
- d) The product shall undergo, periodically and at least once a year, a vulnerability analysis and penetration testing at a laboratory accredited under the ENECSTI. On first qualification, this commitment shall be evidenced by the contract signed with the laboratory for the following year's maintenance; such maintenance shall be performed on the qualified version. In addition, if the qualified version needs to be updated, the scope extension procedure described in section 4.3 shall apply.

If the product ceases to meet the first condition, it shall be excluded from the CPSTIC; if it ceases to meet any of the others, it shall lose its HIGH qualification and shall be listed as qualified for MEDIUM category. In particular, if the periodic vulnerability analysis and penetration testing do not meet the HIGH category requirements, the product shall be listed as qualified for MEDIUM category; if the result is also unfavourable against the MEDIUM category requirements, the product shall be excluded from the CPSTIC.

4.1.2. CLOUD-DEPLOYED ICT SECURITY PRODUCTS

For the qualification of cloud-deployed security products, an evaluation shall be required in accordance with the Cloud Product Evaluation Methodology (**CICLON**) [13], described in CCN-STIC-2010, including the RFS defined for that product family in the requested category, in accordance with section 4.5.1.

The verdict of the CICLON evaluation is the **Composite Assurance Percentage (PGC)**, which combines the Evaluation Assurance Percentage (PGE), obtained in the initial evaluation phase, and the Monitoring Assurance Percentage (PGM), obtained in the continuous and periodic monitoring phase. The PGC is updated at each iteration of the monitoring phase throughout the validity of the certification. Depending on the value of the PGC, the product may:

- a) Be initially included as a qualified product for HIGH or MEDIUM category.
- b) Remain in the CPSTIC in the same or a different category.
- c) Be excluded from the CPSTIC.

4.2 RENEWAL OF THE QUALIFICATION

When a product is included in the CPSTIC, it is assigned a "validity review date" which shall be no later than two (2) years from the initial qualification. As its name suggests, this is the date on which the applicant and the CPSTIC team must review whether or not the product may remain in the catalogue.

To this end, the applicant must ensure the following conditions:

- a) The product, in the version included in the CPSTIC, still has security support, regardless of whether or not it is still marketed.
- b) The certification provided for the qualification is less than five (5) years old.
- c) The product continues to meet the RFS in force and there are no uncorrected critical vulnerabilities; an update of the vulnerability analysis may be required for this purpose.

If all three conditions are met, the manufacturer shall send the corresponding renewal application (FOR-CPSTIC-02) to the CPSTIC; the CCN will carry out the appropriate checks and update the product's "validity review date".

This procedure shall only apply to *on-premise* products.

4.3 EXTENSION OF THE SCOPE OF THE QUALIFICATION (QUALIFICATION OF NEW SOFTWARE VERSIONS OR HARDWARE MODELS)

The Common Criteria and LINCE certification methodologies, used for the qualification of *on-premise* products, apply only to the version or versions of the product and the hardware models specified in the DS associated with the certification.

For the qualification of software versions later than a certified one, or of hardware models not included in the initial certification, a streamlined procedure has been

established that makes it possible to demonstrate compliance with the RFS without undertaking a new certification process, which would be more costly and lengthy and, at times, unfeasible given the product life cycle.

This procedure consists of carrying out a **Complementary STIC Evaluation** as described in section 4.1.1.1, covering:

- **New versions of the product.** The differences with respect to the certified version are evaluated and, where the new version introduces security functionalities affecting the RFS, those functionalities.
- **New models or series of products.** The aim is to extend the qualification to other models in the same series built on the same functional basis. The hardware, firmware and software differences with respect to the certified models are evaluated.

For both cases, the CCN reserves the right not to apply the procedure where any of the following circumstances arises:

- a) The changes detected are considered "major changes" (e.g. they affect the product architecture).
- b) The original certification is more than five (5) years old.

Table 3 sets out the terms used:

Product series	A set of products from a developer, built on the same functional basis, whose design, hardware, firmware or software may vary from one product to another.
Reference TOE	The set of models selected in the original certification provided by the manufacturer.
Additional models	Models not included in the original certification which are to be qualified.

Table 3. Terms used in the qualification of product series

To initiate the procedure, the applicant must provide:

- a) The DS of the original certification.
- b) A Differential Analysis **Report (IAD)**, in accordance with the template in Annex B of this guide [10], signed by the technical manager, with a feature matrix describing the *hardware*, *firmware* and *software* differences with respect to the reference TOE. Where the product has been the subject of previous extensions, the IAD may be based on the latest IAD accepted by the CCN, expressly stating this.
- c) Optionally, the updated proposed PES.

The procedure comprises: verification of the completeness of the IAD and a Complementary STIC Evaluation if differences are found that impact the required security functionalities. No time limits shall be set for testing models with differences affecting certified security functionalities; where sampling is used, a minimum effort of two (2) days per model shall be established.

