Demystifying "simplified CC for CRA"

13/10/2025

CRA Mondays

whoami

Roger Riera Guàrdia

Member of the **European Commission's CRA Expert Group** as a Type A member, contributing to the effective implementation of the CRA regulation and **Technical Manager at Applus+ Laboratories**, specialising in hardware security with 10 years of experience in the field.

Applus laboratories

European Commission

Previous

Background

Common Criteria

GSMA

EMVCo

Global Platform™ SESIP

psacertified™

What is sCC4CRA?

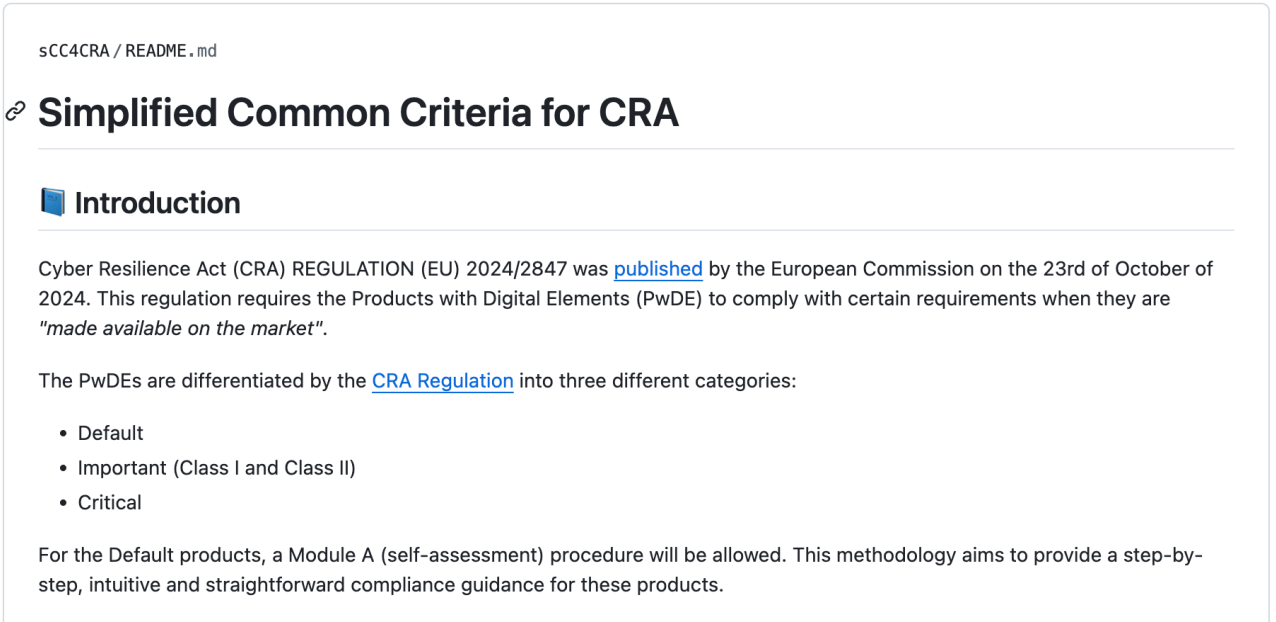
What is sCC4CRA?

“Simplified CC for CRA”

- Publicly accessible methodology
- Self-assessed for Default products
- Based on a simplified Common Criteria
- Designed to meet CRA compliance

Available in Github

🔗 https://github.com/sCC4CRA



sCC4CRA / README.md

Simplified Common Criteria for CRA

📘 Introduction

Cyber Resilience Act (CRA) REGULATION (EU) 2024/2847 was published by the European Commission on the 23rd of October of 2024. This regulation requires the Products with Digital Elements (PwDE) to comply with certain requirements when they are *"made available on the market"*.

The PwDEs are differentiated by the CRA Regulation into three different categories:

- Default
- Important (Class I and Class II)
- Critical

For the Default products, a Module A (self-assessment) procedure will be allowed. This methodology aims to provide a step-by-step, intuitive and straightforward compliance guidance for these products.

