Common Criteria Recognition Arrangement
Common Criteria Maintenance Board

CC Errata and Interpretation

Title: *Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1)*
Maintained by: *CCMB*
Unique identifier: *002*
Version: *1.1*
Date of issue: *2024-07-22*
Status: *Final*
Approved by: *CCDB*

Content Table

Introduction

Objective of the present document is to collect issues of different type that were identified for CC:2022 (Release 1), Parts 1 to 5 and CEM:2022 (Release 1) and to provide appropriate solutions as proposed corrections or interpretations, respectively. Issues might concern for instance (technical) errors, inconsistencies, missing entries on content level as well as layout bugs found in the CC / CEM documents. Furthermore, issues regards the application of the CC / CEM documents might be addressed as well.

For easy handling, this document contains for each CC / CEM document a separate section with specific tables, all those organized with the very same table structure and providing the necessary information. In particular, for each identified issue a detailed problem description is provided and accompanied by a corresponding resolution in form of a proposed correction or interpretation respectively. Hereby, each resolution carries specific information that indicates its status of applicability, i.e. in case of mandatory

application an entry of type ‘ma’, for recommended use an entry of type ‘re’, and entries of type ‘op’ address general issues that are of more open character and that expect further clarifying technical discussion or (future) work for their resolution.

The document is intended at the same time for support of the next revision of the CC / CEM in the sense of corresponding bugfixing and improvement.

Hint: As there is no difference on content level and technical wording between the core parts of CC:2022 (all parts) / CEM:2022 and the corresponding ISO/IEC 15408:2022 series / ISO/IEC 18045:2022 all issues and resolutions provided in the present document are analogously applicable for the aforementioned ISO CC / CEM version (except where indicated).

The present document is considered as a ‘living document’ that will be continually maintained and supplemented.

Terms and Definitions

For CC / CEM related abbreviations, terms and definitions refer to the CC / CEM documents listed in the section ‘References’ at the end of this document.

Legend for table entries:

Reference:	section in the respective CC Part / CEM document
Type of issue:	ed = editorial te = technical ge = general
Status of resolution:	ma = mandatory re = recommended op = open / in progress

Errata / Interpretation for CC:2022 Part 1

This section provides corrections and interpretations to CC:2022 Part 1 ([CC:2022-1]).

ID	CC2022-P1-R1-0001
Date	2023-12-22
Reference	3.2
Issue – Problem Description	**administrator** Note 1 to entry: Not all *protection profiles (PPs)* (3.68) or security targets (STs) assume the same level of trust for administrators. Typically, administrators are assumed to adhere at all times to the policies in the ST of the *target of evaluation (TOE)* (3.90). Some of these policies can be related to the functionality of the TOE, while others can be related to the *operational environment (3.63)*. Problem: "Security targets (STs)" is defined in the document, therefore it should be in an italic and needs reference number.
Type	ed/te
Resolution - Correction / Interpretation	**administrator** Note 1 to entry: Not all *protection profiles (PPs)* (3.68) or *security targets (STs)* (3.82) assume the same level of trust for administrators. Typically, administrators are assumed to adhere at all times to the policies in the ST of the *target of evaluation (TOE)* (3.90). Some of these policies can be related to the functionality of the TOE, while others can be related to the *operational environment (3.63)*.
Status	ma
Remarks	-

ID	CC2022-P1-R1-0002
Date	2023-12-22
Reference	3.48
Issue – Problem Description	**extended security requirement** Note 1 to entry: An extended security requirement preserves the form and syntax described in CC Part 2. Problem: Both security functional requirements and security assurance requirements can be extended. So, note 1 to entry should also include CC Part 3.

Type	te
Resolution - Correction / Interpretation	**extended security requirement** Note 1 to entry: An extended security requirement preserves the form and syntax described in CC Part 2 and CC Part 3.
Status	ma
Remarks	-

ID	CC2022-P1-R1-0003
Date	2023-12-22
Reference	3.54
Issue – Problem Description	3.54 'implementation representation least abstract representation of the TOE security functionality (TSF) (3.92), specifically the one that is used to create the TSF itself without further design refinement (3.73)' Problem: Wrong reference to section 3.73 where the following definition of the term 'refinement' is provided: 3.73 'refinement addition of details to a security component' In 3.54, the term '(design) refinement' is not meant as 'operation on an SFR / SAR', but in the sense of 'detailing the design'.
Type	ed/te
Resolution - Correction / Interpretation	Skip the reference '(3.73)' in 3.54 and use instead the term 'design refinement' in the sense of 'detailing the design'.
Status	ma
Remarks	For the next CC / CEM revision, it is proposed to supplement the term 'design refinement' including a corresponding definition in the terminology section and to set then a (correct) reference in section 3.54. It could be the case that further terminology sections in CC / CEM are affected in similar manner, i.e. where terms with several definitions / meanings are specified in the CC / CEM and the wrong one is erroneously referenced in other terminology definitions.

ID	CC2022-P1-R1-0004
Date	2023-12-22
Reference	3.60
Issue – Problem Description	**multi-assurance evaluation** evaluation of a *target of evaluation (TOE)* (3.90) using a *PP-Configuration* (3.68) where each PP-Configuration component is associated with its own set of assurance requirements Problem: The subclause number of PP-Configuration is 3.69.
Type	ed/te
Resolution - Correction / Interpretation	**multi-assurance evaluation** evaluation of a *target of evaluation (TOE)* (3.90) using a *PP-Configuration* (3.69) where each PP-Configuration component is associated with its own set of assurance requirements
Status	ma
Remarks	-

ID	CC2022-P1-R1-0005
Date	2023-12-22
Reference	3.71
Issue – Problem Description	**Protection Profile module** **PP-Module** implementation-independent statement of security needs for a *target of evaluation (TOE)* (3.90) type complementary to one or more base *Protection Profiles* (3.68) and possibly some *base PP-Modules* (3.14) Problem: A reference to “base Protection Profile” is more proper than “Protection Profile” here. So, ‘base’ should be in an italic. A reference to the term should be ‘3.13’.
Type	ed/te
Resolution - Correction / Interpretation	**Protection Profile module** **PP-Module** implementation-independent statement of security needs for a *target of evaluation (TOE)* (3.90) type complementary to one or more *base Protection Profiles* (3.13) and possibly some *base PP-Modules* (3.14)
Status	ma
Remarks	-

ID	CC2022-P1-R1-0006
Date	2023-12-22
Reference	4
Issue – Problem Description	CAP composition assurance package Problem: CAP means composed assurance package. Refer to '3.20'.
Type	te
Resolution - Correction / Interpretation	CAP composed assurance package
Status	ma
Remarks	-

ID	CC2022-P1-R1-0007
Date	2023-12-22
Reference	5.2.2.6 / Table 1
Issue – Problem Description	- Column "Evaluators" of Row "Part 3" Shall use for reference when evaluating security functional components given in packages, PPs, PP-Modules and PP-Configurations or security assurance requirements in STs. - Column "Others" of Row "Part 3" May use for reference when reviewing security functional components given in packages, PPs, PP-Modules and PP-Configurations or security assurance requirements in STs. Problem: Part 3 is related to assurance components.
Type	te
Resolution - Correction / Interpretation	- Column "Evaluators" of Row "Part 3" Shall use for reference when evaluating security assurance components given in packages, PPs, PP-Modules and PP-Configurations or security assurance requirements in STs. - Column "Others" of Row "Part 3" May use for reference when reviewing security assurance components given in packages, PPs, PP-Modules and PP-Configurations or security assurance requirements in STs.
Status	ma
Remarks	-

ID	CC2022-P1-R1-0008
Date	2023-12-22
Reference	8.2.4.2 / 1st paragraph / 1st bullet
Issue – Problem Description	A PP, PP-Module or package may define a set of security functional components and/or SFRs called selection-based SFRs. This set of components and/or SFRs is associated with a selection made in another component and/or SFRs in the PP, PP-Module or package. The related selection-based components and/or SFRs shall be included in a PP, PP-Module, package or ST if: — a selection choice identified in the PP, PP-Module or package indicates that it has an associated selection-based SFR; — that selection is made by the author. Problem: Two conditions above shall be satisfied at the same time, so the first bullet needs "and".
Type	ed/te
Resolution - Correction / Interpretation	A PP, PP-Module or package may define a set of security functional components and/or SFRs called selection-based SFRs. This set of components and/or SFRs is associated with a selection made in another component and/or SFRs in the PP, PP-Module or package. The related selection-based components and/or SFRs shall be included in a PP, PP-Module, package or ST if: — a selection choice identified in the PP, PP-Module or package indicates that it has an associated selection-based SFR; and — that selection is made by the author.
Status	ma
Remarks	-

ID	CC2022-P1-R1-0009
Date	2023-12-22
Reference	8.2.4.2 / EXAMPLE
Issue – Problem Description	FTP_ITC.1.1 The TSF shall be capable of using [selection: IPsec, SSH, TLS, HTTPS] to provide a trusted communication channel between... Application Note: *In the selection for FTP_ITC.1.1, the ST author ….* […] The following SFRs are included in the ST if the ST author selects "IPsec" in FTP_ITC.1.1:

	[…] Problem: The element identifier FTP_ITC.1.1 is from CC Part 2, but the statement is not identical to FTP_ITC.1.1 from CC Part 2. This example is a refined SFR (originating from the Network Devices (ND) cPP), but the refinement according to section 8.2.5 is not clearly outlined.
Type	te
Resolution - Correction / Interpretation	EXAMPLE An example of a selection-based SFR is the following one, whereby FTP_ITC.1.1 (refined according to section 8.2.5) is the SFR with the selection and FCS_IPSEC.1 is the selection-based SFR: FTP_ITC1.1 (refined) The TSF shall **be capable of using [selection: IPsec, SSH, TLS, HTTPS] to** provide a trusted communication channel between ... Application Note: […]
Status	ma
Remarks	-

ID	CC2022-P1-R1-0010
Date	2023-12-22
Reference	10.3 / 2nd paragraph / 4th para of e)
Issue – Problem Description	Where PPs claim strict or demonstrable conformance to PP(s) they shall not also claim conformance to the packages claimed in the PPs they claim conformance to, unless the PP augments the package. The PP claims <package>-augmented only in the case where the PP augments the packages beyond that claimed by the PP to which it claims conformance to. Problem: It is unclear. The statement should be more clarified in terms of PPs that makes conformance claims and another PPs that are claimed conformance to.
Type	ed/te
Resolution - Correction / Interpretation	Where PPs claim strict or demonstrable conformance to another PP(s) they shall not also claim conformance to the packages claimed in another PPs they claim conformance to, unless the PP augments the package. The PP claims <package>-augmented only in the case where the PP augments the packages beyond that claimed by another PP to which it claims conformance to.
Status	re
Remarks	-

ID	CC2022-P1-R1-0011
Date	2023-12-22
Reference	10.3, 12.2
Issue – Problem Description	In [CC:2022-3], section 7.3.2, APE_CCL.1.9C to 12C and [CC:2022-3], section 7.4.2, ASE_CCL.1.8C to 11C a conformance claim rationale is required for PPs and STs. Such conformance claim rationale describes the reasons and the logical basis for the author's choice of conformance claims and statement including the topics to be addressed in such conformance claim rationale. However, in the overview of the PP contents in [CC:2022-1], the completeness of the requirements for such conformance claim rationale does not seem to be given in section 10.3 f). In the overview of the ST contents in [CC:2022-1], the conformance claim rationale is not mentioned at all in section 12.2.
Type	ed/te
Resolution - Correction / Interpretation	[CC:2022-1], section 10.3 f) shall be read as: 'If a conformance claim with respect to other PPs or to functional packages was made, then the PP shall contain a conformance claim rationale addressing TOE type, SPD, Security Objectives, Security Requirements, cf. [CC:2022-3], APE_CCL.1.9C to 12C.' [CC:2022-1], section 12.2 e), f) shall be read as: 'If a conformance claim with respect to PPs or PP-Configuration or functional packages was made, then the ST shall contain a conformance claim rationale addressing TOE type, SPD, Security Objectives, Security Requirements, cf. [CC:2022-3], ASE_CCL.1.8C to 11C.'
Status	ma
Remarks	-

ID	CC2022-P1-R1-0012
Date	2023-12-22
Reference	10.3 / 2nd paragraph / g) / 2nd paragraph of "strict conformance"
Issue – Problem Description	Strict conformance allows the conformant PP/ST not to add any element to the PP's SPD, set of objectives and SFRs, i.e. the superset defined in the PP/ST may be identical to the PP's, with all the SFRs resolved; Problem: To be a superset of the PP, the addition shall be allowed.
Type	te

Resolution - Correction / Interpretation	Strict conformance allows the conformant PP/ST to not add any element to the PP's SPD, set of objectives and SFRs, i.e. the superset defined in the PP/ST may be identical to the PP's, with all the SFRs resolved;
Status	ma
Remarks	-

ID	CC2022-P1-R1-0013
Date	2023-12-22
Reference	10.5.1 / last paragraph
Issue – Problem Description	This general statement holds for the different constructs of the PP/ST, namely the SPD, the security objectives for the TOE, the security objectives for the environment, and the security functional and SARs. Problem: The highlighted part is incomplete.
Type	ed/te
Resolution - Correction / Interpretation	This general statement holds for the different constructs of the PP/ST, namely the SPD, the security objectives for the TOE, the security objectives for the environment, and SFRs and SARs.
Status	ma
Remarks	-

ID	CC2022-P1-R1-0014
Date	2023-12-22
Reference	11.2.3.3 / c)
Issue – Problem Description	— *"Package Conformant"*; A PP-Module is conformant to a package if all constituent parts of the functional package, including the SPD, security objectives, and SFRs, of that functional package are present in the corresponding parts of the PP-Module without modification; — *"Package Augmented"*; A PP-Module claims an augmentation of a package if all constituent parts of the functional package, including the SPD, security objectives, and SFRs, contained in the PP-Module are identical to those given in the functional package, but shall also contain at least one SFR that is either additional or hierarchically higher than an SFR in the functional package; — *"Package Tailored"*; A PP-Module claims tailoring of a package if all constituent parts of the functional package, including the SPD, Security Objectives, and SFRs,

	contained in the PP-Module are identical to those given in the functional package, but shall have additional selection items for an SFR with existing selections in the package, and optionally, at least one additional SFR and/or one SFR that is hierarchically higher than an SFR in the functional package; Problem: To be a more clearer description, “package” should be “functional package”. (cf. bullet d) of 11.2.3.3 for the assurance package.)
Type	ed/te
Resolution - Correction / Interpretation	— *“Package Conformant”*; A PP-Module is conformant to a functional package if all constituent parts of the functional package, including the SPD, security objectives, and SFRs, of that functional package are present in the corresponding parts of the PP-Module without modification; — *“Package Augmented”*; A PP-Module claims an augmentation of a functional package if all constituent parts of the functional package, including the SPD, security objectives, and SFRs, contained in the PP-Module are identical to those given in the functional package, but shall also contain at least one SFR that is either additional or hierarchically higher than an SFR in the functional package; — *“Package Tailored”*; A PP-Module claims tailoring of a functional package if all constituent parts of the functional package, including the SPD, Security Objectives, and SFRs, contained in the PP-Module are identical to those given in the functional package, but shall have additional selection items for an SFR with existing selections in the package, and optionally, at least one additional SFR and/or one SFR that is hierarchically higher than an SFR in the functional package;
Status	ma
Remarks	-

ID	CC2022-P1-R1-0015
Date	2023-12-22
Reference	11.3.3 / Figure 6
Issue – Problem Description	The box “Using of a PP-Configuration” states that: See detailed figure “Building a PP-Configuration” The circle at the bottom states that: Evaluation methods are defined by ISO/IEC 18045 plus additional EM/EA Problem: There is no figure named “Building a PP-Configuration”. If it

	refers to figure 7, then it should be updated accordingly. ISO/IEC 18045 should be CEM.
Type	ed/te
Resolution - Correction / Interpretation	The box “Using of a PP-Configuration”: See figure 7 for details of building a PP-Configuration The circle at the bottom: Evaluation methods are defined by CEM plus additional EM/EA
Status	ma
Remarks	Note that this errata is only applicable to CC Part 1 but not to ISO/IEC 15408-1 unlike other errata applicable to both CC Part 1 and ISO/IEC 15408-1.

