RED ALERT LABS
IoT Security

INTRODUCTION TO EUROPEAN COMMON CRITERIA SCH

EUCC CANDIDATE SCHEME

SOG IS (“Senior Officials Group Information Systems Security“)

MRA (Mutual Recognition Agreement),

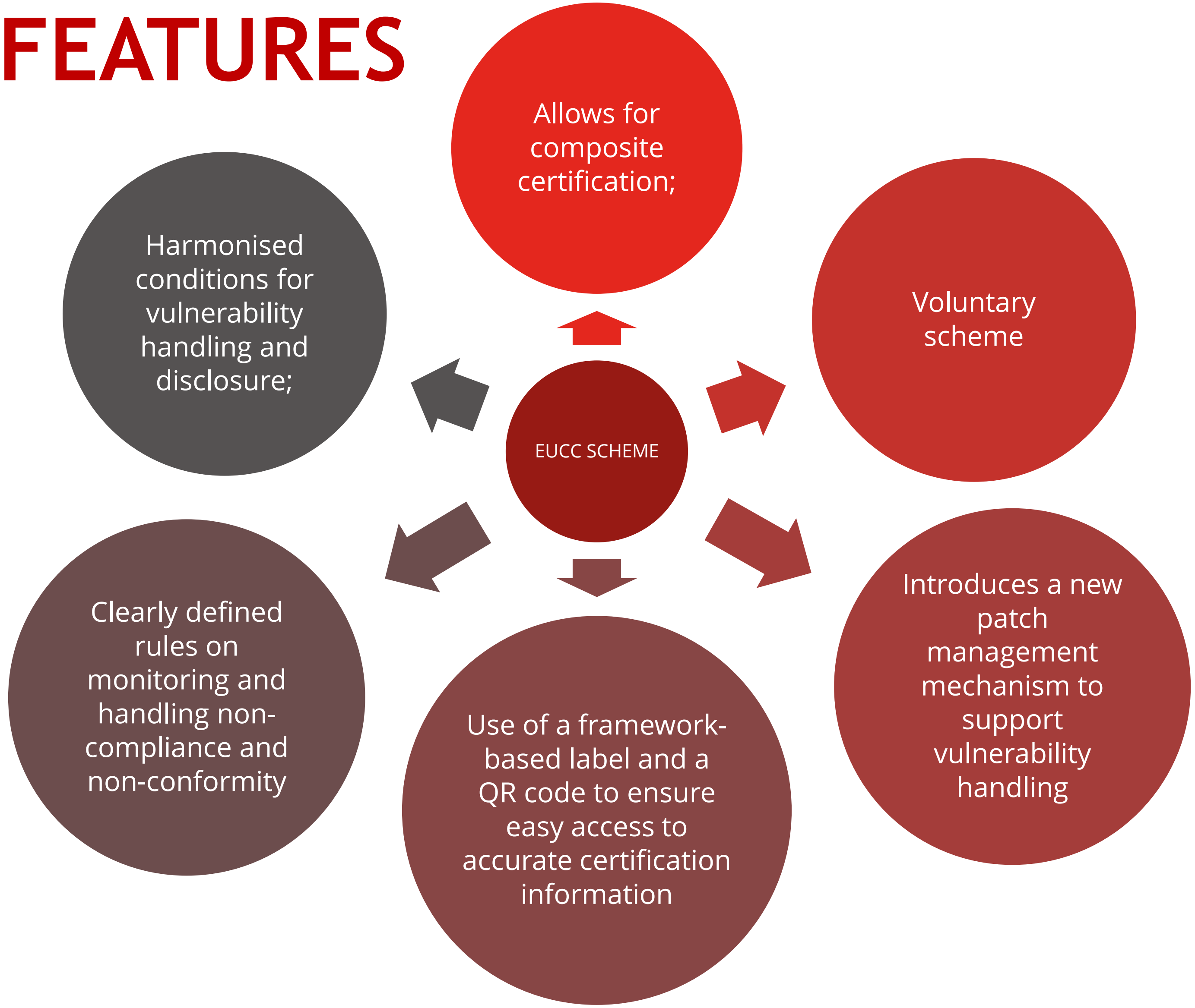
CYBERSECURITY CERTIFICATION
INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

Candidate scheme for EU CSA

Successor to SOG IS MRA

Comprises 32 members from Industry & Accreditation bodies

EUCC KEY FEATURES



EUCC SCHEME

Allows for composite certification;

Voluntary scheme

Introduces a new patch management mechanism to support vulnerability handling

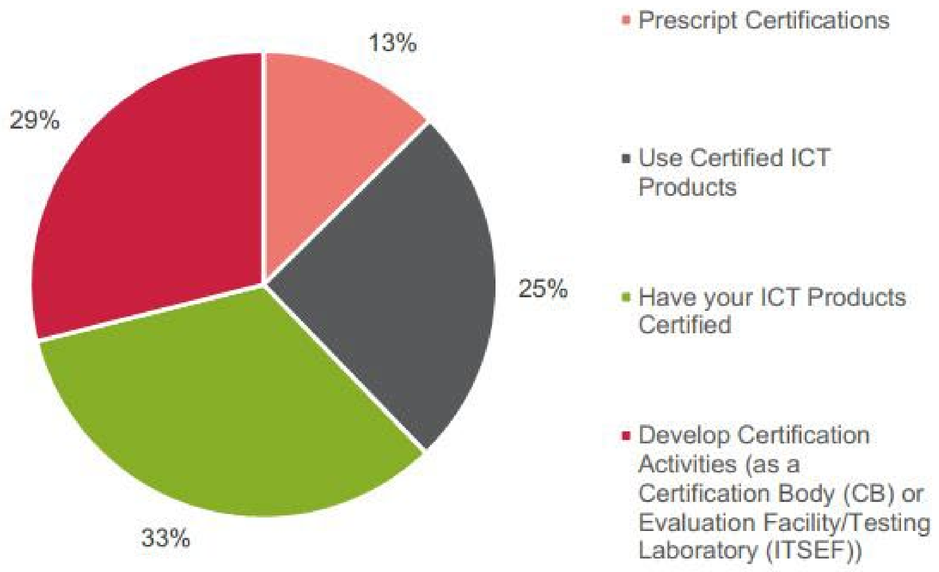
Use of a framework-based label and a QR code to ensure easy access to accurate certification information

Clearly defined rules on monitoring and handling non-compliance and non-conformity

Harmonised conditions for vulnerability handling and disclosure;

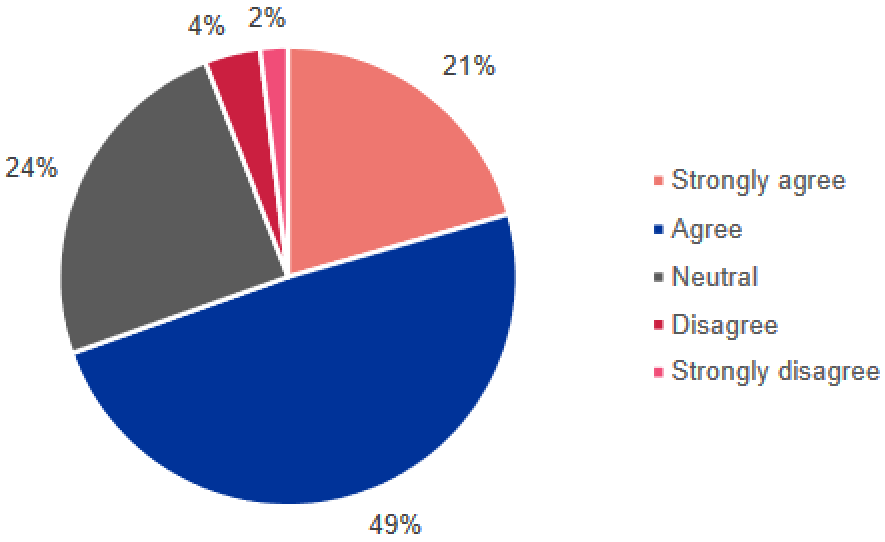
Intention to use the EUCC scheme

82% of the participants (61% outside EU/EEA), for the following usages (in line with the profile of participants):



All MS participants (100%) indicated they intend to use the EUCC scheme.

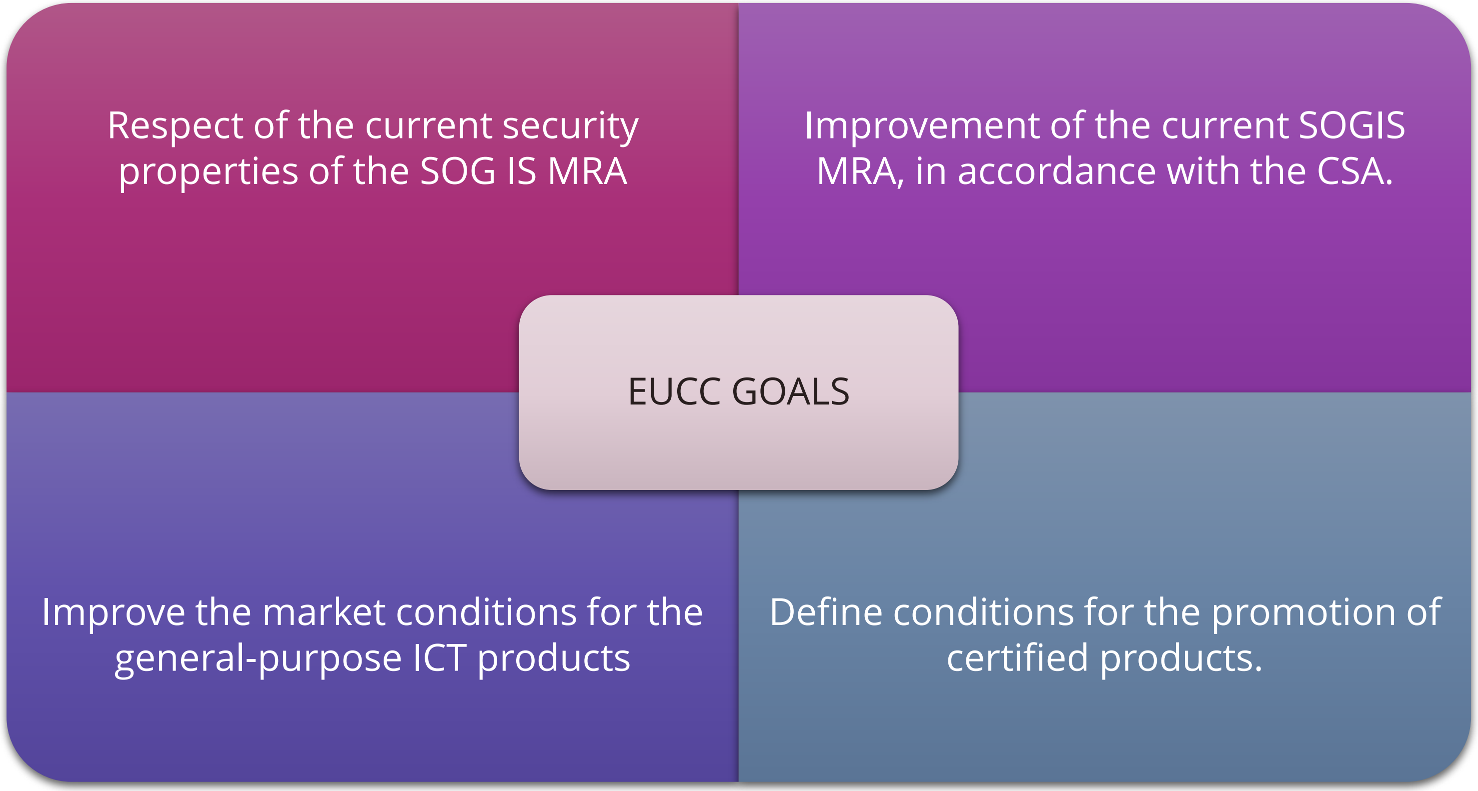
Positive impact of improvements brought by the scheme



On maintenance of the certificates, monitoring and handling of non-compliances, non-conformities and vulnerabilities, patch management)

The important neutral percentage can well be associated with the ambitious expectation level associated with the improvements, all not developed/experimented yet, and their potential impacts (delays and technical requirements) on the existing certification practices.