4.3.1. INCLUSION OF NEW VERSIONS

This applies when the aim is to qualify a version that does not correspond to the certified one because it implements changes, provided that it is demonstrated that the changes do not affect certified security functionalities or that they can be evaluated by means of this evaluation. Where the new version introduces new security functionalities affecting the RFS, the evaluation shall apply to the added functionalities.

This procedure does not apply to cloud-deployed security products, since the CICLON methodology does not use versioning and incorporates a periodic monitoring phase that continuously reviews the security status of the product.

4.4 QUALIFICATION FILES AND TIME LIMITS

The file is the processing unit that links a product or service with its qualification process. All processes relating to a product or service are carried out under the same qualification file until its certification is renewed.

4.4.1. OPENING AND VALIDITY OF THE FILE

Once the CCN has reviewed the qualification application and determined that it is correct, it will send the applicant the **notification of file opening**, as described in section 4.5.2.

The file may remain open for as long as the certification or evaluation on which it is based remains valid, that is:

- a) **A maximum of five (5) years** in the case of Common Criteria or LINCE.
- b) **A maximum of two (2) years** in the case of CICLON.

During this period, applications for renewal and for extension of scope (new models or versions) relating to that certification will be processed.

Obtaining a new certification will result in the opening of a new file and must be applied for as an initial inclusion, even if the product is already listed in the catalogue.

In the case of *on-premise* products, the file will be closed when the certification on which it is based reaches five (5) years of age, at which point renewals and extensions of scope will no longer be accepted.

In the case of cloud-deployed security products, the validity of the file coincides with that of the qualification, so each inclusion gives rise to a new file.

4.4.2. TIME LIMIT FOR RESOLVING THE PROCESS

Each process —initial inclusion, renewal or extension of scope— must be resolved within **one (1) year** of the issue of the corresponding COM-INI.

During that period the applicant must provide the required evidence: the certificate, where a proposed security target has been reviewed (section 4.5.3), or the Evaluation Technical Report (ITE), where an unfavourable RITI with outstanding requirements has

been issued (section 4.5.4). The review of successive versions of the proposed security target does not restart the time limit.

4.4.3. EXTRAORDINARY EXTENSION

The time limit in section 4.4.2 may be extended **once only, by an additional six (6) months**, up to a maximum of eighteen (18) months. The extension must be requested from the CCN in writing, with reasons, before the time limit expires. This extension is independent of the exceptional extension of validity provided for in section 6.2, which refers to products already included in the catalogue.

4.4.4. CLOSURE OF THE FILE AND NEW APPLICATION

Once the time limit, including any extension, has elapsed without the required evidence having been provided, the file will be **closed**. A new application will be processed from the beginning, verifying the RFS of the family and the authorised cryptographic algorithms in force at that time.

4.5 PHASES OF THE PROCEDURE

The procedure is structured into the phases described in this section. The application and its review are common to all use cases; the remaining phases apply depending on the use case requested, in accordance with Table 4.

4.5.1. APPLICATION FOR INCLUSION

Input documents: forms FOR-CPSTIC-02 and FOR-CPSTIC-01 and the evidence required for the declared use case, as detailed in sections 4.5.1.1 to 4.5.1.3.

Regardless of the modality, the process begins with the submission to the CCN (soporte.cpstic@ccn.cni.es) of the **application for inclusion** in the list of Qualified Products and Services, completing the following forms, available on the CPSTIC website (<https://cpstic.ccn.cni.es>):

- **FOR-CPSTIC-02** — Application for inclusion in the Catalogue of STIC Products and Services (CPSTIC).
- **FOR-CPSTIC-01** — Responsible statement for inclusion in the Catalogue of STIC Products and Services (CPSTIC).

The application may be submitted by the manufacturer, a supplier or a public administration body.

4.5.1.1. INITIAL QUALIFICATION

Applicable when the aim is to include a specific product and version in the CPSTIC for the first time, or when a new certification has been obtained that gives rise to the opening of a new file (section 4.4.1). Depending on what is declared in the application, the following shall be provided:

On-premise ICT security product with a valid certification. The following shall be attached to the application:

- a) The **Common Criteria or LINCE** certification and its **Security Target (DS)**.
- b) **Requirements Justification (JR)**, in accordance with the template in Annex A of this guide [9], provided that there are differences between the RFS defined for the requested family and those declared in the security target.
- c) **Differential Analysis Report (IAD)**, in accordance with the template in Annex B of this guide [10], where the version or models to be qualified do not match those covered by the certification provided.
- d) Optionally, the product's **versioning policy**, describing the meaning of each character of the version and the update conditions.
- e) Optionally, the list of cryptographic algorithms used and a proposed PES (mandatory once the product has been included) in accordance with the template in Annex C of this guide [11].