ID	CC2022-P1-R1-0016
Date	2023-12-22
Reference	12.2 / d)
Issue – Problem Description	— “*Package Augmented*” A ST claims augmentation of a package if: — for functional packages, all constituent parts (SPD, security objectives, and SFRs) of the functional package are present in the corresponding parts of the ST but the ST contains at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package; Problem: To be a more clear description, “package” should be “functional package”. (cf. the next bullet for assurance package.)
Type	ed/te
Resolution - Correction / Interpretation	— “*Package Augmented*” A ST claims augmentation of a package if: — for functional packages, all constituent parts (SPD, security objectives, and SFRs) of the functional package are present in the corresponding parts of the ST but the ST contains at least one additional SFR or one SFR that is hierarchically higher than an SFR in the functional package;
Status	ma
Remarks	-

ID	CC2022-P1-R1-0017

Date	2023-12-22
Reference	12.2 / e)
Issue – Problem Description	— *"PP Conformant";* A PP or TOE meets specific PP(s). Problem: 12.2, e) is describing the ST conformance claim to PP(s).
Type	te
Resolution - Correction / Interpretation	— *"PP Conformant";* An ST meets specific PP(s).
Status	ma
Remarks	-

ID	CC2022-P1-R1-0018
Date	2023-12-22
Reference	B.3.1 / Figure B.1, B.5.1 / Figure B.2, C.2.2.1 / Figure C.1, C.2.3 / Figure C.3, C.3.1 / Figure C.4, D.3.1 / Figure D.1, D.4.1 / Figure D.2
Issue – Problem Description	Standard claim (*Reference to the applied ISO/IEC 15408 and ISO/IEC 18045 standards, ISO/IEC 15408-2, ISO/IEC 15408-3 (conformant / extended)*) Problem: Conformance claim shall include CC conformance claim instead of ISO/IEC standards claim.
Type	ed
Resolution - Correction / Interpretation	CC claim (*Reference to the applied CC and CEM, CC Part 2, CC Part 3 (conformant / extended)*)
Status	ma
Remarks	Note that this errata is only applicable to CC Part 1 but not to ISO/IEC 15408-1 unlike other errata applicable to both CC Part 1 and ISO/IEC 15408-1.

ID	CC2022-P1-R1-0019
Date	2023-12-22
Reference	B.3.2.3.3 / 1st paragraph
Issue –	The TOE overview identifies the general type of a TOE addressed by the

Problem Description	PP, such as: firewall, VPN-firewall, smart card, crypto-modem, intranet, web server, database, web server, mobile device, and database, etc. The TOE type definition often includes a characterization of the TOE software and hardware boundaries. Problem: There are duplicated examples for the TOE type.
Type	ed
Resolution - Correction / Interpretation	The TOE overview identifies the general type of a TOE addressed by the PP, such as: firewall, VPN-firewall, smart card, crypto-modem, intranet, web server, database, and mobile device, etc. The TOE type definition often includes a characterization of the TOE software and hardware boundaries.
Status	ma
Remarks	-

ID	CC2022-P1-R1-0020
Date	2023-12-22
Reference	B.5.3 / 1st paragraph / 3rd bullet
Issue – Problem Description	— Security Requirements (APE_REQ) for Direct Rationale PPs. Problem: This shall be a title for a separated subclause.
Type	ed
Resolution - Correction / Interpretation	B.5.4 Security Requirements (APE_REQ) for Direct Rationale PPs
Status	ma
Remarks	-

ID	CC2022-P1-R1-0021
Date	2023-12-22
Reference	C.3.6.1 / 1st paragraph
Issue – Problem Description	The edition of relevant parts of the CC applicable to the PP-Configuration. Problem: The paragraph is incomplete.
Type	te
Resolution - Correction /	The conformance claim shall specify the edition of relevant parts of the CC applicable to the PP-Configuration.

Interpretation	
Status	ma
Remarks	-

ID	CC2022-P1-R1-0022
Date	2023-12-22
Reference	D.4.4
Issue – Problem Description	D.4.4 Security Problem Requirements (ASE_REQ) for Direct Rationale STs Problem: ASE_REQ is related to Security Requirements.
Type	ed/te
Resolution - Correction / Interpretation	D.4.4 Security Requirements (ASE_REQ) for Direct Rationale STs
Status	ma
Remarks	-

ID	CC2022-P1-R1-0023
Date	2023-12-22
Reference	4
Issue – Problem Description	Problem: “CC” and “CEM” is missing from the abbreviated terms list.
Type	ed
Resolution - Correction / Interpretation	CC Common Criteria CEM Common Evaluation Methodology
Status	ma
Remarks	Note that this errata is only applicable to CC Part 1 but not to ISO/IEC 15408-1 unlike other errata applicable to both CC Part 1 and ISO/IEC 15408-1. However, if possible, both documents should be considered to introduce abbreviated terms of “CC” and “CEM” for content level consistency.

Errata / Interpretation for CC:2022 Part 2

This section provides corrections and interpretations to CC:2022 Part 2 ([CC:2022-2]).

ID	CC2022-P2-R1-0001
Date	2023-12-22
Reference	3.13, 3.14
Issue – Problem Description	3.13 'TSF data data for the operation (3.5) of the target of evalution (TOE) upon which the enforcement of the security functional requirement (SFR) relies' 3.14 'user data data received or produced by the target of evaluation (TOE), which is meaningful to some external entity, but which do not affect the operation (3.5) of the TOE security funtionality (TSF)' Problem: Wrong reference to section 3.5 where the following definition of the term 'operation' is provided: 3.5 'operation ⟨on a CC Part 2 component⟩ modification or repetition of a component by assignment, iteration, refinement, or selection' In 3.13 and 3.14, the term 'operation' is not meant as 'operation on an SFR', but in the sense of 'operation of the TOE / TSF'.
Type	ed/te
Resolution - Correction / Interpretation	Remove the reference '(3.5)' in 3.13 and 3.14, and do not use italics for the entry 'operation' in 3.13 and 3.14. The term 'operation' is to be interpreted as 'operation of the TOE / TSF'.
Status	ma
Remarks	It could be the case that further terminology sections in CC / CEM are affected in similar manner, i.e. where terms with several definitions / meanings are specified in the CC / CEM and the wrong one is erroneously referenced in other terminology definitions.

ID	CC2022-P2-R1-0002

Date	2023-12-22
Reference	6 / EXAMPLE 7
Issue – Problem Description	EXAMPLE 7 An example of a subject is an inter-process communication. Problem: The inter-process “communication” is not a subject but an operation.
Type	te
Resolution - Correction / Interpretation	EXAMPLE 7 An example of an operation is an inter-process communication.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0003
Date	2023-12-22
Reference	6 / Paragraph above Figure 2
Issue – Problem Description	Therefore, some, but not all, authentication data ~~~. In the figure, the types of data typically encountered in the authentication data and the secrets subclauses are indicated. Problem: Previous text from CC V3.1 R5, Part 2 Paragraph #42, the highlighted part was “sections”. Here, update is not proper because it is not related to the specific subclause in the document.
Type	ed
Resolution - Correction / Interpretation	Therefore, some, but not all, authentication data ~~~. In the figure, the types of data typically encountered in the authentication data and the secrets sections are indicated.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0004
Date	2023-12-22
Reference	8.5.10
Issue – Problem Description	**8.5.10 FAU_SAR.3 Selectable audit review** Hierarchical to: No other components. Dependencies: FAU_SAR.1 Audit review

	Problem: “Component relationships” is missing.
Type	ed
Resolution - Correction / Interpretation	**8.5.10 FAU_SAR.3 Selectable audit review** **Component relationships** Hierarchical to: No other components. Dependencies: FAU_SAR.1 Audit review
Status	ma
Remarks	-

ID	CC2022-P2-R1-0005
Date	2023-12-22
Reference	10.2.3, 10.2.4
Issue – Problem Description	10.2.3 Management of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.5, CKM.6 10.2.4 Audit of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.5, CKM.6 Problem: Incomplete component identifier.
Type	ed/te
Resolution - Correction / Interpretation	10.2.3 Management of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.5, FCS_CKM.6 10.2.4 Audit of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.5, FCS_CKM.6
Status	ma
Remarks	-

ID	CC2022-P2-R1-0006
Date	2023-12-22
Reference	10.3.5, B.1
Issue – Problem Description	In [CC:2022-2], the SFR FCS_COP.1 seems to show problems concerning the listed dependencies, in particular the important dependency on FCS_CKM.6 (as successor of FCS_CKM.4 of the former CC V3.1 R5 and that was set for FCS_COP.1 in the past) is missing. In section 10.2.2, it is outlined: ‘NOTE Previous editions of this document specified FCS_CKM.4 which has been deprecated in this edition of this document. In order to preserve

	consistency when applying different editions of this document, the component number has not been re-used.' Instead, and as replacement for the former SFR FCS_CKM.4 'Cryptographic key destruction' the new SFR FCS_CKM.6 'Timing and event of cryptographic key destruction' on base of the old SFR FCS_CKM.4 has been incorporated into [CC:2022-2], refer to section 10.2.10. For the SFR FCS_COP.1, the dependency on FCS_CKM.4 was set in the past, but with the deletion of FCS_CKM.4 this dependency vanished and was not replaced by a dependency on the new corresponding SFR FCS_CKM.6. On content level, the dependency on the SFR for key destruction is meaningful and important.
Type	te
Resolution - Correction / Interpretation	The dependencies section for the SFR FCS_COP.1 in section 10.3.5 is replaced by: '[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction' Table B.3 in section B.1 shall be updated accordingly. Hint: For the deletion of the dependency on FCS_CKM.3 Cryptographic key access refer to CC2022-P2-R1-0007. It might be the case that further (crypto-related) SFRs show as well the missing dependency on the SFR FCS_CKM.6 caused by deletion of the SFR FCS_CKM.4, but that shall be handled in similar manner.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0007
Date	2023-12-22
Reference	10.3.5, 10.2.5, 10.2.6, B.1
Issue – Problem Description	In [CC:2022-2], the SFRs FCS_COP.1, FCS_CKM.1 and FCS_CKM.2 newly show the dependency on the SFR FCS_CKM.3 'Cryptographic key access'. What is the reasoning for such additional dependency? Is such dependency (in each case) deemed necessary?
Type	te

Resolution - Correction / Interpretation	The dependencies section for the SFR FCS_COP.1 in section 10.3.5 is replaced by: '[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction' Hint: For the addition of the dependency on FCS_CKM.6 Timing and event of cryptographic key destruction refer to CC2022-P2-R1-0006. The dependencies section for the SFR FCS_CKM.1 in section 10.2.5 is replaced by: '[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction' The dependencies section for the SFR FCS_CKM.2 in section 10.2.6 is replaced by: '[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation or FCS_CKM.5 Cryptographic key derivation]' Table B.3 in section B.1 shall be updated accordingly. It might be the case that further (crypto-related) SFRs require as well the dependency on FCS_CKM.3 which is not reasonable, but that can be handled in similar manner.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0008
Date	2023-12-22
Reference	10.2.10
Issue – Problem	For the SFR FCS_CKM.6, a dependency on the SFR FCS_CKM.5 as or-junction within the brackets seems to be missing. Not only cryptographic

Description	key generation as addressed in FCS_CKM.1, but cryptographic key derivation might as well be linked to key destruction.
Type	te
Resolution - Correction / Interpretation	The dependency section of the SFR FCS_CKM.6 should be supplemented as follows: 'Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation]'
Status	ma
Remarks	-

ID	CC2022-P2-R1-0009
Date	2023-12-22
Reference	10.5.3, 10.3.3
Issue – Problem Description	Section 10.5.3: The following actions can be considered for the management functions in FCS_RNG.1: […] Section 10.3.3: The following actions can be considered for the management functions in FCS: […] Problem: Management functions are defined in FMT.
Type	ed/te
Resolution - Correction / Interpretation	Section 10.5.3: The following actions can be considered for the management functions in FMT: […] Section 10.3.3: The following actions can be considered for the management functions in FMT: […]
Status	ma
Remarks	-

ID	CC2022-P2-R1-0010
Date	2023-12-22

Reference	11.3.5, 11.7.8, 11.7.9
Issue – Problem Description	Dependencies: FDP_***.* FMT_MSA.3 Static attribute Problem: Incomplete component name.
Type	ed/te
Resolution - Correction / Interpretation	Dependencies: FDP_***.* FMT_MSA.3 Static attribute initialization
Status	ma
Remarks	-

ID	CC2022-P2-R1-0011
Date	2023-12-22
Reference	11.13.6
Issue – Problem Description	Dependencies: FCS_COP.1. Problem: Incomplete component name.
Type	ed/te
Resolution - Correction / Interpretation	Dependencies: FCS_COP.1 Cryptographic Operation
Status	ma
Remarks	-

ID	CC2022-P2-R1-0012
Date	2023-12-22
Reference	11.14.8, 11.16.8
Issue – Problem Description	**11.14.8 FDP_SDI.2 Stored data integrity monitoring and action** Hierarchical to: FDP_SDI.1 Stored data integrity monitoring Dependencies: No dependencies. **11.16.8 FDP_UIT.3 Destination data exchange recovery** Hierarchical to: FDP_UIT.2 Source data exchange recovery Dependencies: [FDP_ACC.1 Subset access control, or

	FDP_IFC.1 Subset information flow control] [FDP_UIT.1 Data exchange integrity, or FTP_ITC.1 Inter-TSF trusted channel] Problem: “Components relationships” is missing.
Type	ed
Resolution - Correction / Interpretation	**11.14.8 FDP_SDI.2 Stored data integrity monitoring and action** **Component relationships** Hierarchical to: FDP_SDI.1 Stored data integrity monitoring Dependencies: No dependencies. **11.16.8 FDP_UIT.3 Destination data exchange recovery** **Component relationships** Hierarchical to: FDP_UIT.2 Source data exchange recovery Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FDP_UIT.1 Data exchange integrity, or FTP_ITC.1 Inter-TSF trusted channel]
Status	ma
Remarks	-

ID	CC2022-P2-R1-0013
Date	2023-12-22
Reference	12.6.5, 12.6.8
Issue – Problem Description	**12.6.5 Management of FIA_UAU.3, FIA_UAU.4, FIA_UAU.7** The following actions can be considered for the management functions in FMT: a) there are no management activities foreseen. **12.6.8 Management of FIA_UAU.7** The following actions can be considered for the management functions in FMT: a) the management of the rules for authentication. Problem: FIA_UAU.7 addresses protected authentication feedback. The management activity defined in section 12.6.8 is not related to FIA_UAU.7. And, section 12.6.5 states that FIA_UAU.7 has no management activities foreseen. This is inconsistent on content level. If the management activities for FIA_UAU.7 are described separately, section 12.6.8 shall be updated accordingly.