EUCC SCHEME **GOALS**



EUCC GOALS

Respect of the current security properties of the SOG IS MRA

Improvement of the current SOGIS MRA, in accordance with the CSA.

Improve the market conditions for the general-purpose ICT products

Define conditions for the promotion of certified products.

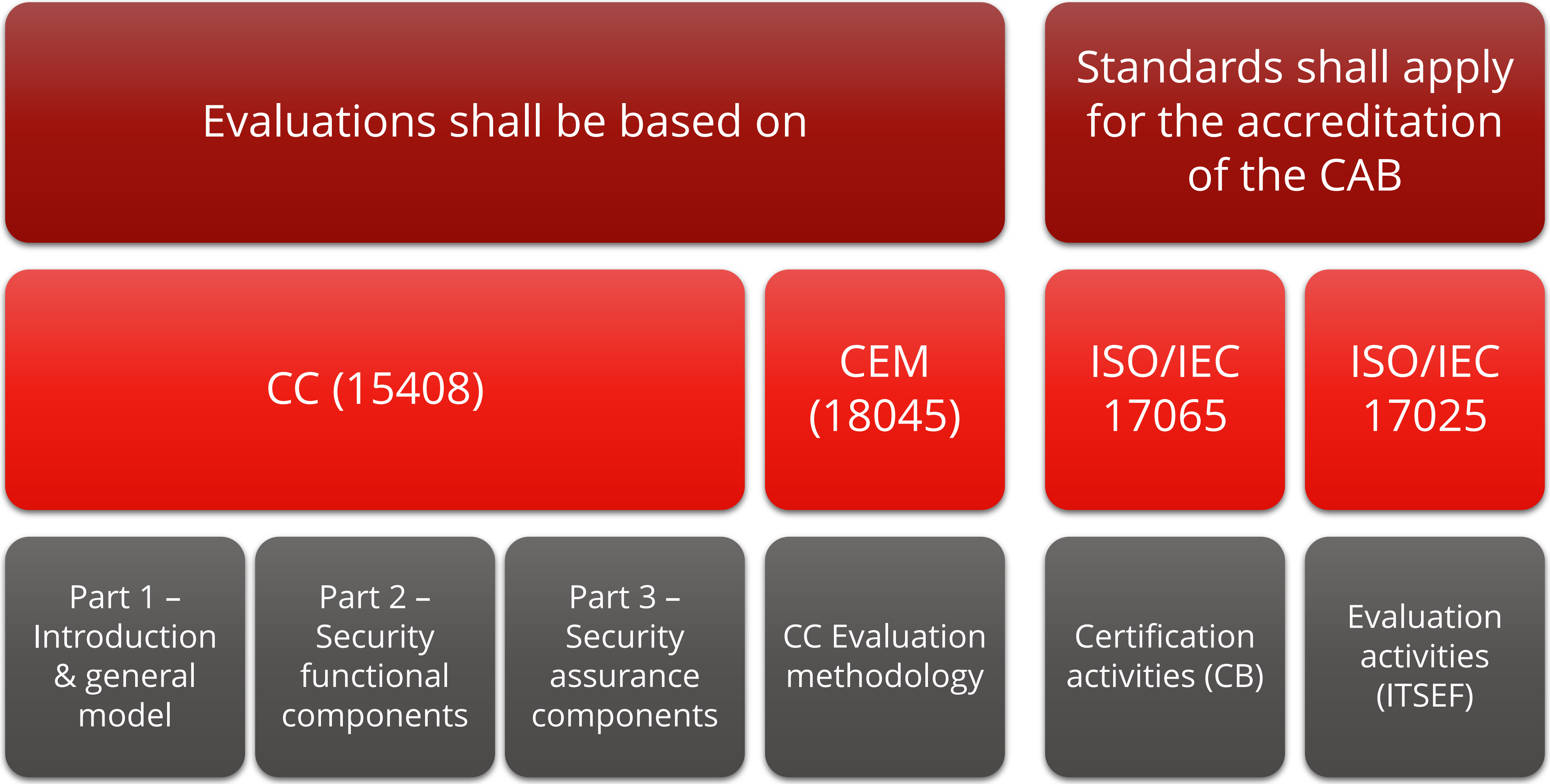
WHAT IS CC ? EUCC CANDIDATE SCHEME HIGHLIGHTS

ITSEF = CAB-E
CB = CAB-R

- The Common Criteria based European cybersecurity certification scheme (the EUCC scheme) covers the certification of ICT products.
- **The EUCC scheme can serve the certification of many different types of generic and sector specific ICT products.**
- **It is more of a horizontal scheme. Users of the scheme may establish Protection profiles to express their security requirements.**
- Certified Protection Profiles may also be defined as applicable or reference standards for specific stakeholders’ communities.

EVALUATION STANDARDS

The EUCC scheme is based on the CC and the CEM, with an additional set of supporting elements, further defined



Evaluations shall be based on

Standards shall apply for the accreditation of the CAB

CC (15408)

CEM (18045)

ISO/IEC 17065

ISO/IEC 17025

Part 1 – Introduction & general model

Part 2 – Security functional components

Part 3 – Security assurance components

CC Evaluation methodology

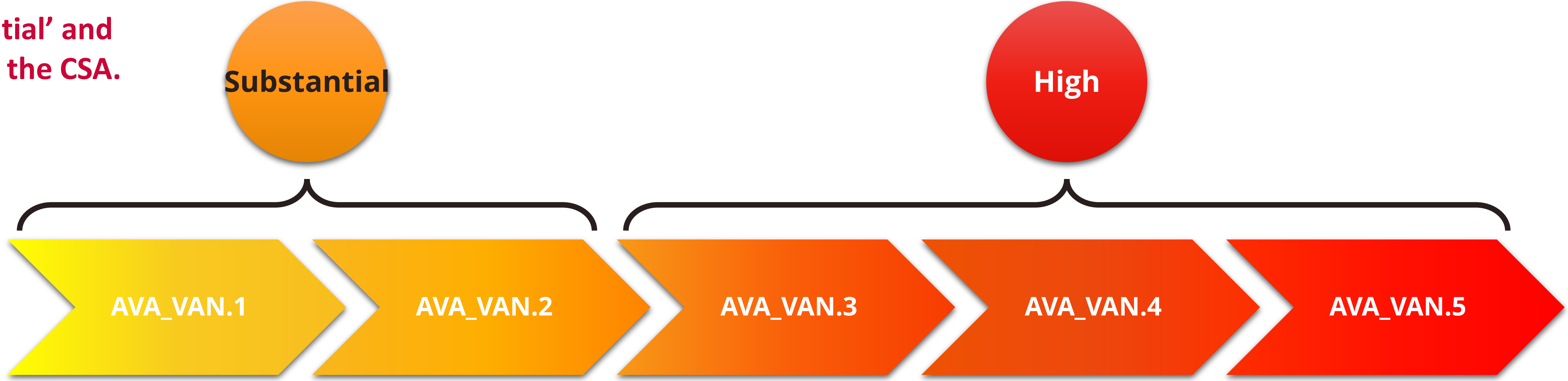
Certification activities (CB)

Evaluation activities (ITSEF)

ASSURANCE LEVELS

The EUCC scheme covers assurance levels 'substantial' and 'high' of the CSA.

The assignment to the assurance levels of the CSA shall be based on the use of the assurance components for vulnerability assessment defined in CC Part 3 as follows:



Unless duly justified by the CB, the dependencies of each assurance component for vulnerability assessment, as defined in the CC Part 3 shall be applied and all assurance components of the first evaluation assurance level (EAL) defined by the CC Part 3 that is associated to the selected AVA_VAN level shall be applied.

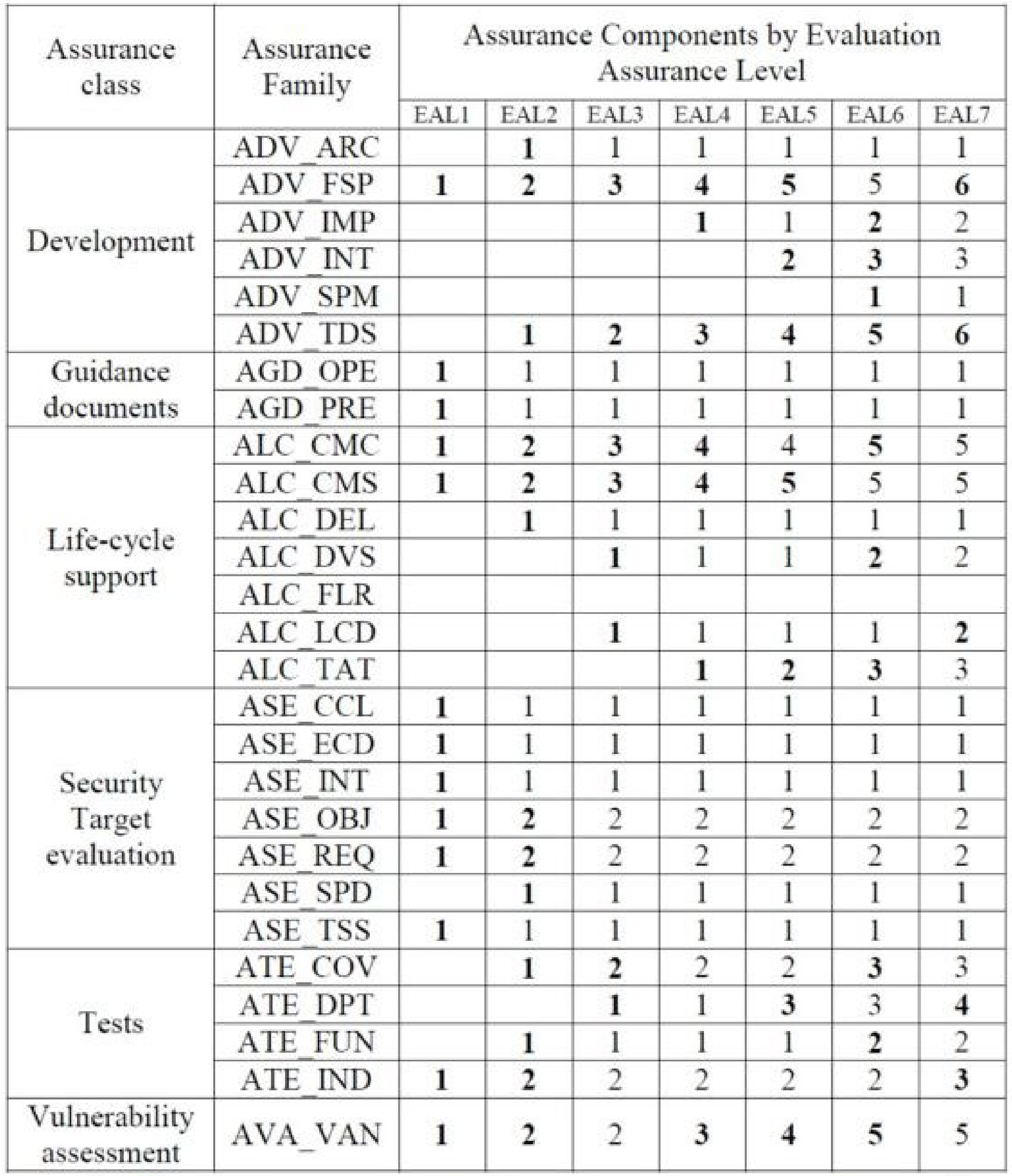
ASSURANCE LEVELS

The EUCC scheme covers assurance levels ‘substantial’ and ‘high’ of the CSA.