On-premise ICT security product without a valid certification. The product does not yet hold a Common Criteria or LINCE certification and is seeking certification. The following shall be attached to the application:

- a) The **proposed Security Target (DS)** under which the product is to be certified, which the CCN will review in accordance with section 4.5.3.
- b) The **Requirements Justification (JR)**, in accordance with the template in Annex A of this guide [9].
- c) The product's **versioning policy**, describing the meaning of each character of the version and the update conditions.
- d) Optionally, the list of cryptographic algorithms used and a proposed PES (mandatory once the product has been included) in accordance with the template in Annex C of this guide [11].

Once the RRPDS has been issued, the file will remain open until the applicant provides the certificate, within the time limit in section 4.4.2. Once the certificate has been provided, the procedure continues with the certification review phase (section 4.5.4).

Cloud-deployed security product. The product must meet the RFS associated with its main functionality (the same as an equivalent on-premise ICT security product). The generic requirements applicable to any cloud-deployed security product are covered by the CICLON methodology itself during evaluation and monitoring.

The following shall be attached to the application:

- a) The **Security Target (DS)**, in accordance with the template in **Annex A of CCN-STIC-2010** [7], which will be validated in the first instance by the CPSTIC team.
- b) The **Service Architecture Document (DAS)**, in accordance with the template in **Annex B of CCN-STIC-2010** [8], which sets out the structure of the TOE and its operating environment, information flows, data jurisdiction and compliance with transparency requirements, among other aspects.

- c) The **Requirements Justification (JR)**, in accordance with the template in Annex A of this guide [9].
- d) Optionally, the list of cryptographic algorithms used and a proposed PES (mandatory once the product has been included).

4.5.1.2. RENEWAL

Applicable when the product is already included in the CPSTIC and the aim is to maintain its qualification when the validity review date is approaching or has been reached.

On-premise ICT security products. To this end, it shall be sufficient to submit the application (FOR-CPSTIC-02), selecting the **renewal** option, and to provide evidence that the product still has security support: a document signed by the manufacturer where this information is not public or, where it is, a report with a screenshot of the evidence and the URL of the public page or document.

Cloud-deployed security products. Renewal requires a **new full application**, providing all the information and evidence as if it were an initial inclusion (section 4.5.1.1), and will give rise to a new CICLON evaluation. If the validity date is reached without renewal, the product will be excluded from the CPSTIC (section 6.3).

4.5.1.3. EXTENSION OF SCOPE

Applicable when the aim is to extend the scope of the qualification to a new version of the product or to new models or *appliances* in a series, on the basis of the existing certification and qualification. The extension updates the qualification review date (section 6.1).

Depending on what is declared in the application, the extension may refer to **product series** or to **versions**. In both cases the following shall be provided:

- a) The **Security Target** of the original certification.
- b) The **Differential Analysis Report (IAD)**, in accordance with the template in Annex B of this guide. Where the product has been the subject of previous extensions, the IAD may be based on the latest IAD accepted by the CCN, expressly stating this. [10].
- c) Optionally, the updated proposed PES.

The CCN will review the IAD and validate which security functions must be evaluated or certified again. If no additional function needs to be evaluated, the file will proceed to the inclusion of the product in the catalogue. If, on the other hand, additional security functions need to be evaluated, the applicant may choose between a **Complementary STIC Evaluation** (section 4.1.1.1) or a **new** Common Criteria or LINCE certification.

4.5.1.4. SUMMARY OF EVIDENCE BY USE CASE

Table 4 summarises, for each use case, the documentation to be provided and the applicable phases and evaluation.

Use case	Documentation to be provided	Applicable phases and evaluation
Initial inclusion · on-premise with valid certification	Application (FOR-CPSTIC-02/01), CC/LINCE certification and DS, JR (where applicable) and versioning policy (optional).	Phases 4.5.1 · 4.5.2 · 4.5.4 · 4.5.5 · 4.5.6. Review of the certification against the RFS; if it does not cover them in full, Complementary STIC Evaluation (4.1.1.1).
Initial inclusion · on-premise without valid certification	Application, proposed DS and JR.	Phases 4.5.1 · 4.5.2 · 4.5.3 · 4.5.4 · 4.5.5 · 4.5.6. Review of the proposed DS (RRPDS); once the certificate is provided, it is reviewed in accordance with section 4.5.4.
Initial inclusion · cloud-deployed security product	Application, DS and DAS (Annexes A and B of CCN-STIC-2010) and JR.	Phases 4.5.1 · 4.5.2 · 4.5.3 · 4.5.4 · 4.5.5 · 4.5.6. CICLON evaluation; PGC verdict (4.1.2).
Renewal · on-premise	Application (FOR-CPSTIC-02) and evidence of current security support; where applicable, update of the vulnerability analysis.	Phases 4.5.1 · 4.5.2 · 4.5.4 · 4.5.7. Verification of valid certification (less than 5 years old) and of security support; renews for 2 years or until end of support, whichever is earlier.
Renewal · cloud-deployed security product	Full application and evidence, as for an initial inclusion.	Phases 4.5.1 · 4.5.2 · 4.5.3 · 4.5.4 · 4.5.5 · 4.5.6. New CICLON evaluation.
Extension of scope · product series	Application, original DS, IAD with feature matrix and, optionally, updated PES.	Phases 4.5.1 · 4.5.2 · 4.5.4 · 4.5.7. Complementary STIC Evaluation (4.1.1.1): evaluation plan validated by the CCN and sampling (minimum of 2 days per model).
Extension of scope · versions	Application, original DS, IAD and, optionally, updated PES.	Phases 4.5.1 · 4.5.2 · 4.5.4 · 4.5.7. Complementary STIC Evaluation (4.1.1.1) of the differences affecting certified security functionalities.
Case · ENS HIGH with LINCE certification (in addition to initial inclusion)	In addition to the requirements for initial inclusion: valid LINCE certification for MEDIUM category and contract with a laboratory for annual maintenance.	Conditions in section 4.1.1.2: HIGH category cryptography; if the HIGH RFS exceed those for MEDIUM, Complementary STIC Evaluation; vulnerability analysis and penetration testing at least once a year.