	Refer as well to CC2022-P2-R1-0014.
Type	te
Resolution - Correction / Interpretation	**12.6.5 Management of FIA_UAU.3, FIA_UAU.4** The following actions can be considered for the management functions in FMT: a) there are no management activities foreseen. **12.6.8 Management of FIA_UAU.7** The following actions can be considered for the management functions in FMT: a) the management of the limited feedback information provided to the user during the authentication.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0014
Date	2023-12-22
Reference	12.6.15
Issue – Problem Description	**12.6.15 Audit of FIA_UAU.7** The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST: a) well-formedness of rules regarding the semantics of rule-set; b) basic: verification of enforceability of rules. Problem: FIA_UAU.7 addresses protected authentication feedback. The auditable events defined in section 12.6.15 is not related to FIA_UAU.7. (cf. a) has no levels of detail regardless of the feasibility of the auditable event.) Refer as well to CC2022-P2-R1-0013.
Type	te
Resolution - Correction / Interpretation	**12.6.15 Audit of FIA_UAU.7** The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST: a) there are no auditable events foreseen.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0015

Date	2023-12-22
Reference	12.7.7
Issue – Problem Description	**12.7.7 FIA_UID.2 User identification before any action** Hierarchical to: FIA_UID.1 Timing of identification Dependencies: No dependencies. Problem: “Components relationships” missing.
Type	ed
Resolution - Correction / Interpretation	**12.7.7 FIA_UID.2 User identification before any action** **Components relationships** Hierarchical to: FIA_UID.1 Timing of identification Dependencies: No dependencies.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0016
Date	2023-12-22
Reference	13.9.11
Issue – Problem Description	**13.9.11 FMT_SMR.3 Assuming roles** Hierarchical to: No other components. Dependencies: FMT_SMR.1 Security roles Problem: “Components relationships” missing.
Type	ed
Resolution - Correction / Interpretation	**13.9.11 FMT_SMR.3 Assuming roles** **Components relationships** Hierarchical to: No other components. Dependencies: FMT_SMR.1 Security roles
Status	ma
Remarks	-

ID	CC2022-P2-R1-0017
Date	2023-12-22
Reference	15.1 / Figure 60, 15.6.2 / Figure 65

Issue – Problem Description	Problem: FPT_ITC family name error.
Type	ed/te
Resolution - Correction / Interpretation	FPT_ITC Confidentiality of exported TSF data
Status	ma
Remarks	-

ID	CC2022-P2-R1-0018
Date	2023-12-22
Reference	15.4, J.1, J.4.2.2
Issue – Problem Description	FPT_INI.1.1 The TOE shall provide an initialization function which is self-protected for integrity and authenticity. FPT_INI.1.2 The TOE initialization function shall ensure that certain properties hold on certain elements immediately before establishing the TSF in a secure initial state, as specified in Table 2: FPT_INI.1.3 The TOE initialization function shall detect and respond to errors and failures during initialization such that the TOE [selection: is halted, successfully completes initialization with [selection: reduced functionality, signaling error state, [assignment: list of actions]]. FPT_INI.1.4 The TOE initialization function shall only interact with the TSF in [assignment: defined methods] during initialization. Problem: FPT_INI.1 requires that “the TOE” provides an initialization function and “the TOE initialization function” ensures some functionalities regarding initialization. Usually part 2 security functional components is to be used as base for the security functional requirements of the TOE, therefore they shall be a part of the TSF. That’s why every functional element (except for FPT_INI.1.1 ~ FPT_INI.1.4) is expressed in the following form: “The TSF shall ~~”. Because the TOE may consist of both the TSF parts and the non-TSF parts, and the TSF parts are subject of evaluation. To clearly define the TSF parts as security functional requirements, FPT_INI shall be expressed in the same way as the other security functional

	components in part 2, as far as meaningful.
Type	te
Resolution - Correction / Interpretation	FPT_INI.1.1 The TOE shall provide a TSF initialization function which is self-protected for integrity and authenticity. FPT_INI.1.2 The TSF initialization function shall ensure that certain properties hold on certain elements immediately before establishing the TSF in a secure initial state, as specified in Table 2: […] FPT_INI.1.3 The TSF initialization function shall detect and respond to errors and failures during initialization such that the TOE [selection: *is halted, successfully completes initialization with [selection: reduced functionality, signaling error state, [assignment: list of actions]]*]. FPT_INI.1.4 The TSF initialization function shall only interact with the TSF in [assignment: *defined methods*] during initialization. Section 15.4.2: This family consists of only one component, Component FPT_INI.1. This component requires the TOE to provide a TSF initialization function that brings the TSF into a secure operational state at power-on. The TOE components related to TSF initialization are considered themselves part of the TSF, and analysed from that perspective. Hint: For the latter entry refer to ADV_ARC.1-3. Refer as well to CEM2022-R1-0119. Section J.4.2.2: In FPT_INI.1.2 the author of a PP, PP-Module, functional package or ST should list the properties and the elements to which they apply, respectively. […] In FPT_INI.1.3 the author of a PP, PP-Module, functional package or ST uses the selections and assignments to describe the behaviour of the TSF initialization function in the case that errors or other failures are encountered during the initialization. In FPT_INI.1.4 the author of a PP, PP-Module, functional package or ST uses the assignment to describe the methods by which the TSF initialization function interacts with the TSF. Section J.1: […] 3rd para, c) TSF initialization (FPT_INI), which addresses the initialization of the TSF into a correct and secure operational state; […]

Status	ma
Remarks	-

ID	CC2022-P2-R1-0019
Date	2023-12-22
Reference	16.3.5
Issue – Problem Description	**16.3.5 FRU_PRS.1 Limited priority of service** Hierarchical to: No other components. Dependencies: No dependencies. Problem: “Components relationships” missing.
Type	ed
Resolution - Correction / Interpretation	**16.3.5 FRU_PRS.1 Limited priority of service** **Components relationships** Hierarchical to: No other components. Dependencies: No dependencies.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0020
Date	2023-12-22
Reference	A.2.3.3 / 1st paragraph
Issue – Problem Description	The user notes contain additional information that is of interest to potential users of the family, that is PP, PP-Module, ST and functional package authors, and developers of TOEs incorporating the functional components. The presentation is informative and can cover warnings about limitations of use and areas where specific attention can be required when using the components. Problem: “User notes” has been changed into “User application notes”.
Type	ed
Resolution - Correction / Interpretation	The user application notes contain additional information that is of interest to potential users of the family, that is PP, PP-Module, ST and functional package authors, and developers of TOEs incorporating the functional components. The presentation is informative and can cover warnings about limitations of use and areas where specific attention can be required when using the components.

Status	ma
Remarks	-

ID	CC2022-P2-R1-0021
Date	2023-12-22
Reference	A.2.4.3 / 3rd paragraph
Issue – Problem Description	The application notes contain additional refinement in the form of narrative qualifications for a specific component. This refinement may pertain to user notes, and/or evaluator notes as described in A.2.3. The application notes may be used to explain the nature of the dependencies. Problem: “User notes” has been changed into “User application notes”.
Type	ed
Resolution - Correction / Interpretation	The application notes contain additional refinement in the form of narrative qualifications for a specific component. This refinement may pertain to user application notes, and/or evaluator notes as described in A.2.3. The application notes may be used to explain the nature of the dependencies.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0022
Date	2023-12-22
Reference	B.1 / 2nd paragraph
Issue – Problem Description	Each of the components that is a dependency of some other functional component is allocated a column. Each functional component is allocated a row. The value in the table cell indicates whether the column label component is a hierarchical requirement (indicated by an “H”). directly required (indicated by a cross “X”), indirectly required (indicated by a dash “-”), or optionally required (indicated by a “O”) by the row label component. Sets of optional requirements are indicated by using a subscript group, e.g. O^1 and O^2. Problem: A comma shall be used instead of a period. Examples for optional requirements indication are not subscript. There is no explicit explanation regarding the difference between group O^1 and O^2.
Type	ed/te
Resolution - Correction /	Each of the components that is a dependency of some other functional component is allocated a column. Each functional component is allocated a row. The value in the table cell indicates whether the column label

Interpretation	component is a hierarchical requirement (indicated by an "H"), directly required (indicated by a cross "X"), indirectly required (indicated by a dash "-"), or optionally required (indicated by a "O") by the row label component. Sets of optional requirements are indicated by using an entry of type O^x (e.g. O^1) whereby an SFR with such entry requires at minimum only one of the SFRs contained in that O^x-set.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0023
Date	2023-12-22
Reference	B.1 / Table B.4
Issue – Problem Description	Problem: Table B.4 indicates that FDP_DAU.2 is hierarchical to FDP_ACC.1 instead of FDP_DAU.1.
Type	te
Resolution - Correction / Interpretation	Table B.4 shall be updated accordingly.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0024
Date	2023-12-22
Reference	C.3.1.2 / 1st paragraph
Issue – Problem Description	FAU_GEN.1.1 has a dependency on FPT_STM.1 Reliable time stamps. If correctness of time is not an issue for this TOE, elimination of this dependency can be justified by the author of a PP, PP-Module, functional package or ST. Problem: Dependency relationship is defined at the level of functional component not of functional element.
Type	ed/te
Resolution - Correction / Interpretation	FAU_GEN.1 has a dependency on FPT_STM.1 Reliable time stamps. If correctness of time is not an issue for this TOE, elimination of this dependency can be justified by the author of a PP, PP-Module, functional package or ST.

Status	ma
Remarks	-

ID	CC2022-P2-R1-0025
Date	2023-12-22
Reference	C.7.1.1 / 3rd paragraph
Issue – Problem Description	FAU_STG.1.1 is dependent upon FTP_ITC.1 Inter-TSF trusted channel, if "transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC" is not selected then the author of a PP, PP-Module, functional package or ST can satisfy the dependency by providing the rationale explaining why it was not selected. Problem: Dependency relationship is defined at the level of functional component not of functional element.
Type	ed/te
Resolution - Correction / Interpretation	FAU_STG.1 is dependent upon FTP_ITC.1 Inter-TSF trusted channel, if "transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC" is not selected then the author of a PP, PP-Module, functional package or ST can satisfy the dependency by providing the rationale explaining why it was not selected.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0026
Date	2023-12-22
Reference	C.7.3.2
Issue – Problem Description	Problem: Since FAU_STG.3.2 includes selection operation, C.7.3.2 shall provide proper application note for that operation.
Type	te
Resolution - Correction / Interpretation	Add the following sentence: In FAU_STG.3.2, the author of PP, PP-module, functional package or ST should specify whether the TSF shall prevent or only be able to detect modifications of the stored audit data in the audit trail. Only one of these options may be chosen.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0027
Date	2023-12-22
Reference	C.7.4, C.7.5
Issue – Problem Description	C.7.4 FAU_STG.4 Prevention of audit data loss C.7.5 FAU_STG.5 Action in case of possible audit data loss Problem: Component identifiers shall be corrected regarding their numbers and short names. And all subclauses below C.7.4 and C.7.5 shall be exchanged. Note that this errata shall be resolved together with CC2022-P2-R1-0028.
Type	ed/te
Resolution - Correction / Interpretation	C.7.4 FAU_STG.4 Action in case of possible audit data loss C.7.5 FAU_STG.5 Prevention of audit data loss
Status	ma
Remarks	-