All dependencies, as defined in the CC Part 3, that apply to the selected AVA_VAN level shall be applied and included into the applicable Security Assurance Requirements for the evaluation.
Preferably, all assurance components of the evaluation assurance level (EAL) defined by the CC Part 3 that is associated to the selected AVA_VAN level shall be applied, in accordance with the associated table.

Where an AVA_VAN level is associated with multiple EALs, either EALs may be chosen.
The **choice of a lower EAL** level than the one(s) associated to the AVA_VAN level in the previous table may remain possible, under the conditions that:

- The chosen EAL shall **not be more than two (2) levels lower** than the lowest EAL associated to the AVA_VAN level;
- The resulting assurance level shall be treated as an augmentation of the chosen EAL as defined by the CC Part 3.



Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary (excerpt from CC Part 3)

ASSESSMENT TYPE

The scheme does not permit conformity self-assessments

Third-party Assessments

Self assessments

REQUIREMENTS APPLICABLE TO A CAB

CAB, including their testing laboratories, are subject to specific requirements in addition to their accreditation for the 'high' assurance level of certification

CB

CSA Annex.19

Required

- ❖ Accredited with the relevant standard, ISO/IEC 17065.

High

Required

- ❖ Authorized by NCCA to produce certificates at the assurance level 'high'

ITSEF

Substantial

- ❖ technical competence shall be assessed through the accreditation of the testing laboratory according to ISO/IEC 17025for evaluations according to ISO/IEC18045in conjunction with ISO/IEC15408

High

- ❖ have the necessary expertise and experience in performing the specific testing activities to determine the product's resistance against specific attacks assuming an attack potential of '<u>basic-enhanced</u> as described in the CC
- ❖ For the <u>technical domain</u> defined in the EUCC
  - ❖ Same things assuming an attack potential of either '<u>moderate</u>' or '<u>high</u>'
  - ❖ be able to demonstratethe specific technical competenceslisted by the related annexof the EUCC

QUIZ

- Which body is ISO 17025 is applicable for ?
- Conformity self assessments are used in EUCC. True or False?
- What standards are EUCC evaluations based on?
- EUCC is a horizontal scheme. True or false?

NOTIFICATION & FUNCTIONING OF CABS

Under this scheme, both certification bodies (CBs) and testing laboratories (ITSEFs) shall be assessed for authorisations to perform certification and evaluation at the assurance level ‘high’ of the CSA.

NOTIFICATION

For each CAB issuing certificates (designated as a certification body or CB) notified in accordance with Article 60.1 of the CSA, the notification shall include:

- the specified CSA assurance level (‘substantial’, or ‘high’);
- where the CSA assurance level is ‘high’, the AVA_VAN level up to which the CB can issue certificates, and where applicable, the technical domains for which certification is offered;
- where applicable, the list of the ITSEFs performing evaluations for the CB, including the AVA_VAN level up to which each ITSEF can evaluate, and where applicable, the technical domains for which evaluation is offered.

NOTIFICATION & FUNCTIONING OF CABS

Authorization

A NCCA shall, for the authorization of a CAB to carry out tasks under the EUCC scheme, proceed to the assessment of the approval performed by the CAB in compliance with the specific requirements described in Chapter 6 SPECIFIC REQUIREMENTS APPLICABLE TO A CAB of the internal testing laboratory of this CAB and, in cases where testing is performed by a subcontractor, of the external testing laboratory.

This assessment may include, for each ITSEF:

- **conducting structured interviews to determine that the ITSEF and its personnel have the necessary expertise and experience in the relevant activities;**
- **reviewing evidences of two pilot evaluations performed by the ITSEF as part of the approval procedure of the CAB and evaluating their performance.**

NOTIFICATION & FUNCTIONING OF CABS

When establishing a request for certification under this scheme at the assurance level ‘high’ of the CSA, a manufacturer or provider may consult any ITSEF associated to an authorised CAB for availability and estimation of resources and costs for the evaluation, and may contract directly to one or more of these ITSEFs. However, the following determinations apply:

- **it shall only establish a contract with an ITSEF that has been properly notified with the CB at the relevant level;**
- **the ITSEF shall inform the CB of the resources (man-days) allocated for the evaluation;**
- **the CB remains the main responsible body for the resulting certificate.**

NOTIFICATION & FUNCTIONING OF CABS

Subcontracting & use of 3rd party facilities

An ITSEF deemed competent for a Technical Domain may only subcontract its work within the technical domain under the following conditions:

Activities shall only be taken in charge by an ITSEF competent for the considered technical domain;

- Further subcontracting shall only be possible with the consent of the CB, the NCCA and the manufacturer or provider of the ICT product;

The activities shall be performed under the full control and responsibility of the subcontracting ITSEF;

- Only partial subcontracting of AVA_VAN activities shall be allowed

EVALUATION CRITERIA & METHODS

The selection of appropriate functional (SFR) and assurance (SAR) requirements from the CC may allow to cover a large variety of security objectives of Article 51 of the CSA.

	Security objectives defined by Article 51	Candidate class/families and/or SAR from the CC of SFR
a	Protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process;	-SFR Class FCO: Communication -SFR Class FCS: Cryptographic support, including SFR Family FCS_COP: Cryptographic operation -SFR Class FDP: User data protection, including SFR Family FDP_UCT: Inter-TSF user data confidentiality transfer protection
B	Protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process;	-SFR Class FDP: User data protection, including SFR Family FDP_SDI: Stored Data Integrity and SFR Family FDP_UIT: Inter-TSF user data integrity transfer protection -SFR Family FCS_COP: Cryptographic operation
c	Authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;	-SFR Class FDP: User data protection, including SFR Family FDP_SDI: Stored Data Integrity and SFR Family FDP_UIT: Inter-TSF user data integrity transfer protection -SFR Family FCS_COP: Cryptographic operation -SFR Family FMT_MSA Management of security attributes -SFR Family FMT_SMF Specification of Management Functions

EVALUATION CRITERIA & METHODS 2

	Security objectives defined by Article 51	Candidate class/families and/or SAR from the CC of SFR
d	Identify and document known dependencies and vulnerabilities;	-SFR Class FDP: User data protection -SAR Family ALC_FLR: Flaw remediation -SAR Family ALC_CMS: CM Scope -SAR Class ASE: Security Target
e	Record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;	-SFR Class FAU: Security audit, including SFR Family FAU_GEN: Security audit data generation -SFR Class FTA: TOE access
f	Make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;	-SFR Class FAU: Security audit, including SFR Family FAU_SAR: Security audit data review -SFR Family FMT_MSA Management of security attributes -SFR Family FMT_SMF Specification of Management Functions
g	Verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;	-SAR Class AVA: Vulnerability assessment, including SAR Family AVA_VAN: Vulnerability analysis
h	Restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;	-SFR Class FPT: Protection of the TSF, including SFR Family FPT_RCV: Trusted recovery

EVALUATION CRITERIA & METHODS 3

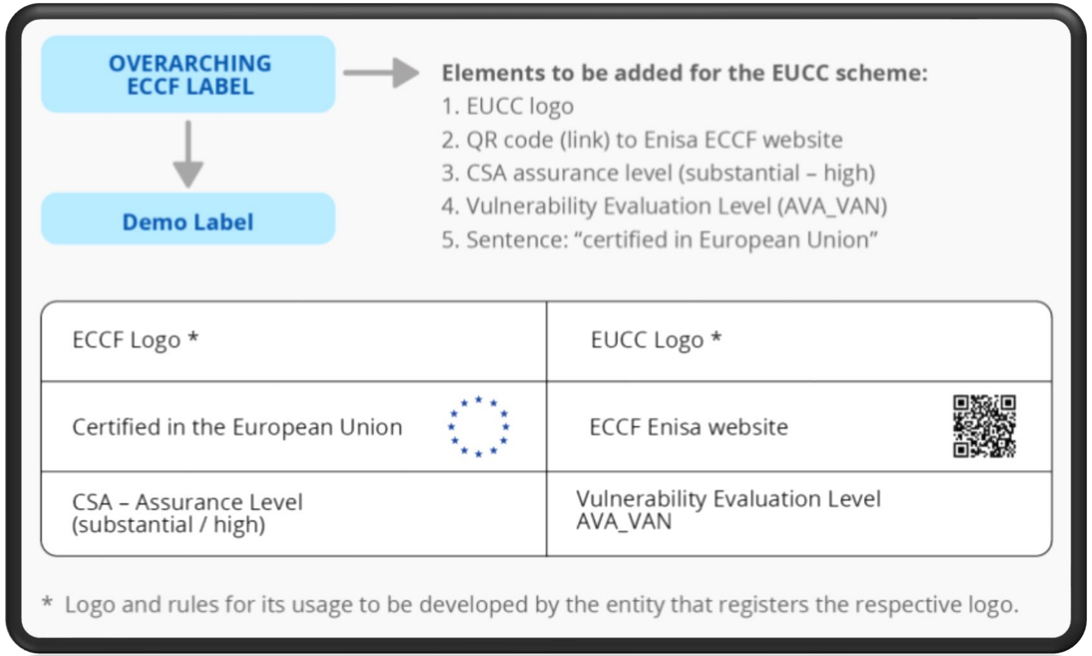
	Security objectives defined by Article 51	Candidate class/families and/or SAR from the CC of SFR
i	ICT products, ICT services and ICT processes are secure by default and by design;	-SAR Family ALC_TAT: Tools and techniques -SAR Family ADV_ARC: Security Architecture -SAR Family ADV_TDS: TOE Design -SAR Family ASE_SPD: Security problem definition
j	ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.	-SAR Class AVA: Vulnerability assessment -SAR Family ALC_FLR: Flaw remediation

QUIZ

- What AVA_VANs are linked to assurance level “High” ?
- List 2 conditions under which an ITSEF can subcontract to a 3rd party.
- Under EUCC, an ITSEF can issue a certificate; True or False?
- List 1 point that the Notification for CAB issuing certificates should include.
- Mention one activity to be carried out by the NCCA when assessing a CAB

NECESSARY INFORMATION FOR CERTIFICATION & MARKS AND LABEL

- The necessary information for certification shall include relevant evidence for evaluation. It may include previous evaluation results.
- It is foreseen that a label is associated with the European Cybersecurity Certification Framework, and specifically implemented for each scheme, including the EUCC scheme.