Table 4. Summary of evidence, phases and evaluation by use case

4.5.2. REVIEW OF THE APPLICATION AND NOTIFICATION OF FILE OPENING

Input documents: no additional documents; where applicable, the correction of any formal defects requested by the CCN.

Once the application has been reviewed and any formal defects corrected, the CCN will give notice of the start of the procedure by means of the **notification of file opening (COM-INI)**, which will assign a file code and determine the calculation of the time limits provided for in section 4.4. CCN staff will then review the documentation and evidence provided.

Output: notification of file opening (COM-INI), which assigns the file code and determines the calculation of the time limits in section 4.4.

4.5.3. REVIEW OF THE PROPOSED SECURITY TARGET

This phase applies only to products that do not hold a valid certification, whether *on-premise* ICT security products or cloud-deployed products.

Input documents: the proposed Security Target and the Requirements Justification (section 4.5.1.1) and, within the time limit in section 4.4.2, the certificate issued.

The CCN will analyse the proposed security target and the Requirements Justification against the RFS of the declared family and category, and will issue the **result of the review of the proposed security target (RRPDS)**, which will indicate whether, once the product has been certified in accordance with that security target, it will meet the requirements of the catalogue. In this way the applicant knows the expected result in advance before investing in certification, and avoids a certification that has already been issued subsequently requiring a Complementary STIC Evaluation or a new certification process.

The file will remain open, under the terms of section 4.4, until the applicant provides the certificate issued. During that period the applicant may ask the CCN to review successive versions of the proposed security target. Once the certificate has been provided, the procedure continues with the certification review phase (section 4.5.4), whether the certification has been issued on the reviewed security target or on a different one.

Output: result of the review of the proposed security target (RRPDS).

4.5.4. REVIEW OF THE CERTIFICATION OR EVALUATION PROVIDED

Input documents: the Common Criteria or LINCE certification, or the CICLON evaluation report, the list of cryptographic algorithms used and any complementary evidence required by the CCN.

In this phase the CCN verifies that the certification or evaluation provided covers the RFS of the requested family and category.

On-premise ICT security products. If the Common Criteria or LINCE certification covers all the applicable RFS, the CCN will carry out a basic review, without additional laboratory evaluations, will issue a FAVOURABLE ITI with the proposal for inclusion and will notify the applicant of the FAVOURABLE Result of the Inclusion Technical Report (RITI).

If the certification does not cover all the RFS, the CCN will issue an **UNFAVOURABLE RITI** indicating the outstanding requirements, which the applicant may demonstrate by

means of a Complementary STIC Evaluation (section 4.1.1.1) or a new certification in accordance with the required requirements, within the time limit provided for in section 4.4.2.

Where the RITI is UNFAVOURABLE, it will indicate the degree of compliance with the RFS and the complementary evaluations or tests required.

Cloud-deployed security products. The CCN will verify the result of the CICLON evaluation under the terms of section 4.1.2.

At the same time, if the product uses cryptographic algorithms, the CCN will validate that they provide the required cryptological security and that they are among those authorised for the ENS (CCN-STIC-807 [16]), according to the category requested.

Output: Inclusion Technical Report (ITI), which incorporates the cryptographic validation, and notification of the RITI. Where the result is unfavourable, the CCN will issue an UNFAVOURABLE RITI indicating the outstanding requirements.

4.5.5. PROVISIONAL INCLUSION AND SUBMISSION OF THE SECURE USE PROCEDURE

Input documents: the favourable Inclusion Technical Report (ITI) issued in the previous phase, the FAVOURABLE RITI notified in the previous phase and the product description and image provided by the applicant.

Once the FAVOURABLE RITI has been notified, the applicant will provide the product description and image for its entry in the catalogue and, if not provided with the application, the Secure Use Procedure (PES).

Once the description and image have been received, the CCN will include the product in the list of Qualified Products and Services as **Qualified**, on a **provisional** basis until the PES is delivered. The provisional period shall last a maximum of **six (6) months**. The PES shall be prepared in accordance with the template in Annex C of this guide [11].