ID	CC2022-P2-R1-0028
Date	2023-12-22
Reference	C.7.5.2 / 1st paragraph, 2nd paragraph, C.7.5.1 / 1st paragraph, C.7.4.1 / 1st paragraph, C.7.5.1 / 1st paragraph
Issue – Problem Description	In FAU_STG.5 Prevention of audit data loss, the author of a PP, PP-Module, functional package or ST should indicate the pre-defined limit. If the management functions indicate that this number can be changed by the authorized user, this value is the default value. The author of a PP, PP-Module, functional package or ST can choose to let the authorized user define this limit. In FAU_STG.5 Prevention of audit data loss, the author of a PP, PP-Module, functional package or ST should specify actions that should be taken in case of imminent audit storage failure indicated by exceeding the threshold. Actions can include informing an authorized user. C.7.4.1 Component rationale and application notes This component specifies the behaviour of the TOE if the audit trail is full: either audit records are ignored, or the TOE is frozen such that no audited events can take place. The requirement also states that no matter how the requirement is instantiated, the authorized user with specific rights to this effect, can continue to generate audited events (actions). The reason is that

	otherwise the authorized user can not even reset the TOE. Consideration should be given to the choice of the action to be taken by the TSF in the case of audit storage exhaustion, as ignoring events, which provides better availability of the TOE, will also permit actions to be performed without being recorded and without the user being accountable. C.7.5.1 Component rationale and application notes This component requires that actions will be taken when the audit trail exceeds certain pre-defined limits. Problem: The application note for both operations are related to FAU_STG.4.1, so both sentences shall be updated accordingly and shifted to section C.7.4.2. As well the entries in section C.7.5.1 belong to FAU_STG.4 and in section C.7.4.1 to FAU_STG.5. Note that this errata shall be resolved together with CC2022-P2-R1-0027.
Type	ed/te
Resolution - Correction / Interpretation	In FAU_STG.4.1, the author of a PP, PP-Module, functional package or ST should indicate the pre-defined limit. If the management functions indicate that this number can be changed by the authorized user, this value is the default value. The author of a PP, PP-Module, functional package or ST can choose to let the authorized user define this limit. In FAU_STG.4.1, the author of a PP, PP-Module, functional package or ST should specify actions that should be taken in case of imminent audit storage failure indicated by exceeding the threshold. Actions can include informing an authorized user. Incorporate proposed new texts on FAU_STG.4.1 in section C.7.4.2, shift existing texts on FAU_STG.5.1 from section C.7.4.2 to section C.7.5.2. Switch text sections C.7.4.1 and C.7.5.1. So, all in all: C.7.4 FAU_STG.4 Action in case of possible audit data loss C.7.4.1 Component rationale and application notes This component requires that actions will be taken when the audit trail exceeds certain pre-defined limits. C.7.4.2 Operations In FAU_STG.4.1, the author of a PP, PP-Module, functional package or ST should indicate the pre-defined limit. If the management functions indicate that this number can be changed by the authorized user, this value is the default value. The author of a PP, PP-Module, functional package or ST can choose to let the authorized user define this limit. EXAMPLE In the case that an authorized user defines the limit, an example of the assignment can be “an authorized user set limit”. In FAU_STG.4.1, the author of a PP, PP-Module, functional package or ST should specify actions that should be taken in case of imminent audit storage failure indicated by exceeding the threshold. Actions can include

	informing an authorized user. C.7.5 FAU_STG.5 Prevention of audit data loss C.7.5.1 Component rationale and application notes This component specifies the behaviour of the TOE if the audit trail is full: either audit records are ignored, or the TOE is frozen such that no audited events can take place. The requirement also states that no matter how the requirement is instantiated, the authorized user with specific rights to this effect, can continue to generate audited events (actions). The reason is that otherwise the authorized user can not even reset the TOE. Consideration should be given to the choice of the action to be taken by the TSF in the case of audit storage exhaustion, as ignoring events, which provides better availability of the TOE, will also permit actions to be performed without being recorded and without the user being accountable. C.7.5.2 Operations In FAU_STG.5.1, the author of a PP, PP-Module, functional package or ST should select whether the TSF shall ignore audited actions, or whether it should prevent audited actions from happening, or whether the oldest audit records should be overwritten when the TSF can no longer store audit records. Only one of these options may be chosen. In FAU_STG.5.1, the author of a PP, PP-Module, functional package or ST should specify other actions that should be taken in case of audit storage failure, such as informing the authorized user. If there is no other action to be taken in case of audit storage failure, this assignment can be completed with “none”.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0029
Date	2023-12-22
Reference	D.2.2.1, D.2.3.1, D.3.2.1, D.3.3.1
Issue – Problem Description	D.2.2.1 User application notes There are no user application notes specified for this component. D.2.3.1 User application notes There are no user application notes specified for this component. D.3.2.1 User application notes There are no user application notes specified for this component. D.3.3.1 User application notes There are no user application notes specified for this component.

	Problem: The title shall be “Component rationale and application notes” according to the A.2.4.
Type	ed
Resolution - Correction / Interpretation	D.2.2.1 Component rationale and application notes There are no component rationale and application notes specified for this component. D.2.3.1 Component rationale and application notes There are no component rationale and application notes specified for this component. D.3.2.1 Component rationale and application notes There are no component rationale and application notes specified for this component. D.3.3.1 Component rationale and application notes There are no component rationale and application notes specified for this component.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0030
Date	2023-12-22
Reference	D.3.1 / EXAMPLE 1
Issue – Problem Description	EXAMPLE 1 An example of a receipt is a digital signature. Problem: A digital signature is an example of evidence of receipt.
Type	te
Resolution - Correction / Interpretation	EXAMPLE 1 An example of evidence of receipt is a digital signature.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0031
Date	2023-12-22

Reference	E.2.1 / EXAMPLE 1
Issue – Problem Description	EXAMPLE 1 — backup; — escrow; — archive; — recovery. Problem: EXAMPLE 1 is specific to key access. So, it shall mention that these examples are related to key access.
Type	ed/te
Resolution - Correction / Interpretation	EXAMPLE 1 Examples of key access include: — backup; — escrow; — archive; — recovery.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0032
Date	2023-12-22
Reference	E.2.1 / last paragraph
Issue – Problem Description	Typically, random numbers are used to generate cryptographic keys. If this is the case, then FCS_CKM.1 Cryptographic key generation should be used instead of the component FIA_SOS.2 TSF Generation of secrets. In cases where random number generation is required for purposes other than for the generation of cryptographic keys, the component FIA_SOS.2 TSF Generation of secrets should be used. Problem: CC:2022 introduced FCS_RBG and FCS_RNG. So, the last paragraph (may come from CC V3.1 R5 which had no security functional component related to random bit/number generation) needs to be revised.
Type	te
Resolution - Correction / Interpretation	Typically, random numbers are used to generate cryptographic keys, and hereby FCS_RNG.1 or FCS_RBG.1 respectively for random number / bit generation should be used. Furthermore, in case of cryptographic key generation, FCS_CKM.1 Cryptographic key generation should be used. In cases where random number generation is required for purposes other than for the generation of cryptographic keys, the component FIA_SOS.2 TSF Generation of secrets can additionally be used.

Status	ma
Remarks	-

ID	CC2022-P2-R1-0033
Date	2023-12-22
Reference	E.2.6.2 Operations
Issue – Problem Description	There are no operations specified for this component. Problem: There exist 5 assignment operations in FCS_CKM.5.1. So, E.2.6.2 shall provide application notes on those operations.
Type	te
Resolution - Correction / Interpretation	Add the following sentences: In FCS_CKM.5.1, the author of a PP, PP-Module, functional package or ST should specify the type of cryptographic key to be derived. In FCS_CKM.5.1, the author of a PP, PP-Module, functional package or ST should specify input parameters associated with the key derivation for a specified type of key. In FCS_CKM.5.1, the author of a PP, PP-Module, functional package or ST should specify key derivation algorithm to be used. In FCS_CKM.5.1, the author of a PP, PP-Module, functional package or ST should specify the cryptographic key sizes to be derived. The key sizes specified should be appropriate for the algorithm and its intended use. In FCS_CKM.5.1, the author of a PP, PP-Module, functional package or ST should specify the assigned standard that documents the method used to derive cryptographic keys. The assigned standard may comprise none, one or more actual standards publications, for example, from international, national, industry or organizational standards.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0034
Date	2023-12-22
Reference	E.2.7.2 Operations
Issue – Problem Description	Problem: There are 1 selection operation and 2 assignment operations in FCS_CKM.6.1 and 2 assignment operations in FCS_CKM.6.2. But currently E.2.7.2 provides application notes for some of them. So, E.2.7.2 shall provide application notes on all operations in FCS_CKM.6.1 and FCS_CKM.6.2.

Type	te
Resolution - Correction / Interpretation	*<Update E.2.7.2>* **E.2.7.2 Operations** In FCS_CKM.6.1, the author of a PP, PP-Module, functional package or ST should provide a list of cryptographic keys and keying material that should be destroyed under certain circumstances. In FCS_CKM.6.1, the author of a PP, PP-Module, functional package or ST should select the circumstances of the destruction of keys or keying material. It can be chosen to destroy keys or keying material in case that these are no longer needed or to specify other circumstances for their destruction, e.g. the destruction of a key on reaching the limit of an error usage counter assigned to that key. In FCS_CKM.6.2, the author of a PP, PP-Module, functional package or ST should provide the cryptographic key destruction method and the list of standards specifying the cryptographic key destruction method. The assigned list of standards may comprise none, one or more actual standards publications, for example, from international, national, industry or organisational standards.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0035
Date	2023-12-22
Reference	E.4.2.2 Operations
Issue – Problem Description	Problem: There are several selection and assignment operations in FCS_RBG.1.1 ~ FCS_RBG.1.3. So, E.4.2.2 shall provide application notes on all operations in FCS_RBG.1.1 ~ FCS_RBG.1.3. On the other hand, “E.4.2.1 Component rationale and application notes” provides some application notes on operations. If possible, theses should be considered relocated in “E.4.2.2 Operation”.
Type	te
Resolution - Correction / Interpretation	*<Update E.4.2.1 and E.4.2.2>* Refer as well to CC2022-P2-R1-0059. **E.4.2.1 Component rationale and application notes** For FCS_RBG.1, these dependencies shall always be met. CC:2022, Part 1, 8.3 c) allows a justification to be provided if a dependency is not met is not allowed for this component. The entropy source could be a raw noise source or conditioned entropy.

	Reseeding is the typical mechanism for updating the DRBG state and means that additional entropy is provided to the DRBG. If reseeding is not feasible, the TSF should uninstantiate and re-instatiate DRBGs rather than produce output that is of insufficient quality. "Uninstantiate" means that the internal state of the DRBG is no longer available for use. The situation "never" should be selected only if the DRBG cannot be reseeded or uninstantiated. The situation "on demand" indicates that there is an interface to trigger reseeding or uninstantiating of the DRBG, whether internal to the TOE or presented as a TSFI (e.g. an API call). The situation "on the condition" allows the PP/ST author to specify application-specific conditions for reseeding. The list of standards should specify the reseed interval, and the process for reseeding. This assignment should be "None" if the situation is "never." Health tests for the DRBG are specified in FPT_TST.1. NOTE If a TOE needs to protect the DRBG state to avoid the possibility that knowledge of this state can compromise a key or keying material derived from its output, then the PP/ST author will include DRBG entropy input, seed input, and internal state of the DRBG in the assignment in an instance of FCS_CKM.6.1. This applies particularly where neither 'reseeding' nor 're-instantiating' apply in the first selection of FCS_RBG.1.3 (and therefore where a different method of destruction needs to be specified). **E.4.2.2 Operations** In FCS_RBG.1.1, the author of a PP, PP-Module, functional package or ST should specify the DRBG algorithm to be used. EXAMPLE Examples of typical DRBG algorithms include, but are not limited to, CTR_DRBG, Hash_DRBG, HMAC_DRBG. In FCS_RBG.1.1, the author of a PP, PP-Module, functional package or ST should specify the assigned standard that documents how the identified DRBG algorithm is performed. The assigned standard may comprise one or more actual standards publications, these may include standards from international, national, industry or organizational standards. In FCS_RBG.1.2, the author of a PP, PP-Module, functional package or ST should specify the entropy source or the TSF interface for obtaining entropy by providing the name. EXAMPLE Examples of typical TSF entropy sources include, but are not limited to, Jitter, IRQs, CPU timing differences. In FCS_RBG.1.3, the author of a PP, PP-Module, functional package or ST should specify the entropy source or the TSF interface for obtaining entropy by providing the name. In FCS_RBG.1.3, the author of a PP, PP-Module, functional package or ST should specify the condition or the time interval for the update of the DRBG state. In FCS_RBG.1.3, the author of a PP, PP-Module, functional package or ST

	should specify the assigned standard that documents how the identified DRBG state is updated. The assigned standard may comprise one or more actual standards publications, these may include standards from international, national, industry or organizational standards. When the first selection in FCS_RBG.1.3 is completed with „reseeding“, the standard should match the one specified in FCS_RBG.1.1. When the first selection in FCS_RBG.1.3 is completed with „uninstantiating and re-instantiating“, the assignment should be completed with „none“.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0036
Date	2023-12-22
Reference	E.4.3.2 Operations
Issue – Problem Description	There are no operations specified for this component. Problem: There is an assignment operation in FCS_RBG.2.1. So, E.4.3.2 shall provide application notes on all operations in FCS_RBG.2.1.
Type	te
Resolution - Correction / Interpretation	*<Update E.4.3.2>* Refer as well to CC2022-P2-R1-0059. **E.4.3.2 Operations** In FCS_RBG.2.1, the author of a PP, PP-Module, functional package or ST should specify the minimum input length greater than zero in bits by providing a number.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0037
Date	2023-12-22
Reference	E.4.4.2 Operations
Issue – Problem Description	There are no operations specified for this component. Problem: There are several operations including assignment and selection in

	FCS_RBG.3.1. So, E.4.4.2 shall provide application notes on all operations in FCS_RBG.3.1.
Type	te
Resolution - Correction / Interpretation	*<Update E.4.4.2>* Refer as well to CC2022-P2-R1-0059. **E.4.4.2 Operations** In FCS_RBG.3.1, the author of a PP, PP-Module, functional package or ST should specify the TSF entropy source by providing the name. In FCS_RBG.3.1, the author of a PP, PP-Module, functional package or ST should specify the number of bits of min-entropy for seeding the DRBG. The bits of min-entropy have to be declared regardless of the number of bits supplied.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0038
Date	2023-12-22
Reference	E.4.5
Issue – Problem Description	Problem: Subclause “E.4.5.2 Operations” is missing in E.4.5. There are several operations including assignment and selection in FCS_RBG.4.1. So, E.4.5.2 shall be introduced to provide application notes on all operations in FCS_RBG.4.1.
Type	te
Resolution - Correction / Interpretation	*<Introduce E.4.5.2>* Refer as well to CC2022-P2-R1-0059. **E.4.5.2 Operations** In FCS_RBG.4.1, the author of a PP, PP-Module, functional package or ST should specify the number of TSF software-based and/or TSF hardware-based entropy sources.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0039

Date	2023-12-22
Reference	Between E.4.5 and E.4.6
Issue – Problem Description	Problem: Application notes for FCS_RBG.5 is missing from E.4.
Type	te
Resolution - Correction / Interpretation	*<Introduce application notes for FCS_RBG.5 between FCS_RBG.4 and FCS_RBG.6.>* Refer as well to CC2022-P2-R1-0059. **E.4.6 FCS_RBG.5 Random bit generation (combining entropy sources)** **E.4.6.1 Component rationale and application notes** This component addresses operations used for combining multiple entropy sources to obtain min-entropy for further processing. Input to the combining operation can come from the TSF entropy source(s) specified in FCS_RBG.3.1 and/or FCS_RBG.4.1 and/or from the TSF interface(s) for obtaining entropy specified in FCS_RBG.2.1. **E.4.6.2 Operations** In FCS_RBG.5.1, the author of a PP, PP-Module, functional package or ST should specify the operation to combine the output from the TSF entropy source(s) and/or input from the TSF interface(s) for obtaining entropy. EXAMPLE Examples of typical combining operations include, but are not limited to, XORing or hashing. In FCS_RBG.5.1, the author of a PP, PP-Module, functional package or ST should specify the assigned standard that documents how the entropy input is combined. The assigned standard may comprise one or more actual standards publications, these may include standards from international, national, industry or organizational standards. In FCS_RBG.5.1, the author of a PP, PP-Module, functional package or ST should specify the number of bits of the resulting min-entropy.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0040
Date	2023-12-22
Reference	E.4.6.2 Operations
Issue – Problem	Other interface types can be a service over a network interface. EXAMPLE Ethernet, wireless.