Elements to be added for the EUCC scheme:

1. EUCC logo
2. QR code (link) to Enisa ECCF website
3. CSA assurance level (substantial – high)
4. Vulnerability Evaluation Level (AVA_VAN)
5. Sentence: "certified in European Union"

ECCF Logo *	EUCC Logo *
Certified in the European Union	ECCF Enisa website
CSA – Assurance Level (substantial / high)	Vulnerability Evaluation Level AVA_VAN

* Logo and rules for its usage to be developed by the entity that registers the respective logo.

MONITORING COMPLIANCE

Monitoring rules are based on potential cases of non-compliances and non-conformity and shall consist of prevention, and detection measures

Monitoring shall allow where possible to avoid and where needed to detect the following general cases of non-compliance:

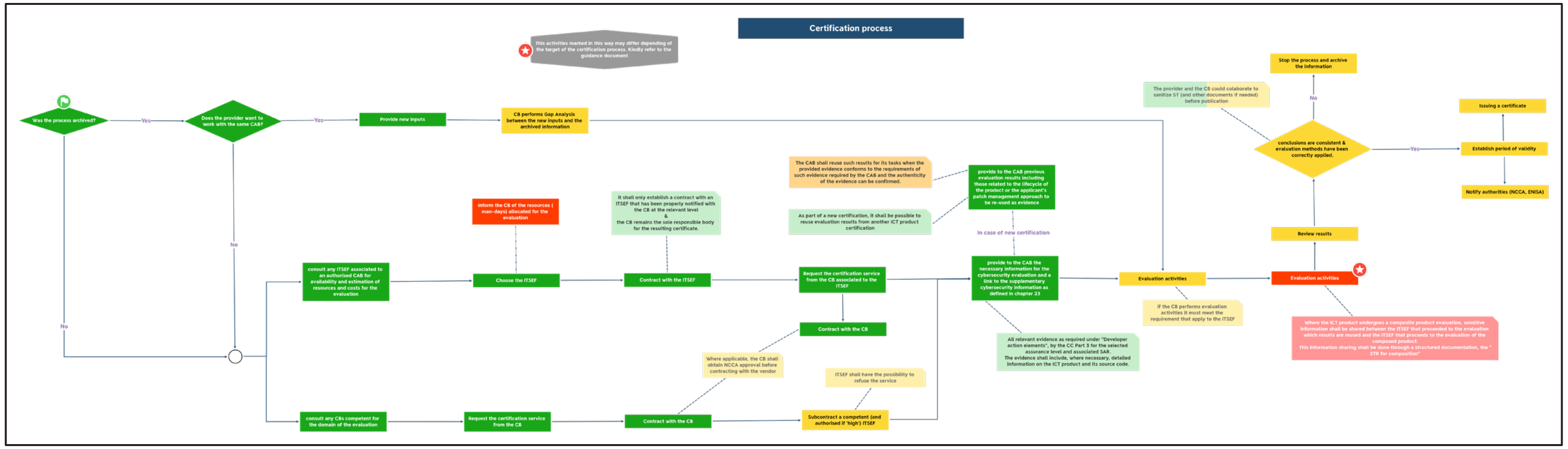
- a non-compliance in the application by a manufacturer or provider of the rules and obligations related to a certificate issued on their ICT product;
- a non-compliance in the conditions under which the certification takes place and that are not related to the individual ICT product;
- a non-conformity of a certified ICT product with its security requirements, which includes and is not limited to a:
    - change in the threat environment after the issuance of the certificate, which has an adverse impact on the security of the certified ICT product;
    - vulnerability identified and related to the certified ICT product, that has an adverse impact on the security of the certified ICT product.

The general monitoring of the certified ICT products shall be based on sampling, using generic criteria such as product type, evaluation level, manufacturer or provider, CAB and any relevant information brought to the knowledge of the NCCA (e.g. complaints, security events). The NCCAs on their respective territories and in cooperation with other relevant market surveillance authorities, shall sample annually a minimum of 5% of the products and at least one product per annum which received certificates in the previous year.

CONDITIONS FOR ISSUING A CERTIFICATE - A CERTIFICATION PROCESS OVERVIEW

Legend

- 🟨 CB
- 🟥 ITSEF
- 🟧 CAB
- 🟦 NCCA
- 🟩 Provider
- 🟪 ECCG
- 🟦 Peer Assessment Team
- 🟩 ENISA
- □ Generic actions
- ■ To Define
- Start point of the process
- ◆ Decision
- Process Or Action



Certification process

This activities marked in this way may differ depending of the target of the certification process. Kindly refer to the guidance document

Was the process archived?

Yes

Does the provider want to work with the same CAB?

Yes

Provide new inputs

CB performs Gap Analysis between the new inputs and the archived information

No

No

consult any ITSEF associated to an authorised CAB for availability and estimation of resources and costs for the evaluation

inform the CB of the resources (man-days) allocated for the evaluation

Choose the ITSEF

It shall only establish a contract with an ITSEF that has been properly notified with the CB at the relevant level
&
the CB remains the sole responsible body for the resulting certificate.

Contract with the ITSEF

Request the certification service from the CB associated to the ITSEF

Contract with the CB

consult any CBs competent for the domain of the evaluation

Request the certification service from the CB

Contract with the CB

Where applicable, the CB shall obtain NCCA approval before contracting with the vendor

ITSEF shall have the possibility to refuse the service

Subcontract a competent (and authorised if 'high') ITSEF

The CAB shall reuse such results for its tasks when the provided evidence conforms to the requirements of such evidence required by the CAB and the authenticity of the evidence can be confirmed.

As part of a new certification, it shall be possible to reuse evaluation results from another ICT product certification

provide to the CAB previous evaluation results including those related to the lifecycle of the product or the applicant's patch management approach to be re-used as evidence

In case of new certification

provide to the CAB the necessary information for the cybersecurity evaluation and a link to the supplementary cybersecurity information as defined in chapter 23

All relevant evidence as required under "Developer action elements", by the CC Part 3 for the selected assurance level and associated SAR.
The evidence shall include, where necessary, detailed information on the ICT product and its source code.

Evaluation activities

if the CB performs evaluation activities it must meet the requirement that apply to the ITSEF

Evaluation activities

Where the ICT product undergoes a composite product evaluation, sensitive information shall be shared between the ITSEF that proceeded to the evaluation which results are reused and the ITSEF that proceeds to the evaluation of the composed product.
This information sharing shall be done through a structured documentation, the " ETR for composition"

Review results

conclusions are consistent & evaluation methods have been correctly applied.

No

Stop the process and archive the information

The provider and the CB could colaborate to sanitize ST (and other documents if needed) before publication

Yes

Establish period of validity

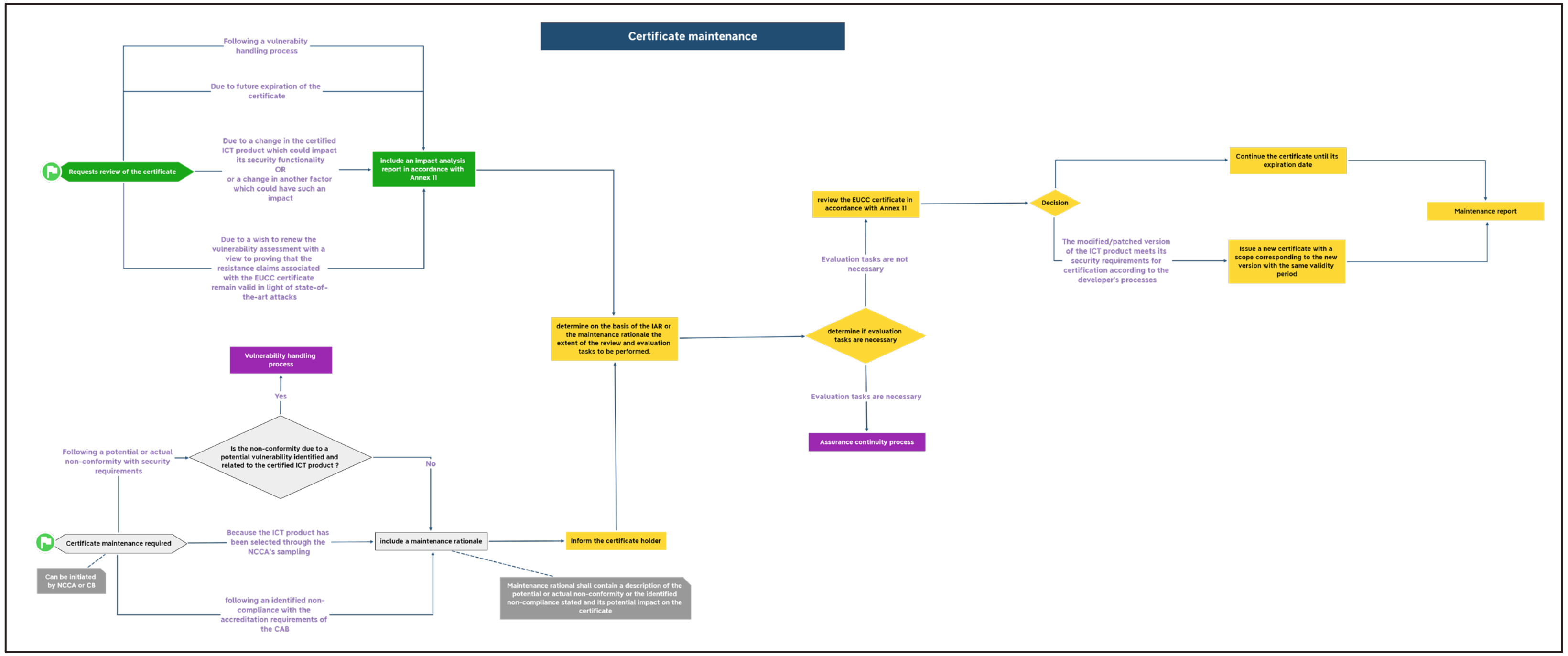
Issuing a certificate

Notify authorities (NCCA, ENISA)

CONDITIONS FOR MAINTAINING, CONTINUING AND RENEWING CERTIFICATE- A MAINTENANCE PROCESS OVERVIEW

Legend

- CB
- ITSEF
- CAB
- NCCA
- Provider
- ECCG
- Peer Assessment Team
- ENISA
- Generic actions
- To Define
- Start point of the process
- Decision
- Process Or Action



Certificate maintenance

Requests review of the certificate

Following a vulnerabity handling process

Due to future expiration of the certificate

Due to a change in the certified ICT product which could impact its security functionality
OR
or a change in another factor which could have such an impact

Due to a wish to renew the vulnerability assessment with a view to proving that the resistance claims associated with the EUCC certificate remain valid in light of state-of-the-art attacks

include an impact analysis report in accordance with Annex 11

determine on the basis of the IAR or the maintenance rationale the extent of the review and evaluation tasks to be performed.

determine if evaluation tasks are necessary

Evaluation tasks are not necessary

review the EUCC certificate in accordance with Annex 11

Evaluation tasks are necessary

Assurance continuity process

Decision

Continue the certificate until its expiration date

The modified/patched version of the ICT product meets its security requirements for certification according to the developer's processes

Issue a new certificate with a scope corresponding to the new version with the same validity period

Maintenance report

Vulnerability handling process

Yes

Is the non-conformity due to a potential vulnerability identified and related to the certified ICT product ?