The proposal shall be sent, in editable format and respecting the structure and styles of that template, to soporte.cpstic@ccn.cni.es, stating the product name and the file code in the subject line.

Annex C is published in PDF format; its editable version may be requested from the same address.

Where the product is also to be approved for handling national classified information in accordance with CCN-STIC-102, the PES shall cover the use case provided for this purpose in Annex C.

The product shall be considered qualified from the notification of the favourable RITI, even if, for editorial reasons, it is not yet listed in the catalogue.

Output: provisional inclusion of the product in the CPSTIC. The provisional status ends with the delivery of the PES, within a maximum of six (6) months.

4.5.6. FINAL INCLUSION

Input documents: the Secure Use Procedure (PES) delivered in accordance with section 4.5.5.

The CCN will review the PES provided and may return it with comments; the applicant will send the corrected versions through the same channel until the CCN's approval is obtained. Once validated, the CCN will publish it as a CCN-STIC guide in the 1000 series.

Once the guide has been published, the product will no longer be listed on a provisional basis and will be included **permanently** in the list, for the corresponding period, in accordance with section 6.1.

Any extension of scope or new qualified version affecting the content of the PES will require the applicant to send an updated version through the same channel, which will give rise to a new edition of the guide.

Output: publication of the PES as a CCN-STIC guide in the 1000 series and final inclusion of the product in the CPSTIC.

4.5.7. RENEWAL OR EXTENSION OF SCOPE

Input documents: the application for renewal or extension of scope and the evidence required under sections 4.5.1.2 and 4.5.1.3, as appropriate.

Once the checks described below have been carried out, the CCN will update the validity review date and renew the qualification for **two (2) years or until the end-of-security-support date declared by the manufacturer, whichever is earlier**, and within the maximum limit of five (5) years from the date of the certification.

The procedure is as follows:

- a) Sufficiently in advance of expiry, the manufacturer sends the application (FOR-CPSTIC-02), indicating the modality: renewal of the qualification or extension of scope.
- b) It provides **evidence of current security support** (for example, the manufacturer's life cycle or support statement) and, in the case of an extension, the Differential Analysis Report (IAD).
- c) The CCN verifies that the certification (CC/LINCE) is less than five (5) years old and that security support is maintained.
- d) Once the verification and, where applicable, the tests associated with the extension have been passed, the CCN extends the validity for two (2) years or until the declared end-of-support date, whichever is earlier.
- e) If a Complementary STIC Evaluation or a certification is in progress, the exceptional extension of three (3) months shall apply (section 6.2).

If the validity review date is reached without renewal or extension taking place, the product will be excluded from the CPSTIC in accordance with section 6.3.

Output: renewal or extension of the scope of the qualification.

5. PROCEDURE FOR INCLUSION IN THE COMPLIANCE AND GOVERNANCE LIST

This section describes the procedure for inclusion in the Compliance and Governance list. *Figure 4* illustrates it.