Methodology

Chapter 1 - Manufacturer risk assessment

📘 Introduction and Description (ASE_INT.1)

- **IAD-1** - The Technical Documentation introduction shall have a unique name and version.
- **IAD-2** - The Technical Documentation introduction shall include the manufacturer information.
- **IAD-3** - The Technical Documentation introduction shall include CRA compliance statements.
- **IAD-4** - The Technical Documentation introduction shall uniquely identify the PwDE.
- **IAD-5** - The PwDE description shall identify the product type.
- **IAD-6** - The PwDE description shall summarize the usage.
- **IAD-7** - The PwDE description shall describe the physical description of the PwDE.
- **IAD-8** - The PwDE description shall describe the logical description of the PwDE.

🛡️ Risk Assessment Analysis (ASE_SPD.1)

- **SPD-1** - Describe all threats in terms of a threat agent, an asset and an adverse action.
- **SPD-2** - Describe the OSPs.
- **SPD-3** - Describe the assumptions about the operational environment of the PwDE.

🎯 Security Objectives (ASE_OBJ.1)

- **OBJ-1** - Describe the security objectives for the operational environment.
- **OBJ-2** - Trace each security objective for the operational environment to the threat it addresses.
- **OBJ-3** - Trace each security objective for the operational environment to the OSPs which it enforces.
- **OBJ-4** - Trace each security objective for the operational environment to the assumptions it supports.
- **OBJ-5** - Demonstrate that the security objectives for the operational environment uphold all assumptions.

🔐 Security Functionalities (ASE_REQ.1 & ASE_TSS.1)

- **REQ-1** - Describe the Security Functions of the PwDE.
- **REQ-2** - For each threat, the Security Functions must demonstrate that they are suitable to meet that threat.
- **REQ-3** - For each OSP, the Security Functions must demonstrate that they are suitable to enforce that OSP.
- **REQ-4** - Shall be internally consistent.

For more details see the Playbook of Chapter 1 - Manufacturer risk assessment.

Chapter 2 - Guidance

🔧 Operational Guidance (AGD_OPE.1)

- **OPE-1** - Describe, for each end user, the Security Functions that should be controlled.
- **OPE-2** - Describe, for each interface, the privileges that should be controlled.
- **OPE-3** - Describe, for each end user, how to use the available interfaces provided in a secure manner.
- **OPE-4** - Describe, for each end user, the available interfaces.
- **OPE-5** - For each end user, clearly present each security actions they can perform.
- **OPE-6** - Identify all possible modes of operation of the PwDE.
- **OPE-7** - For each user, describe the security measures needed to meet the operational security objectives.

🧹 Decommissioning (AGD_DEC.1)

- **DEC-1** - Describe all the steps necessary for secure decommissioning upon end-of-life.
- **DEC-2** - Describe all the necessary equipment that is required to perform PwDE decommissioning.
- **DEC-3** - Decommissioning must prevent access to PwDE-protected assets after it's retired.
- **DEC-4** - The decommissioning procedures shall be compatible with the operational environment.

📦 Installation Guidance (AGD_PRE.1)

- **INS-1** - Shall describe all the steps necessary for secure acceptance of the delivered PwDE.
- **INS-2** - Shall describe all the steps necessary for secure installation of the PwDE.
- **INS-3** - Shall describe the secure preparation of the operational environment.

For more details see the Playbook of Chapter 2 - Guidance.

Chapter 3 - Development

🔤 Interfaces (ADV_FSP.2)

- **INT-1** - The described interfaces must be coherent with the PwDE design.
- **INT-2** - Describe the purpose, method of use and all parameters associated with each interface.
- **INT-3** - Describe the security action and error messages of the Interfaces.
- **INT-4** - Add a tracing between the Security Functions with the corresponding Interfaces.

🥾 Security Architecture (ADV_ARC.2)

- **ARC-1** - Describe the limitation of the attack surface provided by the PwDE.
- **ARC-2** - Describe how the PwDE initialisation process is secure.
- **ARC-3** - Demonstrate that the PwDE protects itself from tampering.
- **ARC-4** - Demonstrate that the PwDE prevents bypass of the Security Functions.
- **ARC-5** - Demonstrate that the PwDE enforces a secure default configuration when it is delivered.