Description	Problem: The application note should be described according to the other security functional components. There are 1 selection and 1 assignment operation in FCS_RBG.6.1. So, E.4.6.2 shall provide application notes on all operations in FCS_RBG.6.1.
Type	te
Resolution - Correction / Interpretation	*<Update E.4.6.2.>* Refer as well to CC2022-P2-R1-0059. Due to CC2022-P2-R1-0039 new section number E.4.7. **E.4.7 FCS_RBG.6 Random bit generation service** **E.4.7.1 Component rationale and application notes** Specifying the interface type is important for developing evaluation activities and important information for an external instance requesting the DRBG service from the TOE. **E.4.7.2 Operations** In FCS_RBG.6.1, the author of a PP, PP-Module, functional package or ST should either select the interface type „hardware“ or „software“ or should specify another interface type. In FCS_RBG.6.1, the author of a PP, PP-Module, functional package or ST should specify other interface types, if applicable. The assignment inside of the selection is introduced to allow other or more specific interface types than just “hardware” or “software”. Other interface types can be a service over a network interface. EXAMPLE Ethernet, wireless.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0041
Date	2023-12-22
Reference	E.5.1
Issue – Problem Description	NOTE In some cases, certification bodies can apply policies in regard to the selection of random bit generators. (See CEM, A.6 n). Problem: E.5 is regarding random number generator instead of random bit generator.

Type	ed/te
Resolution - Correction / Interpretation	NOTE In some cases, certification bodies can apply policies in regard to the selection of random number generators. (See CEM, A.6 n).
Status	ma
Remarks	-

ID	CC2022-P2-R1-0042
Date	2023-12-22
Reference	E.5.2.2 Operations
Issue – Problem Description	EXAMPLEs and NOTEs should be revised in terms of consistency with defined selection and assignment operations of FCS_RNG.1.1 and FCS_RNG.1.2 in 10.5.5. (Especially, selection and assignment operations used in EXAMPLEs are new ones which are not from FCS_RNG.1.1 and FCS_RNG.1.2.)
Type	te
Resolution - Correction / Interpretation	*<Update E.5.2.2>* **E.5.2.2 Operations** In FCS_RNG.1.1 the author of a PP, PP-Module, functional package or ST should specify the type of random number generator as physical, non-physical true, deterministic, hybrid physical or hybrid deterministic. NOTE 1 A physical random number generator (RNG) produces random numbers using a noise source based on physical random processes. A non-physical true RNG uses a noise source based on non-physical random processes like human interaction (key strokes, mouse movement). A deterministic RNG uses a random seed to produce a pseudorandom output. A hybrid physical or hybrid deterministic RNG combines the principles of physical and deterministic RNGs. A hybrid physical RNG produces at least the amount of entropy the RNG output may contain while the internal state of a hybrid deterministic RNG output contains fresh entropy but less than the output of an RNG may contain. In FCS_RNG.1.1 the author of a PP, PP-Module, functional package or ST should specify the list of security capabilities provided by the random number generator of the TOE. NOTE 2 In the case of a PP, PP-Module or functional package, FCS_RNG.1.1 can be completed with a more restrictive language such as: – [assignment: list of additional security capabilities]; – [selection: security capability_1, …, security capability_n]; – mixtures of such selections and assignments within the list of security capabilities.

	EXAMPLE 1 Examples of security capabilities include: – a total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output; – if a total failure of the entropy source occurs while the RNG is being operated, the RNG [selection: prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source, generates the internal randomnumbers with a post-processing algorithm of class DRG.2 as long as its internal state entropy guarantees the claimed output entropy]; – the online test detects non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected; – the online test procedure be effective to detect non-tolerable weaknesses of the random numbers soon; – the online test procedure checks the quality of the raw random number sequence. It is triggered [selection: externally, at regular intervals, continuously, applied upon specified internal events]. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time; – failure or severe degradation of the noise source be detectable; – continuous tests or other mechanisms in the entropy source protect against producing output during malfunctions. In FCS_RNG.1.2 the author of a PP, PP-Module, functional package or ST should specify the type of random output as bits, octets of bits or numbers whereby in the latter case the format of the numbers has to be specified. In FCS_RNG.1.2 the author of a PP, PP-Module, functional package or ST should specify an appropriate quality metric for the random output. NOTE 3 In the case of a PP, PP-Module or functional package, FCS_RNG.1.2 can be completed with a more restrictive language such as: – [selection: defined quality metric_1, …, defined quality metric_n]; – [assignment: a defined quality metric]; – mixtures of such selections and assignments within the quality metric. NOTE 4 The “quality metric” can include both qualitative metric and quantitative metric. EXAMPLE 2 Examples of quality metrics include – test procedure A [assignment: additional standard test suites] does not distinguish the internal random numbers from output sequences of an

	ideal RNG; NOTE 5 The assignment for additional standard statistical test suite may be empty. – the average Shannon entropy per internal random bit exceeds 0.998; – each output bit is independent of all other output bits; – [selection: full entropy output, [assignment: bias and entropy rate of the output]].
Status	ma
Remarks	-

ID	CC2022-P2-R1-0043
Date	2023-12-22
Reference	F.9.1
Issue – Problem Description	EXAMPLE 2 Cryptographic checksum. Problem: It is unclear what the example is about.
Type	te
Resolution - Correction / Interpretation	EXAMPLE 2 An example of security attribute is a cryptographic checksum.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0044
Date	2023-12-22
Reference	G.2.2.2 / 1st paragraph ~ 4th paragraph
Issue – Problem Description	In FIA_AFL.1 Authentication failure handling, the author of a PP, PP-Module, functional package or ST should select either the assignment of a positive integer, or the phrase “an administrator configurable positive integer” specifying the range of acceptable values. In FIA_AFL.1 Authentication failure handling, the author of a PP, PP-Module, functional package or ST should specify the authentication events. In FIA_AFL.1 Authentication failure handling, if the assignment of a positive integer is selected, the author of a PP, PP-Module, functional package or ST should specify the default number (positive integer) of unsuccessful authentication attempts that, when met or surpassed, will trigger the events.

	In FIA_AFL.1 Authentication failure handling, if an administrator configurable positive integer is selected, the author of a PP, PP-Module, functional package or ST should specify the range of acceptable values from which the administrator of the TOE may configure the number of unsuccessful authentication attempts. The number of authentication attempts should be less than or equal to the upper bound and greater or equal to the lower bound values. Problem: Operation should refer to the related element instead of component (refer to the operation of FIA_AFL.1.2 part.)
Type	ed/te
Resolution - Correction / Interpretation	In FIA_AFL.1.1, the author of a PP, PP-Module, functional package or ST should select either the assignment of a positive integer, or the phrase “an administrator configurable positive integer” specifying the range of acceptable values. In FIA_AFL.1.1, the author of a PP, PP-Module, functional package or ST should specify the authentication events. In FIA_AFL.1.1, if the assignment of a positive integer is selected, the author of a PP, PP-Module, functional package or ST should specify the default number (positive integer) of unsuccessful authentication attempts that, when met or surpassed, will trigger the events. In FIA_AFL.1.1, if an administrator configurable positive integer is selected, the author of a PP, PP-Module, functional package or ST should specify the range of acceptable values from which the administrator of the TOE may configure the number of unsuccessful authentication attempts. The number of authentication attempts should be less than or equal to the upper bound and greater or equal to the lower bound values.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0045
Date	2023-12-22
Reference	G.2.2.2 / The last bullet of EXAMPLE
Issue – Problem Description	EXAMPLE Examples of these authentication events are: — the unsuccessful authentication attempts since the last successful authentication for the indicated user identity; — the unsuccessful authentication attempts since the last successful authentication for the current terminal; — the number of unsuccessful authentication attempts in the last 10 min; — at least one authentication event shall be specified.

	Problem: The last bullet of the EXAMPLE is not an example of authentication events, but application note to complete operation.
Type	ed/te
Resolution - Correction / Interpretation	EXAMPLE Examples of these authentication events are: — the unsuccessful authentication attempts since the last successful authentication for the indicated user identity; — the unsuccessful authentication attempts since the last successful authentication for the current terminal; — the number of unsuccessful authentication attempts in the last 10 min. At least one authentication event shall be specified.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0046
Date	2023-12-22
Reference	G.6.8.2 / 1st paragraph
Issue – Problem Description	In FIA_UAU.7 Protected authentication feedback, the author of a PP, PP-Module, functional package or ST should specify the feedback related to the authentication process that will be provided to the user. Problem: Operation should refer to the related element instead of component (refer to the operation of others.)
Type	ed/te
Resolution - Correction / Interpretation	In FIA_UAU.7.1, the author of a PP, PP-Module, functional package or ST should specify the feedback related to the authentication process that will be provided to the user.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0047
Date	2023-12-22
Reference	J.2.1 / last paragraph
Issue – Problem	FPT_EMS.1.1 Limit of Emissions requires the TOE to not emit intelligible emissions enabling access to TSF data or user data.

Description	Problem: An element does not have short name in Part 2. So, this shall be a component with short name.
Type	ed/te
Resolution - Correction / Interpretation	FPT_EMS.1 Limit of Emissions requires the TOE to not emit intelligible emissions enabling access to TSF data or user data.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0048
Date	2023-12-22
Reference	J.2.2.1 / 2nd paragraph
Issue – Problem Description	The FPT_EMS.1.1 Table found as part of the FPT_EMS.1.1 Limit of Emissions element shall be completed by the author of a PP, PP-Module, functional package or ST. Each row, which can be identified using the "Identifier", provides a set of assignments for completing the SFR, allowing the author of a PP, PP-Module, functional package or ST to specify the requirements for TOE emanation protection for various different combinations of emissions, interfaces, TSF data and user data. Problem: An element does not have short name in Part 2.
Type	ed/te
Resolution - Correction / Interpretation	The FPT_EMS.1.1 Table found as part of the FPT_EMS.1 Limit of Emissions element shall be completed by the author of a PP, PP-Module, functional package or ST. Each row, which can be identified using the "Identifier", provides a set of assignments for completing the SFR, allowing the author of a PP, PP-Module, functional package or ST to specify the requirements for TOE emanation protection for various different combinations of emissions, interfaces, TSF data and user data.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0049
Date	2023-12-22
Reference	J.2.2.2 Operations
Issue – Problem	There are no operations specified for this component.

Description	Problem: There are several assignment operations in FPT_EMS.1.1. So, J.2.2.2 shall provide application notes on all operations in FPT_EMS.1.1. On the other hand, “J.2.2.1 Component rationale and application notes” provides some application notes on operations. If possible, theses should be considered relocated in “J.2.2.2 Operation”.
Type	te
Resolution - Correction / Interpretation	*<Update J.2.2.2>* Section J.2.2.1: The text sections “The FPT_EMS.1.1 Table found as part of the FPT_EMS.1.1 Limit of Emissions element shall be completed by the author of a PP, PP-Module, functional package or ST. Each row, which can be identified using the “Identifier”, provides a set of assignments for completing the SFR, allowing the author of a PP, PP-Module, functional package or ST to specify the requirements for TOE emanation protection for various different combinations of emissions, interfaces, TSF data and user data. It is not expected that an author enters all types of emissions and types of attack surfaces (etc.) in one row.” are moved (with slight adaptation) from section J.2.2.1 to section J.2.2.2. Furthermore, the EXAMPLE section with its two bullets is deleted. So, all in all section J.2.2.1 contains only the following text section: Specifying this component requires a relational representation of any combination of TSF data and/or user data in relation to any emission combined with the attack surface. Data, emissions and attack surfaces may be typified. Section J.2.2.2: The sentence “There are no operations specified for this component.” is replaced by: The FPT_EMS.1.1 Table found as part of the FPT_EMS.1.1 element should be completed by the author of a PP, PP-Module, functional package or ST. Each row, which can be identified using the “Identifier”, provides a set of assignments for completing the SFR, allowing the author of a PP, PP-Module, functional package or ST to specify the requirements for TOE emanation protection for various different combinations of emissions, attack surface, TSF data and user data. In FPT_EMS.1.1, the author of a PP, PP-Module, functional package or ST should specifiy for each assignment the list of types of emissions that have been treated, the list of types of attack surfaces under consideration for attacks based on emissions, the list of types of TSF data protected by emissions treatment, and the list of types of user data protected by

	emissions treatment. This should be done in table form whereby each table row specifies a specific combination of those lists of types of emissions, attack surface, TSF data and user data. Hereby, it is not expected that an author enters all types of emissions and types of attack surface (etc.) in one row. EXAMPLE – Emission and attack surface can be of physical or logical type. – Types of emissions can include audio frequencies, radio frequencies, information on power consumption, electromagnetic radiation, and timing information. – Types of attack surface can include TOE interfaces, physical ports, IC boundaries, electronic components, and logical access.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0050
Date	2023-12-22
Reference	J.5.2.2 / 2nd paragraph
Issue – Problem Description	In FPT_ITA.1.1, the PP, PP-Module, functional package or ST should specify the availability metric for the applicable TSF data. Problem: “author of a” is missing.
Type	ed/te
Resolution - Correction / Interpretation	In FPT_ITA.1.1, the author of a PP, PP-Module, functional package or ST should specify the availability metric for the applicable TSF data.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0051
Date	2023-12-22
Reference	J.7.2.2 / 1st paragraph, 2nd paragraph
Issue – Problem Description	In FPT_ITI.1.1, the PP, PP-Module, functional package or ST should specify the modification metric that the detection mechanism satisfies. This modification metric shall specify the desired strength of the modification detection. In FPT_ITI.1.2, the PP, PP-Module, functional package or ST should specify the actions to be taken if a modification of TSF data has been