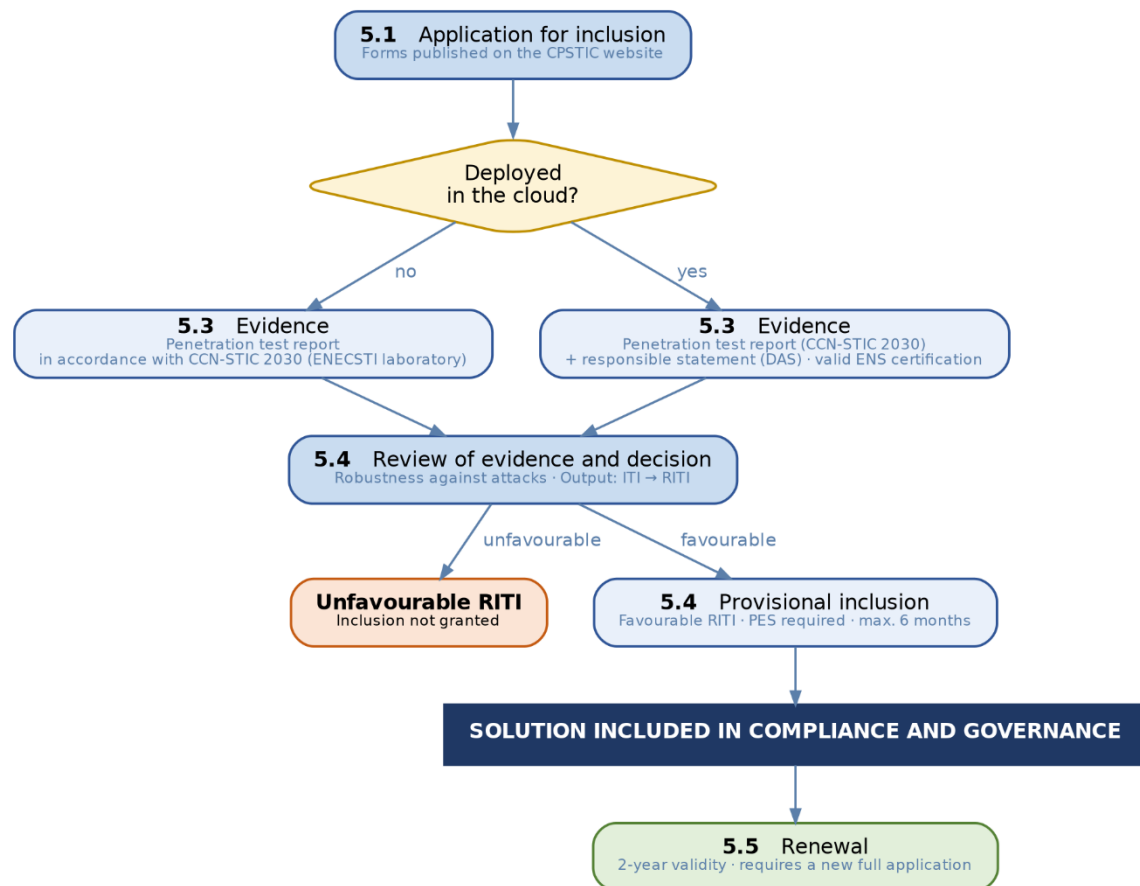


Figure 4. Procedure for inclusion in the Compliance and Governance list

5.1 APPLICATION FOR INCLUSION

The process begins with the submission to the CCN (soporte.cpstic@ccn.cni.es) of the **application for inclusion** in the Compliance and Governance list, completing the application forms published on the CPSTIC website (<https://cpstic.ccn.cni.es>).

The application may be submitted by the manufacturer, a supplier or a public administration body.

The evidence that must accompany the application is detailed in section 5.3.

5.2 GENERAL CONSIDERATIONS

The **Compliance and Governance** list groups solutions which, without forming part of the security architecture of the system, facilitate compliance with security regulations

and security governance. By their nature, they may be used in systems handling any type of information.

As they do not form part of the security architecture, these solutions **do not have associated RFS in CCN-STIC-140** [5]. Consequently, their inclusion is not based on verifying compliance with RFS, but on verifying the robustness of the solution against attacks, under the terms of section 5.3.

By way of guidance, the categories of solutions that may be included in this list include governance, risk and compliance (GRC) tools, tools supporting compliance with the ENS or the GDPR, security awareness and training tools, remote video identification tools and vulnerability management tools, among others.

5.3 REQUIRED EVIDENCE

Together with the application for inclusion (section 5.1), and depending on the type of solution, the following documentation shall be provided.

Solutions not deployed in the cloud. They must provide a penetration test report, prepared by a laboratory accredited under the ENECSTI, verifying their resistance to the tests described in guide CCN-STIC 2030 Security evaluation methodology for web environments [17]. The report shall contain, as a minimum:

- The unambiguous identification of the solution evaluated, its version and the test environment.
- The vulnerabilities detected, their criticality and their exploitability.
- The verdict: the existence of critical vulnerabilities or of uncorrected exploitable vulnerabilities will result in an unfavourable outcome.

Cloud-deployed security products. They must provide the penetration test report under the same terms as solutions not deployed in the cloud and, **in addition**, as the only additional documentary evidence, a responsible statement based on the template in **Annex B of CCN-STIC-2010** [8] (Service Architecture Document, DAS), demonstrating that the system or systems on which the product is deployed hold a **valid ENS certification of conformity**.

5.4 DECISION AND PROVISIONAL INCLUSION

The CCN will review the documentation and evidence provided and prepare the **Inclusion Technical Report (ITI)**, the result of which it will communicate by means of the **Result of the Inclusion Technical Report (RITI)**, which may be FAVOURABLE or UNFAVOURABLE.

If the RITI is favourable, the CCN will include the solution in the Compliance and Governance list, on a **provisional** basis until the Secure Use Procedure (PES) is delivered, if it was not provided with the application. The provisional period shall last a maximum of **six (6) months**. The PES shall be prepared in accordance with the template in Annex

C of this guide [11]. Where the PES is not applicable, the solution will be included permanently.

The proposal shall be sent under the same terms as provided for in section 4.5.5.

Once the solution has been included in the list, it may use the Compliance and Governance badge (section 7.4).

5.5 RENEWAL

Inclusion in the Compliance and Governance list, whether the solution is *on-premise* or a cloud-deployed security product, has a **validity of two (2) years**. **Renewal requires a new application**, providing all the information and evidence as if it were a new inclusion. In accordance with section 6.2, validity may exceptionally be extended by three (3) months where penetration testing is in progress.

5.6 SUMMARY OF EVIDENCE

Table 5 summarises the evidence required for inclusion in the Compliance and Governance list.