🗂️ PwDE Design (ADV_TDS.2)

- **TDS-1** - Describe the structure of the PwDE in terms of subsystems.
- **TDS-2** - Describe the Security Functions behaviour of the subsystems.
- **TDS-3** - Provide a description of the interactions among all subsystems of the PwDE.
- **TDS-4** - Demonstrate that all interfaces trace to the behaviour described in the PwDE design that they invoke.
- **TDS-5** - Demonstrate that all Security Functions trace to the behaviour described in the PwDE design.

🗒️ Data Minimisation (ADV_PDM.1)

- **PDM-1** - Identify all data processed by the PwDE.
- **PDM-2** - Relate each data processed by the PwDE with the input interfaces from which it is received.
- **PDM-3** - Relate each data processed by the PwDE with the outbound interfaces where it is outputted.
- **PDM-4** - Demonstrate that all data handled by the PwDE is needed and appropriate for its purpose.

For more details see the Playbook of Chapter 3 - Development.

Chapter 4 - Life Cycle

🧩 SBOM (ALC_CMS.2 & ALC_SBM.1)

- **SBM-1** - Include the PwDE itself and the parts that comprises the PwDE, each part uniquely identified.
- **SBM-2** - For each hardware component that comprises the PwDE, shall indicate the developer of the item.
- **SBM-3** - For each item of the SBOM, shall indicate the developer of the item in specific format

🔄 Life Cycle (ALC_LCD.1)

- **LCD-1** - Describe the processes used to develop and maintain the PwDE.
- **LCD-2** - Provide for the necessary control over the development and maintenance of the PwDE.

For more details see the Playbook of Chapter 4 - Life Cycle.

Chapter 5 - Testing

🔗 ⬜ Functional (ATE_FUN.1)

- **FUN-1** - The test documentation shall consist of test plans, expected test results and actual test results.
- **FUN-2** - The test plans shall identify the tests to be performed and describe the scenarios for performing each test.
- **FUN-3** - The expected test results shall show the anticipated outputs from a successful execution of the tests.
- **FUN-4** - The actual test results shall be consistent with the expected test results.

🔍 Depth (ATE_DPT.1)

- **DPT-1** - Shall demonstrate the correspondence between the tests and the PwDE subsystems.
- **DPT-2** - The analysis of the depth of testing shall demonstrate that all PwDE subsystems have been tested.

For more details see the Playbook of Chapter 5 - Testing.

Chapter 6 - Vulnerability Analysis

🕵️ Vulnerability Analysis (AVA_VAN.5)

- **VAN-1** - Search public sources for potential vulnerabilities in the PwDE.
- **VAN-2** - Search public sources for potential vulnerabilities in the third-party components.
- **VAN-3** - Perform an independent vulnerability analysis using the Technical Documentation and the code.
- **VAN-4** - Devise penetration testing based on the identified potential vulnerabilities.
- **VAN-5** - Conduct penetration testing based on the identified potential vulnerabilities.
- **VAN-6** - Conclude that the product is placed in the market without known exploitable vulnerabilities.

For more details see the Playbook of Chapter 6 - Vulnerability Analysis.

Step-by-Step Playbook

Methodology

Chapter 1 - Manufacturer risk assessment

🟦 Introduction and Description (ASE_INT.1)

- **IAD-1** - The Technical Documentation introduction shall have a unique name and version.
- **IAD-2** - The Technical Documentation introduction shall include the manufacturer information.
- **IAD-3** - The Technical Documentation introduction shall include CRA compliance statements.
- **IAD-4** - The Technical Documentation introduction shall uniquely identify the PwDE.
- **IAD-5** - The PwDE description shall identify the product type.
- **IAD-6** - The PwDE description shall summarize the usage.
- **IAD-7** - The PwDE description shall describe the physical description of the PwDE.
- **IAD-8** - The PwDE description shall describe the logical description of the PwDE.