	detected. An example of an action is: “ignore the TSF data and request the originating trusted product to send the TSF data again”. Problem: “author of a” is missing.
Type	ed/te
Resolution - Correction / Interpretation	In FPT_ITI.1.1, the author of a PP, PP-Module, functional package or ST should specify the modification metric that the detection mechanism satisfies. This modification metric shall specify the desired strength of the modification detection. In FPT_ITI.1.2, the author of a PP, PP-Module, functional package or ST should specify the actions to be taken if a modification of TSF data has been detected. An example of an action is: “ignore the TSF data and request the originating trusted product to send the TSF data again”.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0052
Date	2023-12-22
Reference	J.7.3.2 / 1st paragraph, 2nd paragraph
Issue – Problem Description	In FPT_ITI.2.1, the PP, PP-Module, functional package or ST should specify the modification metric that the detection mechanism satisfies. This modification metric shall specify the desired strength of the modification detection. In FPT_ITI.2.2, the PP, PP-Module, functional package or ST should specify the actions to be taken if a modification of TSF data has been detected. Problem: “author of a” is missing.
Type	ed/te
Resolution - Correction / Interpretation	In FPT_ITI.2.1, the author of a PP, PP-Module, functional package or ST should specify the modification metric that the detection mechanism satisfies. This modification metric shall specify the desired strength of the modification detection. In FPT_ITI.2.2, the author of a PP, PP-Module, functional package or ST should specify the actions to be taken if a modification of TSF data has been detected.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0053
Date	2023-12-22
Reference	J.9.2.1 / 1st paragraph, J.9.3.1 /1st paragraph, (15.9.10, Table B.8, J.9.3.2)
Issue – Problem Description	FPT_PHP.1 Passive detection of physical attack should be used when threats from unauthorized physical tampering with parts of the TOE are not countered by procedural methods. It addresses the threat of undetected physical tampering with the TSF. Typically, an authorized user would be given the function to verify whether tampering took place. As written, this component simply provides a TSF capability to detect tampering. Specification of management functions in FMT_LIM.1 should be considered to specify who can make use of that capability, and how they can make use of that capability. If this is done by non-IT mechanisms such as physical inspection. management functions are not required. FPT_PHP.2 Notification of physical attack should be used when threats from unauthorized physical tampering with parts of the TOE are not countered by procedural methods, and it is required that designated individuals be notified of physical tampering. It addresses the threat that physical tampering with TSF elements, although detected, may not be noticed. Specification of management functions in FMT_MOF.1 Management of security functions behaviour should be considered to specify who can make use of that capability, and how they can make use of that capability. Problem: FPT_PHP.1 has no dependency on a component from FMT class according to section 15.9.9, while FPT_PHP.2 has a dependency on FMT_LIM.1 according to section 15.9.10. The dependencies outlined in the text sections for FPT_PHP.1 and FPT_PHP.2 cited above do not reflect consistently these dependencies nor seem to fit to the hierarchy of FPT_PHP.2 to FPT_PHP.1. According to H.2.1, 1st paragraph a) and b), FMT_LIM.1 is intended to specify the limited capability policy. But FPT_PHP.1 and FPT_PHP.2 require authorized role for management functions. So, if sections J.9.2.1 and J.9.3.1 are intended to provide application notes for general management functions of FPT_PHP.1 and FPT_PHP.2 with designated user or role, FMT_MOF.1 seems more appropriate. Also, correspondingly the dependency of FPT_PHP.2 on FMT_LIM.1 needs to be revised in section 15.9.10, Table B.8 and section J.9.3.2, 2nd paragraph. All in all, it is proposed to keep the original entries for FPT_PHP.1 and FPT_PHP.2 from CC V3.1 R5 Part 2.
Type	te
Resolution - Correction / Interpretation	Update of text sections as follows (refer as well to CC2022-P2-R1-0054): **15.9.10 FPT_PHP.2 Notification of physical attack** **Component relationships**

	Hierarchical to: FPT_PHP.1 Passive detection of physical attack Dependencies: FMT_MOF.1 Management of security functions behaviour **J.9.2.1 Component rationale and application notes** FPT_PHP.1 Passive detection of physical attack should be used when threats from unauthorized physical tampering with parts of the TOE are not countered by procedural methods. It addresses the threat of undetected physical tampering with the TSF. Typically, an authorized user would be given the function to verify whether tampering took place. As written, this component simply provides a TSF capability to detect tampering. Specification of management functions in FMT_MOF.1 Management of security functions behaviour should be considered to specify who can make use of that capability, and how they can make use of that capability. If this is done by non-IT mechanisms such as physical inspection, management functions are not required. **J.9.3.2 Operations** […] In FPT_PHP.2.3, the author of a PP, PP-Module, functional package or ST should designate a user or role that is to be notified when tampering is detected. The type of user or role may vary depending on the particular security administration component (from the FMT_MOF.1 component) included in the PP, PP-Module, functional package or ST. Furthermore, corresponding adaptation of Table B.8 concerning the dependencies of FPT_PHP.2.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0054
Date	2023-12-22
Reference	J.9.3.2 / 2nd paragraph
Issue – Problem Description	In FPT_PHP.2.3, the author of a PP, PP-Module, functional package or ST should designate a user or role that is to be notified when tampering is detected. The type of user or role may vary depending on the particular security administration component (from the FMT_LIM.1 family) included in the PP, PP-Module, functional package or ST. Problem: The SFR entry is a component, not a family. Refer as well to CC2022-P2-R1-0053.
Type	ed/te

Resolution - Correction / Interpretation	In FPT_PHP.2.3, the author of a PP, PP-Module, functional package or ST should designate a user or role that is to be notified when tampering is detected. The type of user or role may vary depending on the particular security administration component (from the FMT_MOF.1 component) included in the PP, PP-Module, functional package or ST.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0055
Date	2023-12-22
Reference	J.10.1.2 / 4th paragraph, 6th paragraph
Issue – Problem Description	- 4th paragraph: It is assumed that the robustness of the automated recovery mechanisms will be verified. - 6th paragraph: It is assumed that the evaluators will verify the robustness of the automated recovery mechanisms. Problem: They are almost same and no need to provide duplicated application notes. One of them should be removed.
Type	ed/te
Resolution - Correction / Interpretation	Remove 4th paragraph.
Status	re
Remarks	-

ID	CC2022-P2-R1-0056
Date	2023-12-22
Reference	J.13
Issue – Problem Description	Problem: Application notes for FPT_STM.2 is missing from J.13.
Type	te
Resolution - Correction / Interpretation	*<Introduce application notes for FPT_STM.2 below FPT_STM.1.>*

	J.13.3 FPT_STM.2 Time source **J.13.3.1 Component rationale and application notes** In continuation of FPT_STM.1 Reliable time stamps, FPT_STM.2 focuses on the time source used in such time stamps. FPT_STM.2 requires the description of the time source used for time stamps whereby setting the time directly or configuring another time source by an authorized user according to the respective security policy can be chosen. **J.13.3.2 Operations** In FPT_STM.2 1, the author of a PP, PP-Module, functional package or ST should specify the user that is authorized by the security policy to choose the time source used in timestamps. The time can be set directly by that authorized user or result from the configuration of another time source by that authorized user.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0057
Date	2023-12-22
Reference	J.14.2.2 / 2nd paragraph
Issue – Problem Description	In FPT_TDC.1.2, the PP, PP-Module, functional package or ST should assign the list of interpretation rules to be applied by the TSF. Problem: “author of a” is missing.
Type	ed/te
Resolution - Correction / Interpretation	In FPT_TDC.1.2, the author of a PP, PP-Module, functional package or ST should assign the list of interpretation rules to be applied by the TSF.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0058
Date	2023-12-22
Reference	4
Issue – Problem Description	Problem: “CC” and “CEM” is missing from the abbreviated terms list.
Type	ed

Resolution - Correction / Interpretation	CC Common Criteria CEM Common Evaluation Methodology
Status	ma
Remarks	Note that this errata is only applicable to CC Part 2 but not to ISO/IEC 15408-2 unlike other errata applicable to both CC Part 2 and ISO/IEC 15408-2. However, if possible, both documents should be considered to introduce abbreviated terms of “CC” and “CEM” for content level consistency.

ID	CC2022-P2-R1-0059
Date	2024-06-07
Reference	10.4.2, 10.4.6, 10.4.7, 10.4.8, 10.4.9, 10.4.10, 10.4.11
Issue – Problem Description	Improved, requirements-clarifying versions of the SFRs for random bit generation are available and should be used.
Type	te
Resolution - Correction / Interpretation	**FCS_RBG.1.1** **The TSF shall perform deterministic random bit generation services using [assignment: *DRBG algorithm*] in accordance with [assignment: *list of standards*] after initialization.** **FCS_RBG.1.2** **The TSF shall use a [selection: *TSF entropy source [assignment: name of entropy source*], *TSF interface for obtaining entropy*] for initialization and reseeding.** **FCS_RBG.1.3** **The TSF shall update the DRBG state by [selection: *reseeding, uninstantiating and re-instantiating*] using a [selection: *TSF entropy source [assignment: name of entropy source*], *TSF interface for obtaining entropy [assignment: name of the interface]*] in the following situations: [selection:** **—** ***never;*** **—** ***on demand;*** **—** ***on the condition: [assignment: condition];*** **—** ***after [assignment: time]*]** **in accordance with [assignment: *list of standards*].** **FCS_RBG.2.1** **The TSF shall be able to accept a minimum input of [assignment: *minimum input length greater than zero*] from a TSF interface for obtaining entropy.**

FCS_RBG.3.1

The TSF shall be able to seed the DRBG using a [selection: choose one of: *TSF software-based entropy source*, *TSF hardware-based entropy source*] [assignment: *name of entropy source*] with [assignment: *number of bits*] bits of min-entropy.

FCS_RBG.4 Random bit generation (internal seeding - multiple sources)

Dependencies: FCS_RBG.1 Random bit generation (RBG)
FCS_RBG.5 Random bit generation (combining entropy sources)

FCS_RBG.4.1

The TSF shall be able to seed the DRBG using **[selection: *[assignment: number] TSF software-based entropy source(s)*, *[assignment: number] TSF hardware-based entropy source(s)*].**

FCS_RBG.5 Random bit generation (combining entropy sources)

FCS_RBG.5.1

The TSF shall [assignment: *combining operation*] [selection: *output from TSF entropy source(s), input from TSF interface(s) for obtaining entropy*] resulting in a minimum of [assignment: *number of bits*] bits of min-entropy to create the entropy input into the derivation function as defined in [assignment: *list of standards*].

FCS_RBG.6.1

The TSF shall provide a [selection: *hardware, software, [assignment: other interface type]*] interface to make the DRBG output, as specified in FCS_RBG.1 Random bit generation (RBG), available as a service to entities outside of the TOE.

Corresponding adaptation of section 10.4.2:

FCS_RBG.1 Random bit generation (RBG) requires random bit generation to be performed in accordance with selected standards. It also specifies whether the initial seeding is done via an internal or external entropy source, as well as when and how a DRBG's state is updated.

FCS_RBG.2 Random bit generation (external seeding) gives requirements for seeding by an external (outside the TOE) entropy source.

FCS_RBG.3 Random bit generation (internal seeding – single source) gives requirements for seeding using a TSF entropy source.

FCS_RBG.4 Random bit generation (internal seeding – multiple sources) gives requirements for seeding using multiple TSF entropy sources.

FCS_RBG.5 Random bit generation (combining entropy sources) gives

	requirements for combining multiple entropy sources (multiple internal sources, internal and external). FCS_RBG.6 Random bit generation service requires random bits to be supplied over an external interface as a service to other entities.
Status	ma
Remarks	-

ID	CC2022-P2-R1-0060
Date	2024-06-07
Reference	12.7, G.7
Issue – Problem Description	Problem: Inconsistent descriptions for SFR FIA_UID.1 and FIA_UID.2.
Type	ed/te
Resolution - Correction / Interpretation	**12.7.2 Components leveling and description** […] FIA_UID.2 User identification before any action, requires that users identify themselves before any other action will be allowed by the TSF. **12.7.6 FIA_UID.1 Timing of identification** […] **FIA_UID.1.2** **The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.** **12.7.7 FIA_UID.2 User identification before any action** […] **FIA_UID.2.1** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. **G.7.3.1 Component rationale and application notes** In this component users will be identified. A user is not allowed by the TSF to perform any other action before being identified.
Status	ma
Remarks	-

Errata / Interpretation for CC:2022 Part 3

This section provides corrections and interpretations to CC:2022 Part 3 ([CC:2022-3]).

ID	CC2022-P3-R1-0001
Date	2023-12-22
Reference	3.26, 3.27, 3.29
Issue – Problem Description	Problem: Terms “sub-activity”, “time period to exposure”, and “window of opportunity” are never used in CC Part 3. They should be considered to be deleted.
Type	te
Resolution - Correction / Interpretation	The terms 3.26 “sub-activity” and 3.29 “window of opportunity” are used in CEM, but not in CC Part 3. However, these terms are currently not defined in CEM, and the CEM definition section refers to CC Part 3 and its definition section. So, these terms cannot be easily deleted from CC Part 3. The term 3.27 “time period to exposure” is not used in CC / CEM, but the term “elapsed time” in the CEM. However, the latter one has currently no entry in the CEM definition section and should be used with the following definition: “total amount of time taken by an attacker to identify that a particular potential vulnerability may exist in the TOE, to develop an attack method and to sustain effort required to mount the attack against the TOE”.
Status	ma
Remarks	For future revisions of the CC / CEM, the terms 3.26 “sub-activity” and 3.29 “window of opportunity” could be shifted from CC Part 3 to CEM (definition section). Furthermore, for future revisions of the CC / CEM, the term 3.27 “time period to exposure” can be replaced by a definition for the term “elapsed time” in the CEM (definition section). However, in that case one has to care for references to the definition sections in CC Part 3 and CEM because of re-numbering of definitions.

ID	CC2022-P3-R1-0002
Date	2023-12-22
Reference	4 / 2nd paragraph
Issue – Problem Description	Clause 6 describes the presentation structure of the assurance classes, families, components, evaluation assurance levels along with their relationships, and the structure of the composed assurance packages (CAPs).