Evidence required for inclusion in the Compliance and Governance list	
Type of solution	Evidence and evaluation required
Solution not deployed in the cloud	Penetration test report in accordance with CCN-STIC 2030, carried out by a laboratory accredited under the ENECSTI.
Cloud-deployed security product	Penetration test report in accordance with CCN-STIC 2030, carried out by a laboratory accredited under the ENECSTI; and a responsible statement based on the template in Annex B of CCN-STIC-2010 (DAS) demonstrating that the system or systems on which the product is deployed hold a valid ENS certification of conformity.

Table 5. Evidence required for inclusion in Compliance and Governance

6. VALIDITY AND EXCLUSION OF PRODUCTS

This section sets out the conditions of validity of inclusion in the CPSTIC, the exceptional extension applicable to products already included and the grounds for exclusion from the catalogue.

6.1 VALIDITY OF THE INCLUSION OF PRODUCTS IN THE CPSTIC

Inclusion in the CPSTIC, in any of the lists covered by this guide, has a **validity of two (2) years**. The particulars of renewal and, where applicable, of the extension of validity are set out in sections 4.5.1.2, 4.5.7 and 5.5. Table 6 summarises these conditions.

List	Validity	Renewal / extension
Qualified security products (on-premise)	2 years or until the end of security support declared by the manufacturer (whichever is earlier)	May be renewed or extended if the product maintains security support (with evidence) and the certification (CC/LINCE) is less than 5 years old.
Cloud-deployed security products	2 years	Renewal requires a new application, providing all the information as if it were a new inclusion.
Compliance and Governance (on-premise or cloud)	2 years	Renewal requires a new application, providing all the information as if it were a new inclusion.

Table 6. Validity of inclusion in the CPSTIC by list

6.2 EXCEPTIONAL EXTENSION OF VALIDITY

For the Qualified Products and Services and Compliance and Governance lists, the validity of the inclusion may exceptionally be extended by **an additional three (3) months** where the manufacturer has initiated an inclusion or renewal process requiring a Complementary STIC Evaluation, a certification or, in the case of Compliance and Governance solutions, penetration testing, in order to allow time for that process to be completed.

6.3 EXCLUSION FROM THE CPSTIC

A product, cloud-deployed security product or solution may be excluded from the CPSTIC on any of the following grounds:

- **Reaching the validity date** (two years or, for *on-premise* products, the end-of-security-support date, whichever is earlier) without renewal or, where applicable, extension taking place.
- **Revocation or expiry of any of the required certifications** (*Common Criteria*, LINCE or ENS conformity). For *Common Criteria* or LINCE certifications, a maximum validity of five (5) years shall be considered.
- **Failure to meet the RFS in force** at the time of the validity review.
- **Existence of uncorrected critical vulnerabilities**. The manufacturer may be asked for an impact report; if the vulnerability is exploitable when following the PES, the entry will be excluded. For cloud-deployed security products, a critical vulnerability results in a PGC equal to 0 (FAIL verdict of the CICLON evaluation) and exclusion.
- **Failure to deliver the Secure Use Procedure (PES)** within the provisional inclusion period of six (6) months.
- **End of security support** by the manufacturer, who shall be obliged to notify the CPSTIC thereof.
- **Unfavourable result of the periodic review** of the evidence, including, for Compliance and Governance solutions, an unfavourable result in the update of

the penetration tests. In qualification for HIGH based on a LINCE certification, if the periodic analysis does not meet the HIGH category requirements, the product will move to MEDIUM category, and if it is unfavourable also against the MEDIUM category requirements, it will be excluded from the CPSTIC (section 4.1.1.2).

7. INCLUSION BADGES

7.1 CONDITIONS OF USE

The inclusion of a product, cloud-deployed security product or solution in the CPSTIC may be represented by the **inclusion badges** issued by the CCN, specific to each list. Their use is conditional on inclusion in the CPSTIC. The applicant may, on a voluntary basis, publicise the qualified or included entries by displaying the corresponding badge in its technical or commercial documentation, in any format. The current badges can be found in the "MEDIA" section of the CPSTIC website (<https://cpstic.ccn.cni.es/es/sobre-el-cpstic/media>).

Tampering with or partial reproduction of the badges is expressly prohibited, as is their use without indicating the product or solution with which they are associated. Once an entry has been excluded from the CPSTIC (section 6.3), the applicant must remove the badges used in its documentation.

7.2 QUALIFIED PRODUCT BADGE

This badge applies to qualified *on-premise* security products. It has the following appearance, including the maximum category for which the product is qualified (MEDIUM or HIGH). Table 7 indicates the systems for which each badge is suitable.



Figure 5. Qualified Product Badge — HIGH Category



Figure 6. Qualified Product Badge — MEDIUM Category

Use of products in the ENS according to the badge	
Qualification obtained	Suitable for systems
HIGH	ENS HIGH Cat. · ENS MEDIUM Cat. · ENS BASIC Cat.
MEDIUM	ENS MEDIUM Cat. · ENS BASIC Cat.