🛡️ Risk Assessment Analysis (ASE_SPD.1)

- **SPD-1** - Describe all threats in terms of a threat agent, an asset and an adverse action.
- **SPD-2** - Describe the OSPs.
- **SPD-3** - Describe the assumptions about the operational environment of the PwDE.

Chapter 1 - Manufacturer risk assessment

🟦 Introduction and Description (ASE_INT.1)

IAD-1 - The Technical Documentation introduction shall have a unique name and version

1. MUST have a unique reference with a unique name and version.
2. The unique identification MUST clearly distinguish from other Technical Documentations.

IAD-2 - The Technical Documentation introduction shall include the manufacturer information

1. MUST be indicated the name, registered trade name or registered trademark of the manufacturer.
2. MUST be indicated the postal address, email address or other digital contact details.
3. Where applicable, MUST be indicated the website where the manufacturer can be contacted.
4. The contact details MUST be in a language which can be easily understood by users and market surveillance authorities.
5. MUST be included the single point of contact that enables users to communicate with them.
6. MUST be included the type of technical security support offered to handle vulnerabilities and manage security updates.

1. Self-assessed
2. Step-by-step
3. CRA focused
4. High-level and low-level steps

Why it matters?

- **Horizontal standards (1-15)**
  - Risk-based approach (CRA Annex I)
  - Essential Requirements (CRA Annex I part 1)
  - Vulnerability Handling (CRA Annex I part 2)

→ Led by CEN-CLC/JTC 13 WG 9
- Framework standards
- Product agnostic

- **Vertical standards (16-41)**
  - Important products class 1 (CRA Annex III)
  - Important products class 2 (CRA Annex III)
  - Critical products (CRA Annex IV)

→ 

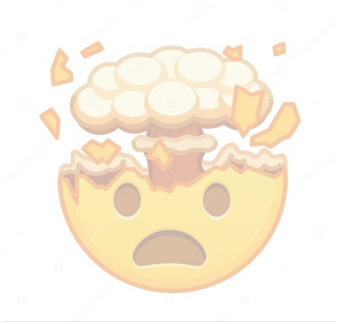
Important products — application of standards/third-party assessment
(operating systems, anti-virus, routers, firewalls…)

Critical products — in the future potentially certification
(smart cards, secure elements, smart meter gateways…)

¿ 

Default category — self-assessment
(memory chips, mobile apps, smart speakers, computer games...) ?

***Source**: Webinar on 10 March 2025 – Organised by CEN/CENELEC - Standards supporting the Cyber Resilience Act*



Based on Common Criteria...

To meet CRA

Based on Common Criteria?

- Common Criteria is seen as the “Voldemort” of cybersecurity certification
- It is often seen as:

Too much formality

High cost

Too much documentation

Complex evaluations

Yes! based on Common Criteria

- But Common Criteria is also a powerful methodology

Common Understanding

Step-by-step Methodology

Risk Based approach

Seamless Composition (CC, SESIP)

Actually... based on the CEM

CC Part 3 ASE_INT.1.2C: *The ST reference shall uniquely identify the ST.*

12.3.1.3.3 Work unit ASE_INT.1-2

The evaluator ***shall examine*** the ST reference to determine that it uniquely identifies the ST.

The evaluator determines that the ST reference identifies the ST itself, so that it may be easily distinguished from other STs, and that it also uniquely identifies each version of the ST, e.g. by including a version number and/or a date of publication.

In evaluations where a CM system is provided, the evaluator may validate the uniqueness of the reference by checking the configuration list. In the other cases, the ST should have some referencing system that is capable of supporting unique references (e.g. use of numbers, letters or dates).

IAD-1 - The Technical Documentation introduction shall have a unique name and version

1. MUST have a unique reference with a unique name and version.
2. The unique identification MUST clearly distinguish from other Technical Documentations.

17.2.5.7.6 Work unit AVA_VAN.5-11

The evaluator ***shall examine*** the results of all penetration testing to determine that the TOE, in its operational environment, is resistant to an attacker possessing a **High** attack potential.