	Problem: EALs and CAPs are not presented in CC Part 3 but Part 5.
Type	ed/te
Resolution - Correction / Interpretation	Clause 6 describes the presentation structure of the assurance classes, families, components.
Status	ma
Remarks	-

ID	CC2022-P3-R1-0003
Date	2023-12-22
Reference	7.3.2 / Dependencies, 7.7.3
Issue – Problem Description	**7.3.2 APE_CCL.1 Conformance claims** Dependencies: APE_INT.1 PP introduction APE_ECD.1 Extended components definition APE_REQ.1 Direct rationale PP-Module security requirements **7.7.3 APE_REQ.1 Direct rationale PP-Module security requirements** Problem: The title 'Direct rationale PP-Module security requirements' of APE_REQ.1 with its entry 'PP-Module' is misleading as it does not reflect the contents of the related C-, D- and E-elements in [CC:2022-3] and Work Units in [CEM:2022]. PP-modules are neither in focus of the assurance component nor is the assurance component restricted to PP-modules. The component name shall be reviewed in terms of the purpose of the component. There is no explicit reason to include "PP-module".
Type	te
Resolution - Correction / Interpretation	Adaptation of the title of APE_REQ.1 according to the title of the corresponding ASE_REQ.1, i.e. 'Direct rationale security requirements' in sections 7.7.3 and 7.3.2. More detailed: **7.3.2 APE_CCL.1 Conformance claims** Dependencies: APE_INT.1 PP introduction APE_ECD.1 Extended components definition APE_REQ.1 Direct rationale security requirements **7.7.3 APE_REQ.1 Direct rationale security requirements**
Status	ma
Remarks	-

ID	CC2022-P3-R1-0004
Date	2023-12-22
Reference	7.3.2 / APE_CCL.1.3C
Issue – Problem Description	**APE_CCL.1.2C** **The conformance claim shall describe the conformance of the PP to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.** **APE_CCL.1.3C** **The conformance claim shall describe the conformance of the PP as either "CC Part 3 conformant" or "CC Part 3 extended".** Problem: APE_CCL.1.2C and APE_CCL.1.3C address similar aspect of the conformance claim of the PP, one is related to CC Part 2 conformance claim and the other is related to CC Part 3 conformance claim. APE_CCL.1.3C should be reviewed to be described in the same way each other.
Type	ed/te
Resolution - Correction / Interpretation	**APE_CCL.1.3C** **The conformance claim shall describe the conformance of the PP to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.**
Status	ma
Remarks	-

ID	CC2022-P3-R1-0005
Date	2023-12-22
Reference	7.5.3 / APE_OBJ.1.2D
Issue – Problem Description	**APE_OBJ.1.2D** **The developer shall provide a security objectives rationale objectives for the operational environment.** Problem: This should be clearly stated to address security objectives rationale for the security objectives for the operational environment.
Type	ed/te
Resolution - Correction / Interpretation	**APE_OBJ.1.2D** **The developer shall provide a security objectives rationale for the security objectives for the operational environment.**
Status	ma
Remarks	-

ID	CC2022-P3-R1-0006
Date	2023-12-22
Reference	7.7.3 / Dependencies
Issue – Problem Description	**7.7.3 APE_REQ.1 Direct rationale PP-Module security requirements** Dependencies: APE_ECD.1 Extended components definition APE_OBJ.1 Security objectives for the operational environment Problem: Under APE_REQ.1, SFRs are derived from SPD. So, the dependency of APE_REQ.1 shall be placed on APE_SPD.1 Security problem definition. Refer as well to CC2022-P3-R1-0003.
Type	te
Resolution - Correction / Interpretation	**7.7.3 APE_REQ.1 Direct rationale security requirements** Dependencies: APE_ECD.1 Extended components definition APE_OBJ.1 Security objectives for the operational environment APE_SPD.1 Security problem definition
Status	ma
Remarks	-

ID	CC2022-P3-R1-0007
Date	2023-12-22
Reference	8.3.2 / Dependencies, 8.8.2 / Dependencies, 8.9.2 / Dependencies
Issue – Problem Description	**8.3.2 ACE_CCL.1 PP-Module conformance claims** Dependencies: ACE_INT.1 PP-Module introduction ACE_ECD.1 PP-Module extended components definition ACE_REQ.1 PP-Module stated security requirements or ACE_REQ.2 PP-Module derived security requirements **8.8.2 ACE_MCO.1 PP-Module consistency** Dependencies: ACE_INT.1 PP-Module introduction ACE_SPD.1 PP-Module Security problem definition ACE_OBJ.1 Direct Rationale PP-Module Security objectives for the environment or ACE_OBJ.2 PP-Module Security objectives ACE_REQ.1 Direct Rationale PP-Module security

	requirements or ACE_REQ.2 PP-Module derived security requirements **8.9.2 ACE_CCO.1 PP-Configuration consistency** Dependencies: ACE_INT.1 PP-Module introduction ACE_CCL.1 PP-Module conformance claims ACE_SPD.1 PP-Module Security problem definition ACE_OBJ.1 Direct Rationale PP-Module Security objectives for the environment or ACE_OBJ.2 PP-Module Security objectives ACE_ECD.1 PP-Module extended component definition ACE_REQ.1 Direct Rational PP-Module security requirements or ACE_REQ.2 PP-Module derived security requirements ACE_MCO.1 PP-Module consistency APE_* (all APE components) Problem: The name of ACE_OBJ.1 is defined and used internally inconsistent way in the CC Part 3. It shall be defined in a consistent way considering 8.5.3. The name of ACE_REQ.1 is defined and used internally inconsistent ways in the CC Part 3. It shall be defined in a consistent way considering APE_REQ.1, ASE_REQ.1 and other ACE_* (starting with "PP-Module").
Type	ed/te
Resolution - Correction / Interpretation	**8.3.2 ACE_CCL.1 PP-Module conformance claims** Dependencies: ACE_INT.1 PP-Module introduction ACE_ECD.1 PP-Module extended components definition ACE_REQ.1 PP-Module Direct rationale security requirements or ACE_REQ.2 PP-Module derived security requirements **8.8.2 ACE_MCO.1 PP-Module consistency** Dependencies: ACE_INT.1 PP-Module introduction ACE_SPD.1 PP-Module Security problem definition ACE_OBJ.1 PP-Module Security objectives for the operational environment or ACE_OBJ.2 PP-Module Security objectives ACE_REQ.1 PP-Module Direct rationale security requirements or ACE_REQ.2 PP-Module derived security requirements **8.9.2 ACE_CCO.1 PP-Configuration consistency** Dependencies: ACE_INT.1 PP-Module introduction

	ACE_CCL.1 PP-Module conformance claims ACE_SPD.1 PP-Module Security problem definition ACE_OBJ.1 PP-Module Security objectives for the operational environment or ACE_OBJ.2 PP-Module Security objectives ACE_ECD.1 PP-Module extended component definition ACE_REQ.1 PP-Module Direct rationale security requirements or ACE_REQ.2 PP-Module derived security requirements ACE_MCO.1 PP-Module consistency APE_* (all APE components)
Status	ma
Remarks	-

ID	CC2022-P3-R1-0008
Date	2023-12-22
Reference	8.3.2 / ACE_CCL.1.4C
Issue – Problem Description	**ACE_CCL.1.2C** **The conformance claim shall describe the conformance of the PP-Module to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.** **ACE_CCL.1.4C** **The conformance claim shall describe the conformance of the PP-Module to this document as either "CC Part 3 conformant" or "CC Part 3 extended".** Problem: ACE_CCL.1.2C and ACE_CCL.1.4C address similar aspect of the conformance claim of the PP-Module, one is related to CC Part 2 conformance claim and the other is related to CC Part 3 conformance claim. ACE_CCL.1.4C should be reviewed to be described in the same way each other.
Type	ed/te
Resolution - Correction / Interpretation	**ACE_CCL.1.4C** **The conformance claim shall describe the conformance of the PP-Module to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.**
Status	ma
Remarks	-

ID	CC2022-P3-R1-0009
Date	2023-12-22
Reference	8.7.3
Issue – Problem Description	**8.7.3 ACE_REQ.1 PP-Module stated security requirements** Dependencies: APE_ECD.1 Extended components definition ACE_SPD.1 PP-Module security problem definition Problem: The name of ACE_REQ.1 is defined and used internally inconsistent ways in the CC Part 3. It shall be defined in a consistent way considering APE_REQ.1, ASE_REQ.1 and other ACE_* (starting with "PP-Module"). The component short name error for ACE_ECD.1.
Type	ed/te
Resolution - Correction / Interpretation	**8.7.3 ACE_REQ.1 PP-module Direct rationale security requirements** Dependencies: ACE_ECD.1 PP-Module extended components definition
Status	ma
Remarks	-

ID	CC2022-P3-R1-0010
Date	2023-12-22
Reference	8.8.2 / ACE_MCO.1.4C, ACE_MCO.1.5C
Issue – Problem Description	**ACE_MCO.1.4C** **The consistency rationale shall demonstrate that:** **— the security objectives definition is consistent with the security objectives of its PP-Module Base(s);** **— the security objectives definition is consistent with the security objectives of any functional package for which conformance is being claimed.** **ACE_MCO.1.5C** **The consistency rationale shall demonstrate that:** **— the security functional requirements definition is consistent with the security functional requirements of its PP-Modules Base(s);** **— the security functional requirements definition is consistent with the security functional requirements of any functional package for which conformance is being claimed.** Problem: The name of relative section shall be used consistently.
Type	ed/te

Resolution - Correction / Interpretation	**ACE_MCO.1.4C** **The consistency rationale shall demonstrate that:** **— the security objectives are consistent with the security objectives of its PP-Module Base(s);** **— the security objectives are consistent with the security objectives of any functional package for which conformance is being claimed.** **ACE_MCO.1.5C** **The consistency rationale shall demonstrate that:** **— the security functional requirements are consistent with the security functional requirements of its PP-Modules Base(s);** **— the security functional requirements are consistent with the security functional requirements of any functional package for which conformance is being claimed.**
Status	ma
Remarks	-

ID	CC2022-P3-R1-0011
Date	2023-12-22
Reference	8.9.2 / ACE_CCO.1.10C
Issue – Problem Description	**ACE_CCO.1.9C** **The conformance claim shall describe the conformance of the PP-Configuration to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.** **ACE_CCO.1.10C** **The conformance claim shall describe the conformance of the PP-Configuration to this document as either "CC Part 3 conformant" or CC Part 3 extended."** Problem: ACE_CCO.1.9C and ACE_CCO.1.10C address similar aspect of the conformance claim of the PP-Configuration, one is related to CC Part 2 conformance claim and the other is related to CC Part 3 conformance claim. ACE_CCO.1.10C should be reviewed to be described in the same way each other.
Type	ed/te
Resolution - Correction / Interpretation	**ACE_CCO.1.10C** **The conformance claim shall describe the conformance of the PP-Configuration to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.**
Status	ma

Remarks	-

ID	CC2022-P3-R1-0012
Date	2023-12-22
Reference	9.3.2 / Dependencies, 9.8.3 / Dependencies, 9.8.4 / Dependencies
Issue – Problem Description	**9.3.2 ASE_CCL.1 Conformance claims** Dependencies: ASE_INT.1 ST introduction ASE_ECD.1 Extended components definition ASE_REQ.1 Direct rationale stated security requirements **9.8.3 ASE_TSS.1 TOE summary specification** Dependencies: ASE_INT.1 ST introduction ASE_REQ.1 Direct rationale stated security requirements ADV_FSP.1 Basic functional specification **9.8.4 ASE_TSS.2 TOE summary specification with architectural design summary** Dependencies: ASE_INT.1 ST introduction ASE_REQ.1 Direct rationale stated security requirements ADV_ARC.1 Security architecture description Problem: The name of ASE_REQ.1 is defined and used internally inconsistent ways in the CC Part 3. It shall be defined in a consistent way considering APE_REQ.1 and ACE_REQ.1.
Type	ed/te
Resolution - Correction / Interpretation	**9.3.2 ASE_CCL.1 Conformance claims** Dependencies: ASE_INT.1 ST introduction ASE_ECD.1 Extended components definition ASE_REQ.1 Direct rationale security requirements **9.8.3 ASE_TSS.1 TOE summary specification** Dependencies: ASE_INT.1 ST introduction ASE_REQ.1 Direct rationale security requirements ADV_FSP.1 Basic functional specification **9.8.4 ASE_TSS.2 TOE summary specification with architectural design summary** Dependencies: ASE_INT.1 ST introduction ASE_REQ.1 Direct rationale security requirements

	ADV_ARC.1 Security architecture description
Status	ma
Remarks	-

ID	CC2022-P3-R1-0013
Date	2023-12-22
Reference	9.3.2 / ASE_CCL.1.3C
Issue – Problem Description	**ASE_CCL.1.2C** **The conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.** **ASE_CCL.1.3C** **The conformance claim shall describe the conformance of the ST as either "CC Part 3 conformant" or "CC Part 3 extended".** Problem: ASE_CCL.1.2C and ASE_CCL.1.3C address similar aspect of the conformance claim of the ST, one is related to CC Part 2 conformance claim and the other is related to CC Part 3 conformance claim. ASE_CCL.1.3C should be reviewed to be described in the same way each other.
Type	ed/te
Resolution - Correction / Interpretation	**ASE_CCL.1.3C** **The conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.**
Status	ma
Remarks	-

ID	CC2022-P3-R1-0014
Date	2023-12-22
Reference	9.7.3 / Dependencies, 7.7.3 / Dependencies, 8.7.3 / Dependencies, 7.5.3 / Dependencies, 8.5.3 / Dependencies, 9.5.3 / Dependencies
Issue – Problem Description	**9.7.3 ASE_REQ.1 Direct rationale security requirements** Dependencies: ASE_ECD.1 Extended components definition Problem: Under ASE_REQ.1, SFRs are derived from SPD. So, the dependency of ASE_REQ.1 shall be placed on ASE_SPD.1 Security problem definition. And the security requirements rationale needs the security objectives for the operational environment. So, the dependency of ASE_REQ.1 shall be also

	placed on ASE_OBJ.1 Security objectives for the operational environment. **7.7.3 APE_REQ.1 Direct rationale PP-Module security requirements** Dependencies: APE_ECD.1 Extended components definition APE_OBJ.1 Security objectives for the operational environment Problem: Relationship to the SPD is given, but currently not mentioned in the dependencies. **8.7.3 ACE_REQ.1 PP-Module stated security requirements** Dependencies: APE_ECD.1 Extended components definition ACE_SPD.1 PP-Module security problem definition Problem: Relationship to the security objectives for the TOE environment is given, but currently not mentioned in the dependencies. Entry APE_ECD.1 wrong and to be corrected. **7.5.3 APE_OBJ.1 Security objectives for the operational environment** Dependencies: No dependencies. Problem: Relationship to the SPD is given, but currently not mentioned in the dependencies. **8.5.3 ACE_OBJ.1 PP-Module security objectives for the operational environment** Dependencies: No dependencies. Problem: Relationship to the SPD is given, but currently not mentioned in the dependencies. **9.5.3 ASE_OBJ.1 Security objectives for the operational environment** Dependencies: No dependencies Problem: Relationship to the SPD is given, but currently not mentioned in the dependencies.
Type	te
Resolution - Correction / Interpretation	**9.7.3 ASE_REQ.1 Direct rationale security requirements** Dependencies: ASE_ECD.1 Extended components definition ASE_OBJ.1 Security objectives for the operational environment

	ASE_SPD.1 Security problem definition **7.7.3 APE_REQ.1 Direct rationale PP-Module security requirements** Dependencies: APE_ECD.1 Extended components definition APE_OBJ.1 Security objectives for the operational environment ASE_SPD.1 Security problem definition **8.7.3 ACE_REQ.1 PP-Module stated security requirements** Dependencies: ACE_ECD.1 Extended components definition ACE_OBJ.1 PP-Module security objectives for the operational environment ACE_SPD.1 PP-Module security problem definition **7.5.3 APE_OBJ.1 Security objectives for the operational environment** Dependencies: APE_SPD.1 Security problem definition **8.5.3 ACE_OBJ.1 PP-Module security objectives for the operational environment** Dependencies: ACE_SPD.1 PP-module security problem definition **9.5.3 ASE_OBJ.1 Security objectives for the operational environment** Dependencies: ASE_SPD.1 Security problem definition
Status	ma
Remarks	-