Table 7. Use of products in the ENS according to the badge

7.3 QUALIFIED CLOUD-DEPLOYED SECURITY PRODUCT BADGE

This badge applies to qualified cloud-deployed security products. It has the following appearance, including the maximum category for which the product is qualified (MEDIUM or HIGH). Table 8 indicates the systems for which each badge is suitable.



Figure 7. Qualified Cloud-Deployed Security Product Badge — HIGH Category



Figure 8. Qualified Cloud-Deployed Security Product Badge — MEDIUM Category

Use of cloud-deployed security products in the ENS according to the badge	
Qualification obtained	Suitable for systems
HIGH	ENS HIGH Cat. · ENS MEDIUM Cat. · ENS BASIC Cat.
MEDIUM	ENS MEDIUM Cat. · ENS BASIC Cat.

Table 8. Use of cloud-deployed security products in the ENS according to the badge

7.4 COMPLIANCE AND GOVERNANCE BADGE

This badge applies to solutions included in the Compliance and Governance list. It has the following appearance.



Figure 9. Compliance and Governance Badge

8. REFERENCES

- [1] Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional (Royal Decree 421/2004 of 12 March, regulating the National Cryptologic Centre).
- [2] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (Royal Decree 311/2022 of 3 May, regulating the National Security Framework).
- [3] CCN-STIC-105 Catalogue of Information and Communications Technology Security Products and Services (CPSTIC).
- [4] CCN-STIC-102 Procedure for the Approval of ICT Security Products for Handling National Classified Information.
- [5] CCN-STIC-140 Reference Taxonomy for ICT Security Products.
- [6] CCN-STIC-2003 Security Target Template (LINCE).
- [7] Annex A CCN-STIC-2010 Security Target (DS) Template.
- [8] Annex B CCN-STIC-2010 Service Architecture Document (DAS) Template.
- [9] Annex A CCN-STIC-106 Requirements Justification (JR) Template.
- [10] Annex B CCN-STIC-106 Differential Analysis Report (IAD) Template.
- [11] Annex C CCN-STIC-106 Secure Use Procedure (PES) Template.
- [12] CCN-STIC-2004 Evaluation Technical Report Template for the National Essential Security Certification (LINCE).
- [13] CCN-STIC-2010 Cloud Product Evaluation Methodology (CICLON).
- [14] CCN-STIC-2001 Definition of the National Essential Security Certification (LINCE).
- [15] CCN-STIC-2002 Evaluation Methodology for National Certification.
- [16] CCN-STIC-807 Cryptology for Use in the ENS.
- [17] CCN-STIC 2030 Security Evaluation Methodology for Web Environments.

9. ABBREVIATIONS

CC	Common Criteria.
CCN	Centro Criptológico Nacional (National Cryptologic Centre).
CICLON	Cloud Product Evaluation Methodology (CCN-STIC-2010).
COM-INI	Notification of opening of an inclusion file (Comunicación de Inicio de Expediente).
CPSTIC	Catalogue of ICT Security Products and Services (Catálogo de Productos y Servicios STIC).
DAS	Service Architecture Document (Documento de Arquitectura del Servicio).
DS	Security Target (Declaración de Seguridad).
ENECSTI	National Information Technology Security Evaluation and Certification Scheme (Esquema Nacional de Evaluación y Certificación de la Seguridad de las TIC).
ENS	National Security Framework (Esquema Nacional de Seguridad).
EU	European Union.
FOR	Form (Formulario).
GDPR	General Data Protection Regulation.
GRC	Governance, Risk and Compliance.
IaaS	Infrastructure as a Service.
IAD	Differential Analysis Report (Informe de Análisis Diferencial).
ICT	Information and Communications Technology.
ITE	Evaluation Technical Report (Informe Técnico de Evaluación).
ITI	Inclusion Technical Report (Informe Técnico de Inclusión).
ITM	Monitoring Technical Report (Informe Técnico de Monitorización).
JR	Requirements Justification (Justificación de Requisitos).
LINCE	National Essential Security Certification (Certificación Nacional Esencial de Seguridad).
NATO	North Atlantic Treaty Organization.
PaaS	Platform as a Service.
PES	Secure Use Procedure (Procedimiento de Empleo Seguro).
PGC	Composite Assurance Percentage (Porcentaje de Garantía Compuesto).
PGE	Evaluation Assurance Percentage (Porcentaje de Garantía de Evaluación).
PGM	Monitoring Assurance Percentage (Porcentaje de Garantía de Monitorización).
RFS	Fundamental Security Requirements (Requisitos Fundamentales de Seguridad).
RITI	Result of the Inclusion Technical Report (Resultado del Informe Técnico de Inclusión).
RRPDS	Result of the Review of the Proposed DS (Resultado de la Revisión de la Propuesta de DS).
SaaS	Software as a Service.
STIC	ICT Security (Seguridad de las Tecnologías de la Información y la Comunicación).
TOE	Target of Evaluation.