If the results reveal that the TOE, in its operational environment, has vulnerabilities exploitable by an attacker possessing an attack potential less than **or equal to** High, then this evaluator action fails.

The guidance in B.4 and the guidance for special technical areas that is relevant for the national scheme should be used to determine the attack potential required to exploit a particular vulnerability and whether it can therefore be exploited in the intended environment. It may not be necessary for the attack potential to be calculated in every instance, only if there is some doubt as to whether or not the vulnerability can be exploited by an attacker possessing an attack potential less than **or equal to** High.

VAN-5 - Conduct penetration testing based on the identified potential vulnerabilities.

1. The PwDE used to perform the penetration testing MUST be identified as per [AGD_PRE.1].
2. The PwDE SHOULD be in Security by Default configuration as per [AGD_PRE.1].
3. MUST be coherent with the security objectives for the operational environment described in [ASE_OBJ.1].
4. If any test resources are used, they MUST be calibrated and used correctly.
5. MUST record the actual results of the penetration tests.

⚠️ If no penetration testing was devised, this requirement DOES NOT apply.

VAN-6 - Conclude that the product is placed in the market without known exploitable vulnerabilities.

1. The manufacturer MUST fix all known actively exploited vulnerabilities before placing the PwDE in the market.
2. The manufacturer MUST fix all known exploitable vulnerabilities before placing the PwDE in the market.

⚠️ The section 5.3.2 of the TR-03183 interprets as optional the fixing known exploitable vulnerabilities.

Designed to meet CRA

- **July 2023:** Request from the Commission to ENISA
- **Nov 2023:** Nov 2023: First strategy report linking CRA & EUCC, presented at ENISA Certification Week (Málaga).
- **July 2024:** Revised to reflect CRA changes (Mar 2024) & EUCC Implementing Act; shared with ECCG/SCCG.
- **September 2024:** received and applied feedback from stakeholders
- **January 2025:** final version published in ENISA website

Purpose: Initial analysis to guide future use of EUCC to demonstrate CRA compliance.

1. Maintain requirements for complaince
2. Resolve GAP's mentioned
3. Slight improvements
4. Do not reinvent the wheel

***Source**: Webinar on 5 June 2025 – Organised by ENISA - EUCC–CRA Interplay Webinar*

Designed to meet CRA

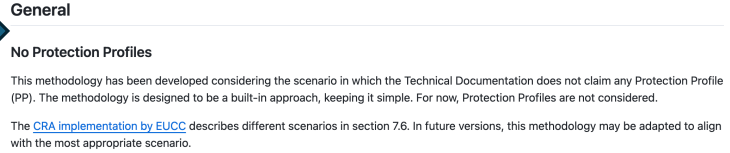
Essential security requirement (CRA Annex I, Part I)	CC SFRs (from [CC2022P2] or extended)	CC SARs (from [CC2022P3] or extended)	Notes
(1) *Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;*		ASE_SPD.1 Security problem definition ASE_OBJ.1 Security objectives ASE_REQ.1 Direct rationale security requirements	The Security Problem Definition is based on a risk analysis that ultimately leads in CC to selection of SFRs and SARs that can define security aspects equivalent to those in CRA ESRs. It is done in a way similar than that in CRA, where the manufacturer's risk assessment leads to the selection of applicable ESRs from those in CRA Annex I, part 1.
(2) *On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:*	-	-	-
(2)(a) *be made available on the market without known exploitable vulnerabilities;*		AVA_VAN.1 Vulnerability survey	Any EUCC evaluation with assurance level "substantial" or "high" may directly fulfil this requirement.
(2)(b) be *made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;*	FMT_SMF.1 Specification of Management Functions	ADV_ARC.2 Security Architecture with Default Secure Configuration (Extended)	FMT_SMF.1 shall include a management function that permits resetting the TOE to its initial or default configuration. Other SFRs or SARs with equivalent functionality could also meet the requirements, the ones given here are merely one proposal. Alternatively, ADV_ARC.2 could be left out of the evaluation if: a) An agreement as mentioned in the ESR is provided with the technical documentation. b) The risk assessment contemplates a compensating security measure making the requirement not applicable or necessary. A practical

***Source**: Webinar on 5 June 2025 – Organised by ENISA - EUCC–CRA Interplay Webinar*

Designed to meet CRA

Rationale of changes can be found in:

- https://github.com/sCC4CRA/sCC4CRA/blob/main/rationale.md



Rationale for the analysis, changes and exclusions

This document describes the rationale used to simplify the Common Criteria CC:2022 Release 1 methodology to build this methodology.