No

Following a potential or actual non-conformity with security requirements

Certificate maintenance required

Can be initiated by NCCA or CB

Because the ICT product has been selected through the NCCA's sampling

following an identified non-compliance with the accreditation requirements of the CAB

include a maintenance rationale

Inform the certificate holder

Maintenance rational shall contain a description of the potential or actual non-conformity or the identified non-compliance stated and its potential impact on the certificate

CASES AND DECISIONS TO BE TAKEN BY CB

CASES	NOMINAL DECISIONS
The same ICT product still meets its security requirements for certification.	Continue the certificate until its expiration date.
The expiration date of the certificate has been reached and no request for maintenance has been submitted.	Archive the certificate.
New evaluation tasks including vulnerability testing were performed on the same version of the ICT product and are successful.	Renew the certificate with potentially an extended validity period.
The modified/patched version of the ICT product meets its security requirements for certification according to the developer's processes and no new evaluation tasks have been deemed necessary.	Issue a new certificate with a scope corresponding to the new version with the same validity period.
New evaluation tasks including vulnerability testing were performed on a modified/patched version of the ICT product and are successful.	Issue new certificate with an extended scope corresponding to the modified version and with an extended validity period.
Necessary evaluation tasks were performed and identify the same version of ICT product does not meet all applicable requirements, and a reduction of scope of the certificate would allow to maintain the security level.	Issue a new certificate with a reduced scope with possibly an extended validity period.

CASES AND DECISIONS TO BE TAKEN BY CB 2

CASES	NOMINAL DECISIONS
Necessary evaluation tasks were performed and identify the same version of ICT product does not meet all applicable requirements, and a reduction of the assurance level would allow to maintain a certificate.	Issue a new certificate with a reduced assurance level with possibly an extended validity period
Necessary evaluation tasks were performed and identify the same version of ICT product does not meet all applicable requirements, and action is possible to maintain the certificate at the same level and with the same scope, though not immediately, or improper use of the certificate or of the mark is not immediately solved by suitable retractions and appropriate corrective actions by the manufacturer or provider.	Suspend the certificate pending remedial action by the manufacturer or provider of the ICT product
Necessary evaluation tasks were not performed	Withdraw the certificate
Necessary evaluation tasks were performed and identify the same version of ICT product does not meet all applicable requirements.	Withdraw the certificate
Necessary maintenance activities were not performed in due time.	Withdraw the certificate

QUIZ

- **Describe one condition under which a CB is allowed to issue a new certificate.**
- **Describe the condition in certificate maintenance when a certificate is:**
  a. withdrawn b. continued and c. issued
- **List one conditions under which maintenance may be initiated by the certificate owner.**
- **What happens to a certificate that has reached expiry and no request has been made for renewal?**
- **What is the exceptional case that permits a certificate to remain "suspended" for more than 3 months?**

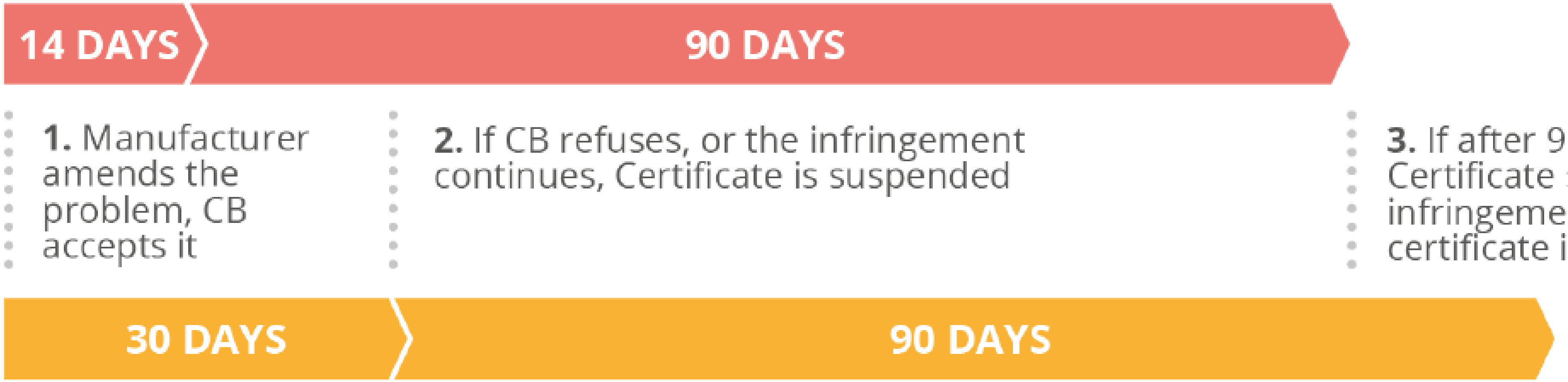
NON-COMPLIANCE RULES

Consequences vary according to the assessed non-conformities and non-compliances. Certificate suspension is introduced as to allow the necessary changes and/or controls to occur.

For confirmed deviations or irregularities associated to a non-compliance in the application by a manufacturer or provider of the requirements related to a certificate issued on their ICT product, the following consequences shall be in the general case:

- the CAB issuing the certificate shall request the manufacturer or provider for assertions and amendments to be provided within the time frame of 14 days/30 days for certificates at the assurance level 'high' /'substantial' of the CSA, in order to restore compliance;
- the CAB shall review the provided assertions and amendments and accept or refuse them; the decision shall be sent to the manufacturer or provider
- continued infringements of such obligations shall trigger certificate suspension of the certificate for the ICT product and temporal suspension of certificate applications to the CAB by the manufacturer or provider, with an information from the CAB to the NCCA.
- when the handling is refused, or the suspension reaches a 90-day period the certificate shall be withdrawn.

NON-COMPLIANCE RULES: TIMELINES



14 DAYS

90 DAYS

1. Manufacturer amends the problem, CB accepts it

2. If CB refuses, or the infringement continues, Certificate is suspended

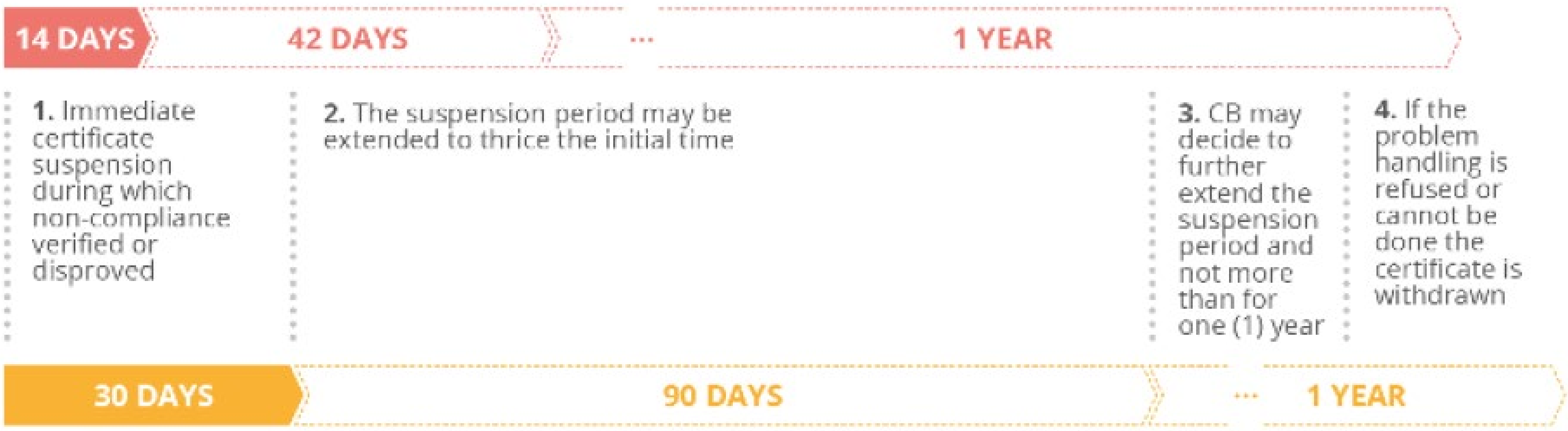
3. If after 90 days of Certificate suspension the infringement still persists, certificate is withdrawn

30 DAYS

90 DAYS

Timelines of non-compliance handling in the application of the requirements related to a certificate.

NON-COMPLIANCE RULES: TIMELINES



1. Immediate certificate suspension during which non-compliance verified or disproved

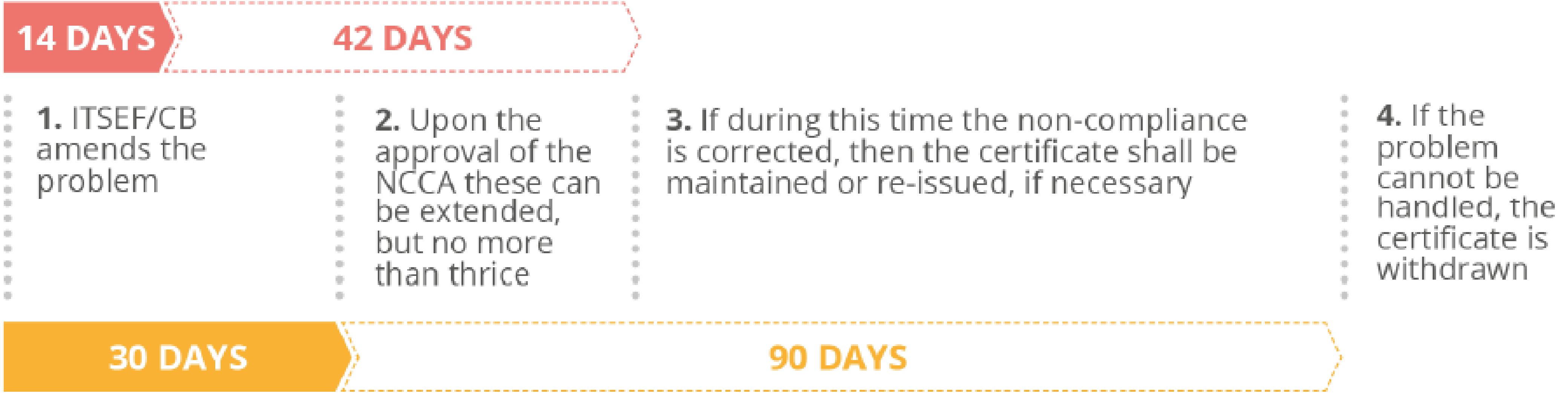
2. The suspension period may be extended to thrice the initial time

3. CB may decide to further extend the suspension period and not more than for one (1) year

4. If the problem handling is refused or cannot be done the certificate is withdrawn

Timelines of non-compliance handling in case of a confirmed deviation from the requirements on the certificate holder’s obligations towards maintaining the certificate validity, or towards informing the appropriate authorities or bodies of any subsequently detected vulnerabilities

NON-COMPLIANCE RULES: TIMELINES



1. ITSEF/CB amends the problem

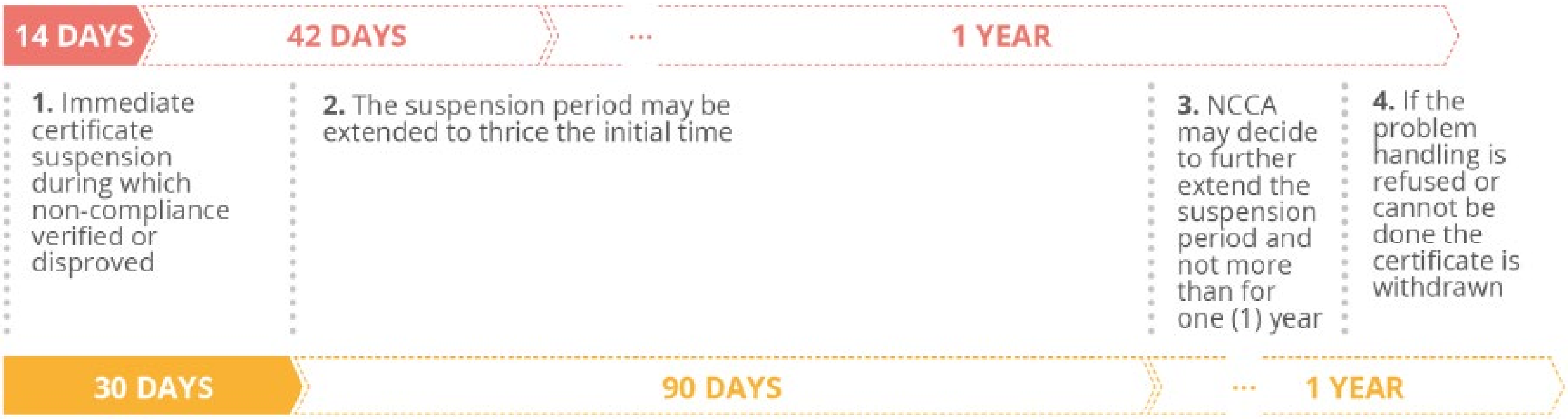
2. Upon the approval of the NCCA these can be extended, but no more than thrice

3. If during this time the non-compliance is corrected, then the certificate shall be maintained or re-issued, if necessary

4. If the problem cannot be handled, the certificate is withdrawn

Timelines of non-compliance handling in the conditions under which the certification takes place.