General

No Protection Profiles

This methodology has been developed considering the scenario in which the Technical Documentation does not claim any Protection Profile (PP). The methodology is designed to be a built-in approach, keeping it simple. For now, Protection Profiles are not considered.

The CRA implementation by EUCC describes different scenarios in section 7.6. In future versions, this methodology may be adapted to align with the most appropriate scenario.

Some examples are:

No SARs

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_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
ST 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

Remove SFR Formality

11.2.5 FDP_ACC.1 Subset access control

Component relationships

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute-based access control

FDP_ACC.1.1

The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].

But… with partial compliance…

- Considering → **Horizontal standards (1-15)**
  - Risk-based approach (CRA Annex I)
  - Essential Requirements (CRA Annex I part 1)
  - Vulnerability Handling (CRA Annex I part 2)

- Part 2 is already integrated.
- Part 1 (Risk assessment) and Part 3 (Vulnerability Handling) are still not integrated.

CRA Compliance

The CRA Regulation describes many obligations to be fulfilled by the Products with Digital Elements (PwDEs) and the stakeholders managing them (e.g. the Manufacturers).

This methodology is intended to facilitate the Manufacturer obligations (Article 13) for Default Products, in order to allow that their products fulfill the requirements for PwDEs as indicated in (Article 6) and to develop the Technical Documentation as set out in (Article 31).

To verify the applicability of this methodology, should be checked that your product does NOT fall under the product descriptions set out in Annex III or in Annex IV.

The following table shows the actual coverage of the CRA Regulation requirement of this methodology:

Annex	Coverage	Comments
Annex I Part I	🟡✅	All requirements are covered except for: * Risk assesment * Vulnerability Handling See rationale
Annex I Part II	❌	The Vulnerability Handling are not covered, see rationale
Annex II	✅	All requirements covered ✅ by [ASE_INT.1]
Annex VII	🟡✅	All requirements are covered except for the Security Updates. See rationale

How to use sCC4CRA?

How to use sCC4CRA?

Table of Contents

Chapter 1 – Manufacturer Risk Assessment

Introduction and Description (ASE_INT.1)

ST and TOE Reference [IAD-1][IAD-2]

TD name	TD version

PwDE name	PwDE version

PwDE Description [IAD-3] [IAD-4] [IAD-5] [IAD-6]

Risk Assessment Analysis (ASE_SPD.1)

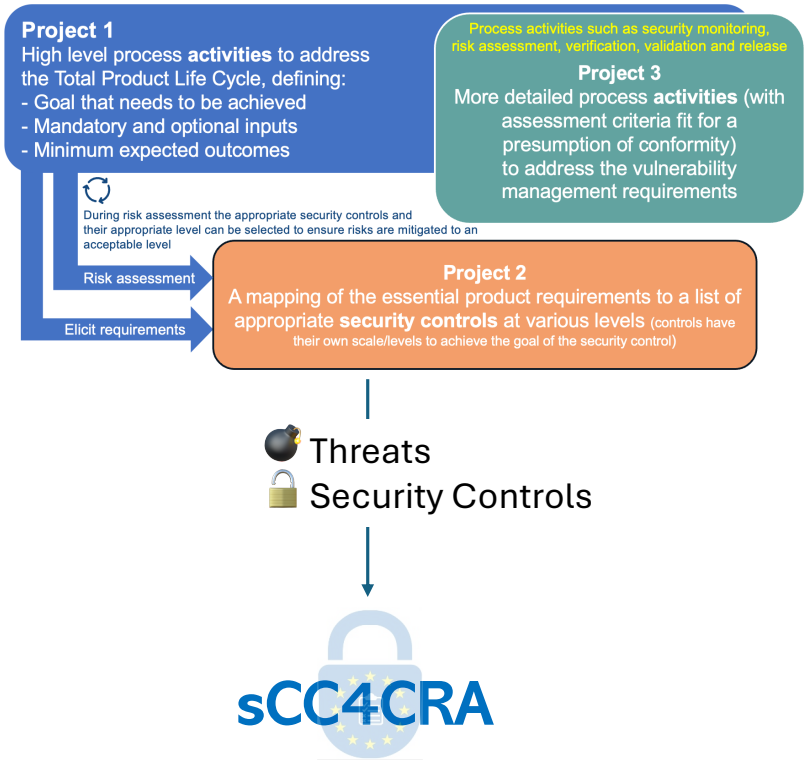
Threats [SPD-1]