NON-COMPLIANCE RULES: TIMELINES



1. Immediate certificate suspension during which non-compliance verified or disproved

2. The suspension period may be extended to thrice the initial time

3. NCCA may decide to further extend the suspension period and not more than for one (1) year

4. If the problem handling is refused or cannot be done the certificate is withdrawn

Timelines of non-compliance handling in the conditions under which the certification takes place and where impacts are confirmed to affect the validity of a certificate

VULNERABILITY HANDLING RULES

Previously undetected vulnerability shall be reported and handled in accordance with the general rules of ISO/IEC 30111 and ISO/IEC 29147, adapted for this scheme with the additional possibility of patch management

Manufacturers or providers of ICT products shall use the general steps of ISO/IEC 30111 for vulnerability handling: preparation, receipt, verification, remediation development, release, post Release.

The EUCC Scheme vulnerability handling and disclosure processes are based on the ISO standards ISO/IEC 30111 and ISO/IEC 29417. However, as these standards do not contain any assurance on whether the developed and deployed remediation does not introduce new vulnerabilities, and do not define any tasks for a third-party assessment body and its methodology, additional information was provided to cover these gaps.

VULNERABILITY HANDLING RULES – PROCESS OVERVIEW

Legend

CB

ITSEF

CAB

NCCA

Provider

ECCG

Peer Assessment Team

ENISA

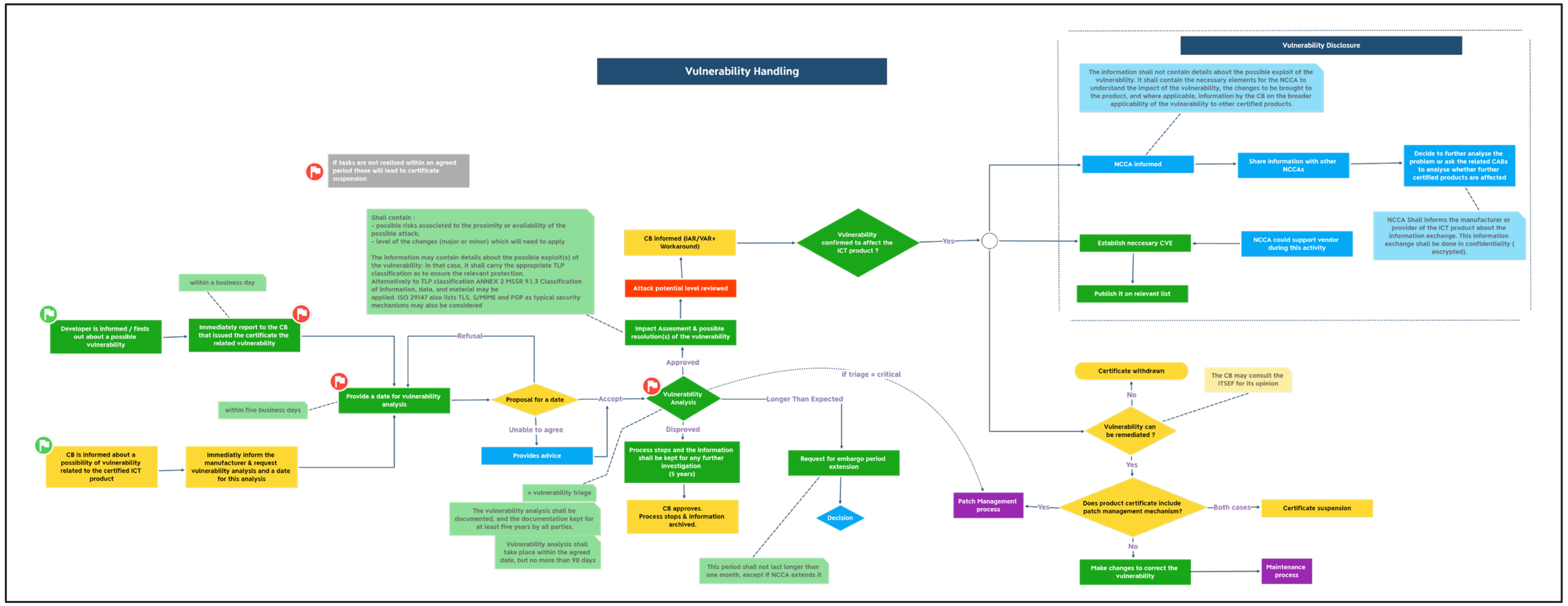
Generic actions

To Define

Start point of the process

Decision

Process Or Action



Vulnerability Handling

If tasks are not realised within an agreed period these will lead to certificate suspension

Developer is informed / finds out about a possible vulnerability

within a business day

Immediately report to the CB that issued the certificate the related vulnerability

CB is informed about a possibility of vulnerability related to the certified ICT product

Immediatly inform the manufacturer & request vulnerability analysis and a date for this analysis

within five business days

Provide a date for vulnerability analysis

Refusal

Proposal for a date

Unable to agree

Provides advice

Accept

Shall contain :
- possible risks associated to the proximity or availability of the possible attack;
- level of the changes (major or minor) which will need to apply

The information may contain details about the possible exploit(s) of the vulnerability: in that case, it shall carry the appropriate TLP classification as to ensure the relevant protection.
Alternatively to TLP classification ANNEX 2 MSSR 9.1.3 Classification of information, data, and material may be applied. ISO 29147 also lists TLS, S/MIME and PGP as typical security mechanisms may also be considered

Vulnerability Analysis

+ vulnerability triage

The vulnerability analysis shall be documented, and the documentation kept for at least five years by all parties.

Vulnerability analysis shall take place within the agreed date, but no more than 90 days

Approved

Impact Assesment & possible resolution(s) of the vulnerability

Attack potential level reviewed

CB informed (IAR/VAR+ Workaround)

Disproved

Process stops and the information shall be kept for any further investigation (5 years)

CB approves. Process stops & information archived.

Longer Than Expected

Request for embargo period extension

Decision

This period shall not last longer than one month, except if NCCA extends it

if triage = critical

Vulnerability confirmed to affect the ICT product ?

Yes

Vulnerability Disclosure

The information shall not contain details about the possible exploit of the vulnerability. It shall contain the necessary elements for the NCCA to understand the impact of the vulnerability, the changes to be brought to the product, and where applicable, information by the CB on the broader applicability of the vulnerability to other certified products.

NCCA informed

Share information with other NCCAs

Decide to further analyse the problem or ask the related CABs to analyse whether further certified products are affected

NCCA Shall informs the manufacturer or provider of the ICT product about the information exchange. This information exchange shall be done in confidentiality (encrypted).

Establish neccesary CVE

NCCA could support vendor during this activity

Publish it on relevant list

Certificate withdrawn

No

The CB may consult the ITSEF for its opinion

Vulnerability can be remediated ?

Yes

Does product certificate include patch management mechanism?

Yes

Patch Management process

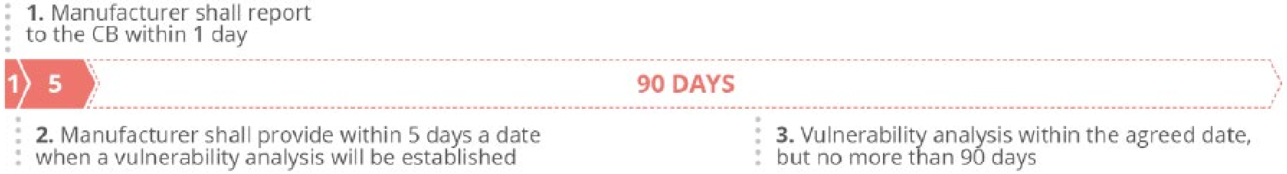
Both cases

Certificate suspension

No

Make changes to correct the vulnerability

Maintenance process



1. Manufacturer shall report to the CB within 1 day

2. Manufacturer shall provide within 5 days a date when a vulnerability analysis will be established

3. Vulnerability analysis within the agreed date, but no more than 90 days

Timeline of the general vulnerability handling

PATCH MANAGEMENT

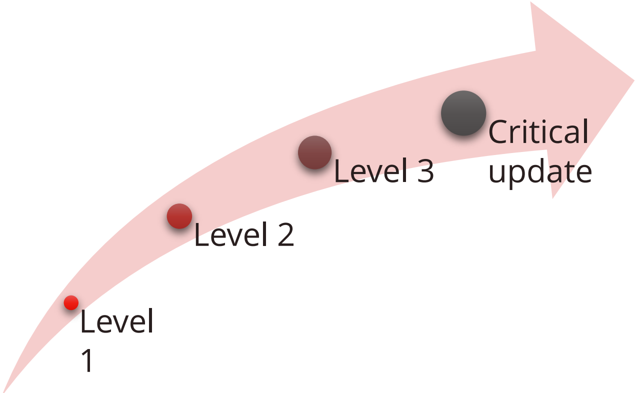
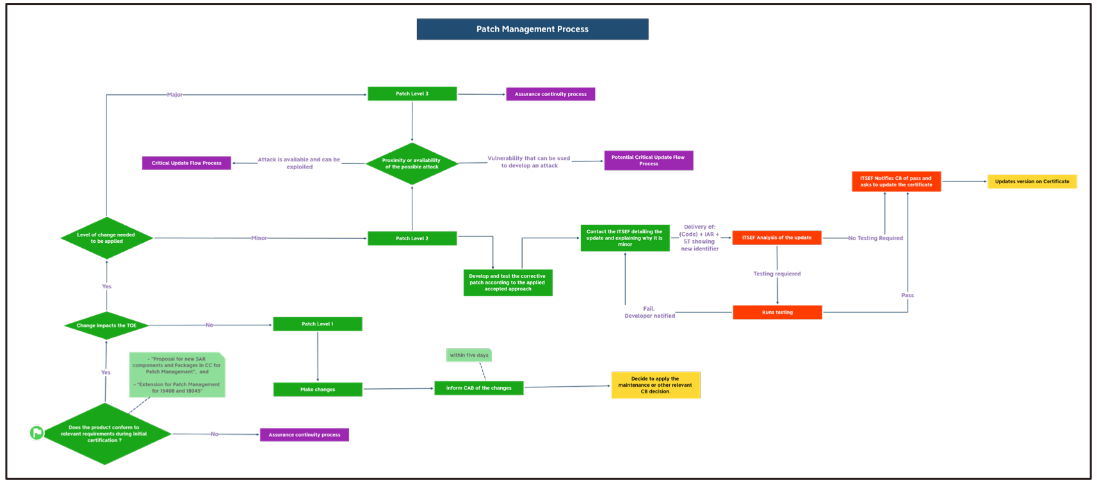


Table : Applicable patch levels

Proximity or availability of the possible attack	Level of change needed to be applied	Patch levels applicable
Attack is available and can be exploited (exploitable vulnerability)	Outside of the TOE	Level 1
	Minor	Critical Update Flow/Level 2
	Major	Critical Update Flow/Level 3
Vulnerability that can be used to develop an attack (exploitable or potential vulnerability)	Outside of the TOE	Level 1
	Minor	Level 2 with potentially Critical Update Flow
	Major	Level 3 with potentially Critical Update Flow
Vulnerability where an attack is not likely or cannot be used for development of an attack potential or residual vulnerability)	Outside of the TOE	Level 1
	Minor	Level 2
	Major	Level 3

Patch management is an annexe of the EUCC. This annex shall be for trial use. The period of the trial use should be of 2 years, but the maintenance organisation of the scheme may propose to reduce this period, be significant progress in its global adoption acknowledged earlier.

A product may include a patch management mechanism **assessed within its certification**. The content of this Annex are supplementing the content of Annex 11, ASSURANCE CONTINUITY. For a certified ICT product, either approaches can be applied, but where the patch management approach has been selected, several requirements shall apply.


Patch Management Process
Major
Patch Level 3
Assurance continuity process
Critical Update Flow Process
Attack is available and can be exploited
Proximity or availability of the possible attack
Vulnerability that can be used to develop an attack
Potential Critical Update Flow Process
ITSEF Notifies CB of pass and asks to update the certificate
Updates version on Certificate
Level of change needed to be applied
Minor
Patch Level 2
Contact the ITSEF detailing the update and explaining why it is minor
Delivery of: (Code) + IAR + ST showing new identifier
ITSEF Analysis of the update
No Testing Required
Yes
Develop and test the corrective patch according to the applied accepted approach
Testing requiered
Pass
Fail. Developer notified
Runs testing
Change impacts the TOE
No
Patch Level 1
Yes
- "Proposal for new SAR components and Packages in CC for Patch Management", and
- "Extension for Patch Management for 15408 and 18045"
within five days
Make changes
inform CAB of the changes
Decide to apply the maintenance or other relevant CB decision.
Does the product conform to relevant requirements during initial certification ?
No
Assurance continuity process

ASSURANCE CONTINUITY

The purpose of Assurance Continuity is to enable developers to support the maintenance activities related to ICT certified products, as defined in Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES, and where applicable, to vulnerability handling, as defined in Chapter 14, VULNERABILTY HANDLING.

Legend

CB

ITSEF

CAB

NCCA

Provider

ECCG

Peer Assessment Team

ENISA

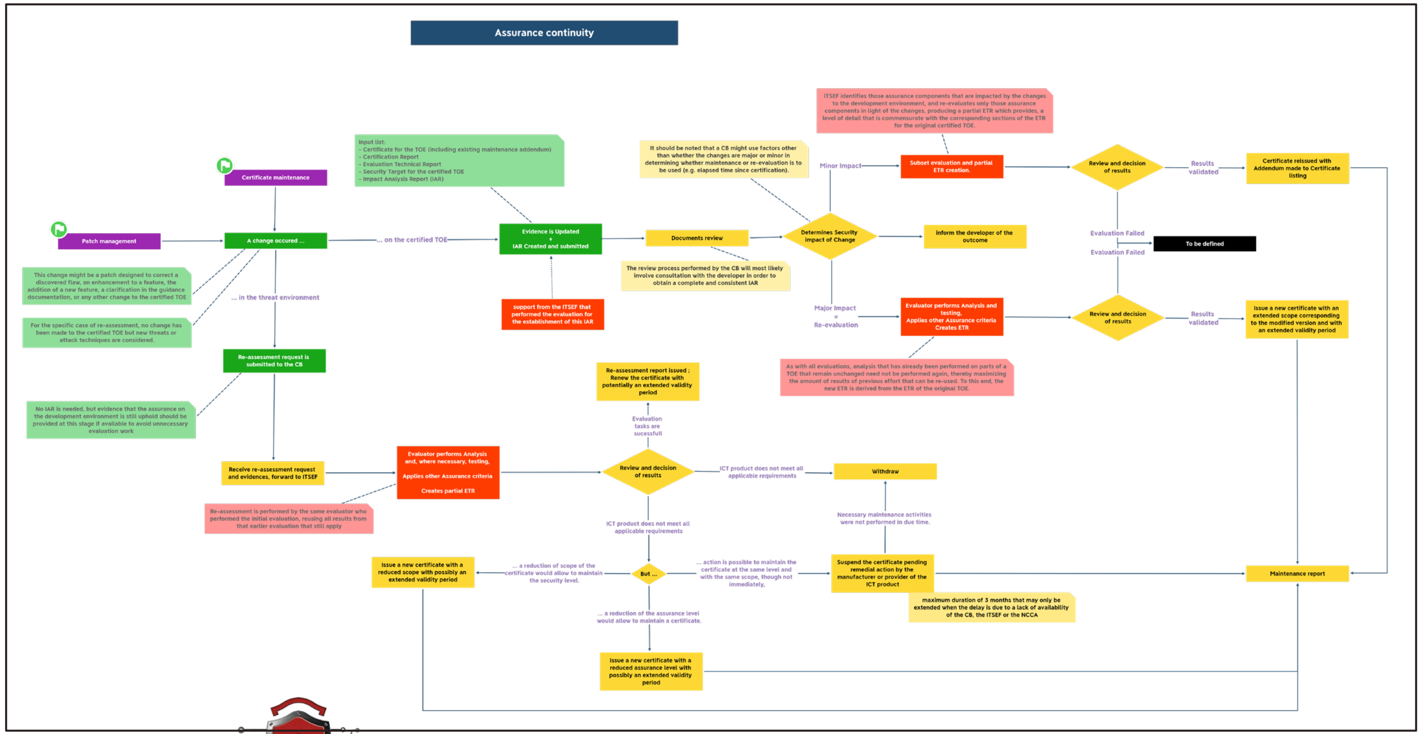
Generic actions

To Define

Start point of the process

Decision

Process Or Action


Assurance continuity
Certificate maintenance
Patch management
A change occured ...
... on the certified TOE
... in the threat environment
This change might be a patch designed to correct a discovered flaw, an enhancement to a feature, the addition of a new feature, a clarification in the guidance documentation, or any other change to the certified TOE
For the specific case of re-assessment, no change has been made to the certified TOE but new threats or attack techniques are considered.
Input list:
- Certificate for the TOE (including existing maintenance addendum)
- Certification Report
- Evaluation Technical Report
- Security Target for the certified TOE
- Impact Analysis Report (IAR)
Evidence is Updated + IAR Created and submitted
support from the ITSEF that performed the evaluation for the establishment of this IAR
Documents review
The review process performed by the CB will most likely involve consultation with the developer in order to obtain a complete and consistent IAR
It should be noted that a CB might use factors other than whether the changes are major or minor in determining whether maintenance or re-evaluation is to be used (e.g. elapsed time since certification).
Determines Security impact of Change
inform the developer of the outcome
Minor Impact
Subset evaluation and partial ETR creation.
ITSEF identifies those assurance components that are impacted by the changes to the development environment, and re-evaluates only those assurance components in light of the changes, producing a partial ETR which provides, a level of detail that is commensurate with the corresponding sections of the ETR for the original certified TOE.
Review and decision of results
Results validated
Certificate reissued with Addendum made to Certificate listing
Evaluation Failed
To be defined
Evaluation Failed
Major Impact = Re-evaluation
Evaluator performs Analysis and testing, Applies other Assurance criteria Creates ETR
As with all evaluations, analysis that has already been performed on parts of a TOE that remain unchanged need not be performed again, thereby maximizing the amount of results of previous effort that can be re-used. To this end, the new ETR is derived from the ETR of the original TOE.
Review and decision of results
Results validated
Issue a new certificate with an extended scope corresponding to the modified version and with an extended validity period
Re-assessment request is submitted to the CB
No IAR is needed, but evidence that the assurance on the development environment is still uphold should be provided at this stage if available to avoid unnecessary evaluation work
Receive re-assessment request and evidences, forward to ITSEF
Evaluator performs Analysis and, where necessary, testing, Applies other Assurance criteria Creates partial ETR
Re-assessment is performed by the same evaluator who performed the initial evaluation, reusing all results from that earlier evaluation that still apply
Review and decision of results
Evaluation tasks are sucessfull
Re-assessment report issued ; Renew the certificate with potentially an extended validity period
ICT product does not meet all applicable requirements
Withdraw
ICT product does not meet all applicable requirements
But ...
... a reduction of scope of the certificate would allow to maintain the security level.
Issue a new certificate with a reduced scope with possibly an extended validity period
... a reduction of the assurance level would allow to maintain a certificate.
Issue a new certificate with a reduced assurance level with possibly an extended validity period
... action is possible to maintain the certificate at the same level and with the same scope, though not immediately,
Suspend the certificate pending remedial action by the manufacturer or provider of the ICT product
maximum duration of 3 months that may only be extended when the delay is due to a lack of availability of the CB, the ITSEF or the NCCA
Necessary maintenance activities were not performed in due time.
Maintenance report

QUIZ

- What action must be taken by NCCA in case of a confirmed deviation from the requirements (e.g. non-disclosure of vulnerabilities by certificate holder) ?

- What happens when a manufacturer is unable to handle a problem within the defined period?

- Describe the vulnerability handling process

- What is the patch level for a vulnerability that is exploitable and requires minor changes to the TOE?

WHAT IS CC ? EUCC CANDIDATE SCHEME HIGHLIGHTS

Retention of records by CAB shall follow the general rules of accreditation standards ISO/IEC 17065 and ISO/IEC

17025.

Some EU schemes participating to the SOG-IS MRA cover the same type or categories of ICT products but may go beyond the EUCC in terms of national certification or cover partly the EUCC assurance levels.

A certificate contains the most relevant information for the identification of the product and the assurance level obtained.

Information associated to a certified ICT product shall be available for a period of at least five years after the expiration date of the certificate.

WHAT IS CC ? EUCC CANDIDATE SCHEME HIGHLIGHTS

Maximum period of validity of certificates shall be 5 years

ENISA will publish the certificates with appropriate relevant information attached. To manage accurate and up to date dataflows, ENISA will establish conditions and/or guidance for the delivery and publication of information.

The establishment of a mutual recognition agreement (MRA) between the participants shall support mutual recognition with third countries. Preliminary conditions for mutual recognition of certificates and for peer assessment are defined.