Assumptions [SPD-2]

Security Objectives (ASE_OBJ.1)

Security Functionalities (ASE_REQ.1 & ASE_TSS.1)

How to use sCC4CRA?



***Source**: Webinar on 8 September 2025 – Organised by CEN/CENELEC - Unlocking CRA Security Controls: preparation for UNE Event*

How to use sCC4CRA?

ECR ANNEX I Part I (2) (d) - Access Control

(d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;

Threat	Security Objective
Threat.UnauthorizedAccess	SO.AccessControl
Threat.NotReportedUnauthorizedAccess	SO.AccessControlReport

Threats

Risk Assessment Analysis (ASE_SPD.1)

- **SPD-1** - Describe all threats in terms of a threat agent, an asset and an adverse action.
- **SPD-2** - Describe the OSPs.
- **SPD-3** - Describe the assumptions about the operational environment of the PwDE.

Mapping with 18031-X:2024

[ACM] Access control mechanism

- [ACM-1] Applicability of access control mechanisms
- [ACM-2] Appropriate access control mechanisms

Security Controls

Security Functionalities (ASE_REQ.1 & ASE_TSS.1)

- **REQ-1** - Describe the Security Functions of the PwDE.
- **REQ-2** - For each threat, the Security Functions must demonstrate that they are suitable to meet that threat.
- **REQ-3** - For each OSP, the Security Functions must demonstrate that they are suitable to enforce that OSP.
- **REQ-4** - Shall be internally consistent.

For more details see the Playbook of Chapter 1 - Manufacturer risk assessment.

***Source**: Webinar on 8 September 2025 – Organised by CEN/CENELEC - Unlocking CRA Security Controls: preparation for UNE Event*

and finally...

But… why not…

Why not just Common Criteria EAL1?

Why keep using Common Criteria?

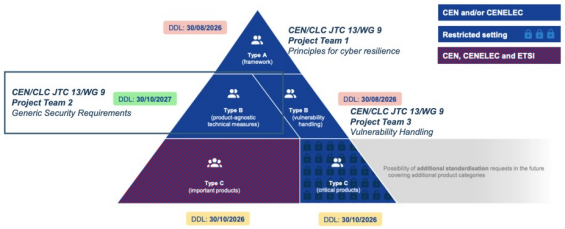
Why not just simplifying another EN standard?

Why not just using the CEN/CLC/JTC 13/WG 9?

The Future work and next steps

Continuously simplifying

Align with Standardization Work



Include Composition

Add Composition Guidelines

Add Remote Data Processing

Prepare courses and trainings

About the industry

- Looking for collaboration and support 🤝
- Interest from some players
  - Applus+ Laboratories is considering to use part of the methodology for our CoC for CRA
- Other potential interest
  - Products with CC or SESIP certified components
  - Stakeholders with experience with CC
- Main target is manufacturers of products falling in the Default category

Default category — self-assessment
(memory chips, mobile apps, smart speakers, computer games...)

Thank you!

Open Regulatory Compliance

https://es.linkedin.com/in/rogerriera28