WHAT IS CC ? EUCC CANDIDATE SCHEME HIGHLIGHTS

- Certificates will provide a link to Supplementary cybersecurity information. Such information may be required for certification activities.
- In addition to the certification of ICT products, the scheme shall as well cover the certification of Protection Profiles.
- Security of information used for and created by certification shall be insured.
- Based on its experience, the AHWG recommends a transition period of two (2) years to adopt the new rules while introducing no market disruption. Any shorter period should be accompanied with temporary derogations to the EUCC rules.
- Groups of experts involving NCCA, CAB and their testing facilities, and manufactures or providers of ICT products should be considered as to further develop harmonised requirements for the scheme.

PEER ASSESSMENT

The EUCC scheme requires that each authority or body issuing certificates at the assurance level 'high' undergo a peer assessment at periodic intervals.

PEER REVIEW ≠ PEER ASSESSMENT

The peer assessment is not intended to interfere with or make judgement to the activities performed by the NCCA, as this is the subject of the peer review process as required by Article 59 of CSA. Nor shall it interfere with or make judgement to the activities performed by the National Accreditation Body (NAB).

A peer assessment shall be established for every authority or body issuing certificates (further designated under the term certification bodies, or CBs) for assurance level 'high' pursuant to provisions of the CSA, including associated testing laboratories (ITSEFs) to:

- assess that they work in an harmonised way and produce the same quality of certificates;
- allow the reuse of certificates for composite product certification,
- identify any potential strength that result out of their daily work and that may benefit to others;
- identify any potential weakness that result out of their daily work and that shall be considered for improvement by the peer assessed CB.
- find a harmonised way to handle vulnerabilities disclosure and handling and exchange best practices regarding the handling of complaints.

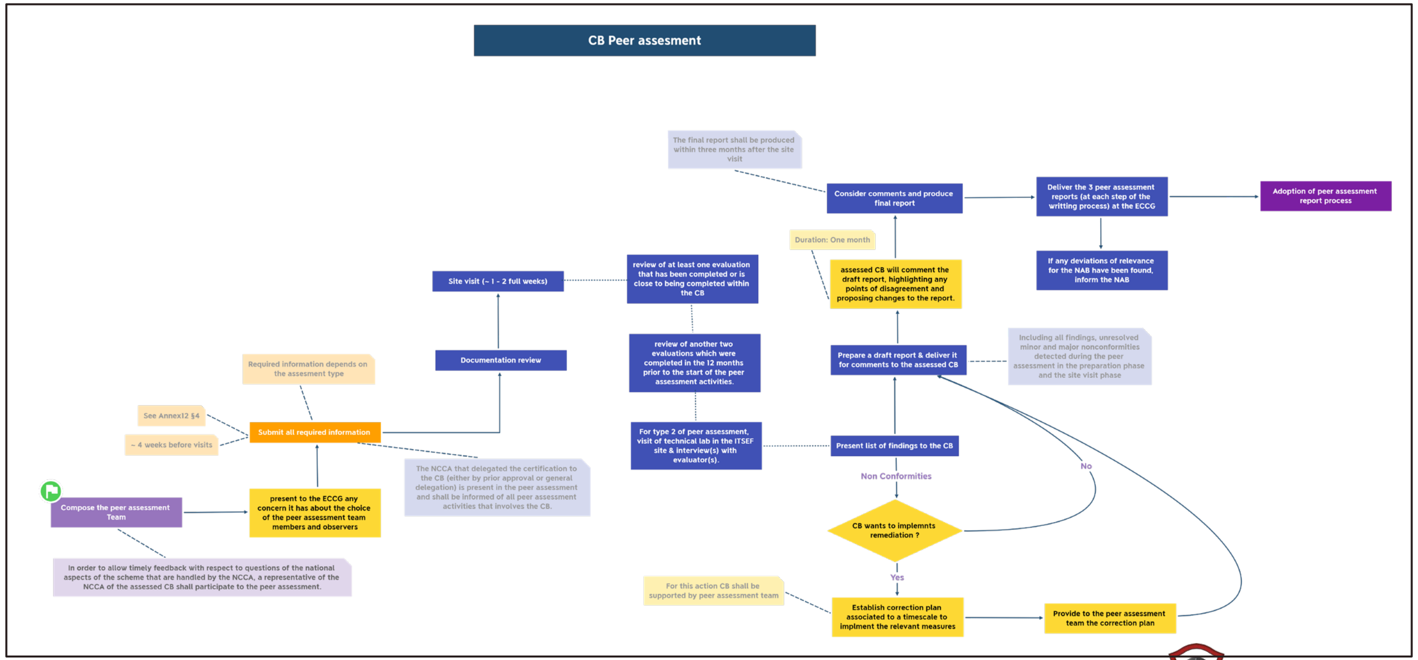
PEER ASSESSMENT PROCEDURE

This procedure covers three types of peer assessments:

- **Type 1**: When a Certification Body (CB) performs certification activities at the AVA_VAN.3 level;
- **Type 2**: When a CB performs certification activities related to a Technical Domain;
- **Type 3**: When a CB performs certification activities above the AVA_VAN.3 level according to a Protection Profile defined specifically for this usage and annexed to the EUCC scheme. (to be development)

Legend

CB | ITSEF
CAB | NCCA
Provider | ECCG
Peer Assessment Team | ENISA
Generic actions
To Define
Start point of the process
Decision | Process Or Action



CB Peer assesment

Compose the peer assessment Team

In order to allow timely feedback with respect to questions of the national aspects of the scheme that are handled by the NCCA, a representative of the NCCA of the assessed CB shall participate to the peer assessment.

present to the ECCG any concern it has about the choice of the peer assessment team members and observers

Submit all required information

Required information depends on the assesment type

See Annex12 §4

~ 4 weeks before visits

The NCCA that delegated the certification to the CB (either by prior approval or general delegation) is present in the peer assessment and shall be informed of all peer assessment activities that involves the CB.

Documentation review

Site visit (~ 1 - 2 full weeks)

review of at least one evaluation that has been completed or is close to being completed within the CB

review of another two evaluations which were completed in the 12 months prior to the start of the peer assessment activities.

For type 2 of peer assessment, visit of technical lab in the ITSEF site & interview(s) with evaluator(s).

Present list of findings to the CB

CB wants to implemnts remediation ?

Establish correction plan associated to a timescale to implment the relevant measures

For this action CB shall be supported by peer assessment team

Provide to the peer assessment team the correction plan

Prepare a draft report & deliver it for comments to the assessed CB

Including all findings, unresolved minor and major nonconformities detected during the peer assessment in the preparation phase and the site visit phase

assessed CB will comment the draft report, highlighting any points of disagreement and proposing changes to the report.

Duration: One month

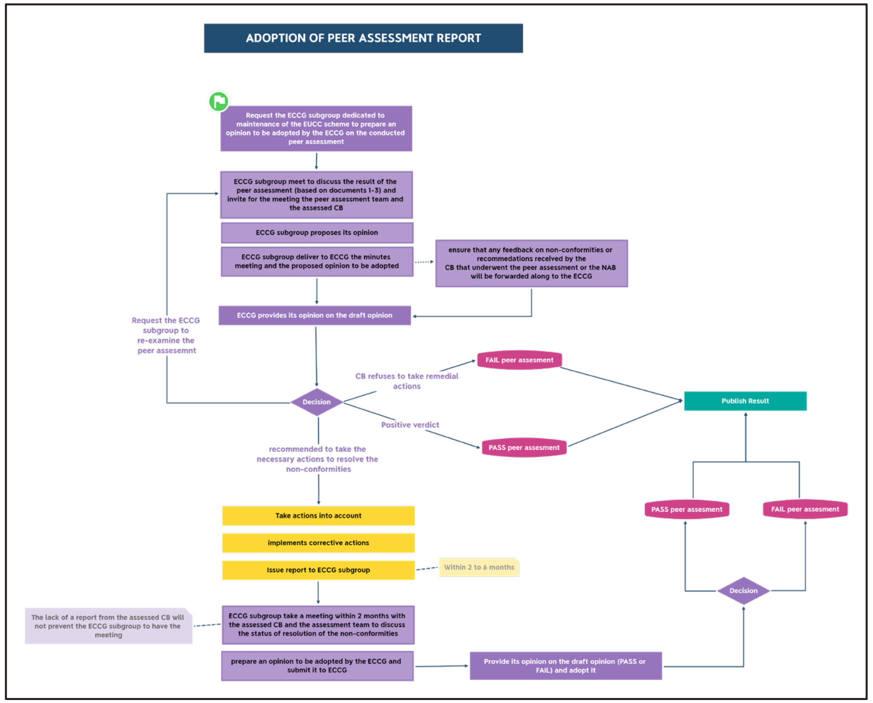
Consider comments and produce final report

The final report shall be produced within three months after the site visit

Deliver the 3 peer assessment reports (at each step of the writting process) at the ECCG

If any deviations of relevance for the NAB have been found, inform the NAB

Adoption of peer assessment report process



ADOPTION OF PEER ASSESSMENT REPORT

Request the ECCG subgroup dedicated to maintenance of the EUCC scheme to prepare an opinion to be adopted by the ECCG on the conducted peer assessment

ECCG subgroup meet to discuss the result of the peer assessment (based on documents 1-3) and invite for the meeting the peer assessment team and the assessed CB

ECCG subgroup proposes its opinion

ECCG subgroup deliver to ECCG the minutes meeting and the proposed opinion to be adopted

ensure that any feedback on non-conformities or recommedations received by the CB that underwent the peer assessment or the NAB will be forwarded along to the ECCG

ECCG provides its opinion on the draft opinion

Decision
Request the ECCG subgroup to re-examine the peer assesemnt
CB refuses to take remedial actions
Positive verdict
recommended to take the necessary actions to resolve the non-conformities

FAIL peer assesment

PASS peer assesment

Publish Result

Take actions into account

implements corrective actions

Issue report to ECCG subgroup

Within 2 to 6 months

ECCG subgroup take a meeting within 2 months with the assessed CB and the assessment team to discuss the status of resolution of the non-conformities

The lack of a report from the assessed CB will not prevent the ECCG subgroup to have the meeting

prepare an opinion to be adopted by the ECCG and submit it to ECCG

Provide its opinion on the draft opinion (PASS or FAIL) and adopt it

PASS peer assesment

FAIL peer assesment

QUIZ

- **How long must evaluation related information be kept by the CB after expiry of the certificate?**

- **Why is it important to have peer assessment?**

- **The peer assessment team submits their report to…?**

- **The peer-assessed CB provides their response to the assessment team. True or False?**

- **How long does the peer assessment team have to prepare the report?**

CONTACT

Red Alert Labs
71, rue Carnot | 94700 Maisons-Alfort

✉ *contact@redalertlabs.com*

☎ +33 9 53 55 54 11

🌐 **www.redalertlabs.com**

RED ALERT LABS
IoT Security

APPENDIX

PHASE 2: CONDUCT - SAR
DEVELOPMENT SECURITY (ALC_DVS)

Describes the security measures (physical, procedural and personal) taken to protect the TOE development process.

- personal access restriction
- IP transfer
- access revocation procedures

→ on-site visit by the evaluator is mandatory to evaluate this requirement

PHASE 2: CONDUCT - SAR
VULNERABILITY ANALYSIS (AVA_VAN.5)

- Data Loading
- Hostile Applet Loading
- Unintended Control Flow
- Simple and Differential Power Analysis
- Differential Fault Analysis
- Electromagnetic Analysis
- Brute-force Attack
- RNG Perturbation
- RSA Key Generation
- Perturbation Attacks

Vulnerability Characterization

Threats

Non-exploitability rationale