ID	CC2022-P3-R1-0015
Date	2023-12-22
Reference	9.7.3
Issue – Problem Description	**ASE_REQ.1.8C** **The security requirements rationale shall demonstrate that the SFRs (in conjunction with the security objectives for the environment) counter all threats for the TOE.** **ASE_REQ.1.9C** **The security requirements rationale shall demonstrate that the SFRs (in conjunction with the security objectives for the environment) enforce all OSPs.**

	Problem: ASE_REQ.1.8C and ASE_REQ.1.9C require to demonstrate the security requirements rationale in terms of threats and OSPs. But there is no explicit element to require to trace each SFR back to them. (cf. APE_REQ.1.6C and ACE_REQ.1.6C) ASE_REQ.1 does not contain a corresponding C-element as APE_REQ.1.6C/ACE_REQ.1.6C, ASE_REQ.1.8C corresponds to APE_REQ.1.7C/ACE_REQ.1.7C, and ASE_REQ.1.9C corresponds to APE_REQ.1.8C/ACE_REQ.1.8C.
Type	te
Resolution - Correction / Interpretation	**ASE_REQ.1.8C** **The security requirements rationale shall trace each SFR back to the threats countered by that SFR and the OSPs enforced by that SFR.** **The security requirements rationale shall demonstrate that the SFRs (in conjunction with the security objectives for the environment) counter all threats for the TOE.** **ASE_REQ.1.9C** **The security requirements rationale shall demonstrate that the SFRs (in conjunction with the security objectives for the environment) enforce all OSPs.**
Status	ma
Remarks	The proposed resolution is in principle OK on content level, but we face once more the problem that the CC:2022 Part 3 describes ASE_REQ.2 as hierarchical higher than ASE_REQ.1, but this is not really the case. Within the proposed resolution ASE_REQ.1.8C is supplemented with comparable content as in APE_REQ.1.6C/ACE_REQ.1.6C. The proposed solution works regards hierarchy aspects (in a broad view) only if the resolution outlined in CC2022-P1-R1-0016 is carried out. Introduction of new Content and presentation elements in the middle of a security assurance component requires many changes to the CC Part 3 and CEM. So, this should be addressed carefully and the proposed resolution added content in the existing Content and presentation element ASE_REQ.1.8C instead of inserting new Content and presentation element. A shift of C-elements and their numbering should currently be avoided because of all the side effects on other CC / CEM text sections, but for future revisions of the CC / CEM a separate C-element for the missing requirement on the security requirements rationale should be taken into account. In particular, to be consistent with APE and ACE structuring.

ID	CC2022-P3-R1-0016
Date	2023-12-22
Reference	9.7.4
Issue – Problem	**ASE_REQ.2.8C** **The security requirements rationale shall demonstrate that the SFRs**

Description	**meet all security objectives for the TOE.** Problem: ASE_REQ.2.8C requires to demonstrate the security requirements rationale in terms of security objectives for the TOE. But there is no explicit element to require to trace each SFR back to them. (cf. APE_REQ.2.6C and ACE_REQ.2.6C) ASE_REQ.2 does not contain a corresponding C-element as APE_REQ.2.6C/ACE_REQ.2.6C, and ASE_REQ.2.8C corresponds to APE_REQ.2.7C/ACE_REQ.2.7C.
Type	te
Resolution - Correction / Interpretation	**ASE_REQ.2.8C** **The security requirements rationale shall trace each SFR back to the security objectives for the TOE.** **The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.**
Status	ma
Remarks	The proposed resolution is in principle OK on content level, but we face once more the problem that the CC:2022 Part 3 describes ASE_REQ.2 as hierarchical higher than ASE_REQ.1, but this is not really the case. Within the proposed resolution ASE_REQ.2.8C is supplemented with comparable content as in APE_REQ.2.6C/ACE_REQ.2.6C. The proposed solution works regards hierarchy aspects (in a broad view) only if the resolution outlined in CC2022-P1-R1-0015 is carried out. Introduction of new Content and presentation elements in the middle of a security assurance component requires many changes to the CC Part 3 and CEM. So, this should be addressed carefully and the proposed resolution added content in the existing Content and presentation element ASE_REQ.2.8C instead of inserting new Content and presentation element. A shift of C-elements and their numbering should currently be avoided because of all the side effects on other CC / CEM text sections, but for future revisions of the CC / CEM a separate C-element for the missing requirement on the security requirements rationale should be taken into account. In particular, to be consistent with APE and ACE structuring.

ID	CC2022-P3-R1-0017
Date	2023-12-22
Reference	10.6, 10.1
Issue – Problem Description	**10.6 Security policy modelling (ADV_SPM)** Problem: Wrong title in section 10.6. Correct is “Formal TSF model (ADV_SPM)”. Compare to [CEM:2022], section 13.7. Further entries of same type in section 10.1 are as well affected.

Type	ed/te
Resolution - Correction / Interpretation	**10.6 Formal TSF model (ADV_SPM)** Adaptation of setion 10.1 as follows: Section 10.1, 3rd paragraph: When documenting the security functionality of a TOE, there are two properties that need to be demonstrated. The first property is that the security functionality works correctly, i.e. it performs as specified. The second property, and one that is arguably harder to demonstrate, is that the TOE cannot be used in a way such that the security functionality can be corrupted or bypassed. These two properties require somewhat different approaches in analysis, and so the families in ADV are structured to support these different approaches. The families Functional specification (ADV_FSP), TOE design (ADV_TDS), Implementation representation (ADV_IMP), and Formal TSF model (ADV_SPM) deal with the first property: the specification of the security functionality. The families Security Architecture (ADV_ARC) and TSF internals (ADV_INT) deal with the second property: [...] Section 10.1, paragraph below Figure 7: The requirements for all other correspondence shown in Figure 7 are defined in the ADV class for the TOE. The Formal TSF model (ADV_SPM) family defines the requirements for formally modelling selected SFRs and providing correspondence between the functional specification and the formal model. [...] Section 10.1, Figure 8: ADV_SPM: Formal TSF model
Status	ma
Remarks	-

ID	CC2022-P3-R1-0018
Date	2023-12-22
Reference	10.7.3.1 / last paragraph
Issue – Problem Description	In the requirements for this family, the term interface is used as the means of communication (between two subsystems or modules). It describes how the communication is invoked; this is similar to the details of TSFI [see Functional specification (ADV_FSP)]. The term interaction is used to identify the purpose for communication; it identifies why two subsystems or modules are communicating.

	Problem: Inconsistency regards section 10.7.3.2 bullet g). In CC Part 3, section 10.7.3.2 it is outlined: "f) A *description of interactions* among or between subsystems or modules identifies the reason that subsystems or modules communicate and characterizes the information that is passed. It need not define the information to the same level of detail as an interface specification. For example, it would be sufficient to say "subsystem X requests a block of memory from the memory manager, which responds with the location of the allocated memory. g) A *description of interfaces* provides the details of how the interactions among modules are achieved. Rather than describing the reason the modules are communicating or the purpose of their communication (i.e. the description of interactions), the description of interfaces describes the details of how that communication is accomplished, in terms of the structure and contents of the messages, semaphores, internal process communications."
Type	te
Resolution - Correction / Interpretation	In the requirements for this family, the term interface is used as the means of communication (between two modules). It describes how the communication is invoked; this is similar to the details of TSFI [see Functional specification (ADV_FSP)]. The term interaction is used to identify the purpose for communication; it identifies why two subsystems or modules are communicating.
Status	ma
Remarks	-

ID	CC2022-P3-R1-0019
Date	2023-12-22
Reference	10.8.3
Issue – Problem Description	Typo in the text part 'i. […] determine whether the dependent component uses services of the related base document within its own composite product ST to provide domain separation, self-protection, non-bypassability and protected start-up […].' The entry 'base document' is wrong, and obviously the term 'base component' is meant.
Type	ed/te
Resolution - Correction / Interpretation	Replace the wrong entry 'base document' by 'base component', thus reading 'i. […] determine whether the dependent component uses services of the related base component within its own composite product ST to provide domain separation, self-protection, non-bypassability and protected start-up

	[…].’
Status	ma
Remarks	-

ID	CC2022-P3-R1-0020
Date	2023-12-22
Reference	12.1 / last two bullets from 3rd paragraph
Issue – Problem Description	The ALC class consists of nine families: — ALC_TDA is concerned with the generation of certain artefacts during the development process; — ALC_COMP is concerned with the integration of composition parts and a consistency check of delivery procedures. Comment: These two families should be referred using names together with short names like other ALC families.
Type	ed/te
Resolution - Correction / Interpretation	The ALC class consists of nine families: — TOE development artefacts (ALC_TDA) is concerned with the generation of certain artefacts during the development process; — Integration of composition parts and consistency check of delivery procedures (ALC_COMP) is concerned with the integration of composition parts and a consistency check of delivery procedures.
Status	ma
Remarks	-

ID	CC2022-P3-R1-0021
Date	2023-12-22
Reference	12.1 / Figure 10
Issue – Problem Description	ALC_DVS: Development security ALC_LCD: Life-cycle definition Problem: Family names shall be consistent with the 12.5 and 12.7.
Type	ed/te
Resolution - Correction / Interpretation	ALC_DVS: Developer environment security ALC_LCD: Development Life-cycle definition

Status	ma
Remarks	-

ID	CC2022-P3-R1-0022
Date	2023-12-22
Reference	12.2.6 / Dependencies, 12.2.7 / Dependencies, 12.2.8 / Dependencies
Issue – Problem Description	**12.2.6 ALC_CMC.3 Authorization controls** Dependencies: ALC_CMS.1 TOE CM coverage ALC_DVS.1 Identification of security measures ALC_LCD.1 Developer defined life-cycle processes **12.2.7 ALC_CMC.4 Production support, acceptance procedures and automation** Dependencies: ALC_CMS.1 TOE CM coverage ALC_DVS.1 Identification of security measures ALC_LCD.1 Developer defined life-cycle processes **12.2.8 ALC_CMC.5 Advanced support** Dependencies: ALC_CMS.1 TOE CM coverage ALC_DVS.2 Sufficiency of security measures ALC_LCD.1 Developer defined life-cycle processes Problem: “security measures” shall be replaced with “security controls”.
Type	ed/te
Resolution - Correction / Interpretation	**12.2.6 ALC_CMC.3 Authorization controls** Dependencies: ALC_CMS.1 TOE CM coverage ALC_DVS.1 Identification of security controls ALC_LCD.1 Developer defined life-cycle processes **12.2.7 ALC_CMC.4 Production support, acceptance procedures and automation** Dependencies: ALC_CMS.1 TOE CM coverage ALC_DVS.1 Identification of security controls ALC_LCD.1 Developer defined life-cycle processes **12.2.8 ALC_CMC.5 Advanced support** Dependencies: ALC_CMS.1 TOE CM coverage ALC_DVS.2 Sufficiency of security controls

	ALC_LCD.1 Developer defined life-cycle processes
Status	ma
Remarks	-

ID	CC2022-P3-R1-0023
Date	2023-12-22
Reference	12.2.6, 12.2.7, 12.2.8
Issue – Problem Description	Problem: ALC_CMC.3/4/5 has a dependency on ALC_LCD.1 and it declares this dependency using a reference to that assurance component. But it seems that all "Application notes" from ALC_LCD.1 have copied to Dependencies section of ALC_CMC.3/4/5.
Type	te
Resolution - Correction / Interpretation	*<Remove all application notes copied from ALC_LCD.1.>*
Status	ma
Remarks	-

ID	CC2022-P3-R1-0024
Date	2023-12-22
Reference	12.2.7 / Objectives / 6th paragraph, 12.2.8 / Objectives / 6th paragraph
Issue – Problem Description	12.2.7 / Objectives / 6th paragraph: In a CM system where the quantity and organization of configuration items is complex, it is difficult to control changes without the support of automated tools. In particular, these automated tools need to be able to support the numerous changes that occur during development and ensure that those changes are authorized. It is an objective of this component to ensure that the configuration items are controlled through automated means. In the case where the overall CM system includes more than one CM application then automated tools can also support integration between the CM applications and of the TOE. 12.2.8 / Objectives / 6th paragraph: In development environments where the configuration items are complex, it is difficult to control changes without the support of automated tools. In particular, these automated tools need to be able to support the numerous changes that occur during development and ensure that those changes are authorized. It is an objective of this component to ensure that the configuration items are controlled through automated means. If the TOE is

	developed by multiple developers, i.e. integration has to take place, the use of automatic tools is adequate. Problem: The 6th paragraph from objectives section of ALC_CMC.4 and ALC_CMC.5 should be checked in terms of consistency because they are addressing similar aspects such as automated tools but they are described differently. The entry "ALC_LCD.1 Developer defined life-cycle processes" directly before the sub-section Objectives is wrong and has to be deleted. Such entry was as well not contained in CC Part 3 of CC V3.1 R5. Proposal for resolution: Deletion of entry "ALC_LCD.1 Developer defined life-cycle processes". Furthermore, concerning the 6th paragraph of sections 12.2.7 and 12.2.8: Hint: These paragaphs correspond to CC V3.1 R5 Part 3, paragraphs 354 and 361 for ALC_CMC.4 and ALC_CMC.5. However, for CC:2022 Part 3 the text in section 12.2.7 for ALC_CMC.4 was adapted, but not transfered to section 12.2.8 for ALC_CMC.5. In CC V3.1 R5 the texts for both assurance components were the same, but this is no longer the case for CC:2022 Part 3: Paragraph 361 is taken over to section 12.2.8, but now differs from the adapted text in section 12.2.7.
Type	te
Resolution - Correction / Interpretation	Combine the 6th paragraph of sections 12.2.7 and 12.2.8 and use the resulting text for both text sections as a replacement: In development environments where the configuration items or their quantity or organization are complex, it is difficult to control changes without the support of automated tools. In particular, these automated tools need to be able to support the numerous changes that occur during development and ensure that those changes are authorized. It is an objective of this component to ensure that the configuration items are controlled through automated means. If the TOE is developed by multiple developers, i.e. integration has to take place, the use of automatic tools is adequate. Furthermore, in the case where the overall CM system includes more than one CM application then automated tools can also support integration between the CM applications and of the TOE.
Status	ma
Remarks	-

ID	CC2022-P3-R1-0025
Date	2023-12-22
Reference	12.4.3, 12.4.4
Issue – Problem	12.4.3, 3rd paragraph, a) and d): a) ensuring that the TOE received by the consumer corresponds precisely to

Description	the evaluated version of the TOE; d) avoiding unwanted knowledge of distribution of the TOE to the consumer: there can be cases where potential attackers should not know when and how it is delivered; 12.4.4, ALC_DEL.1.1D: **The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.** 12.4.4, ALC_DEL.1.1C: **The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.** Problem: Check the term "consumer". In section 12.1, the term "downstream user" is used regarding ALC_DEL instead of "user" or "consumer". "downstream user" is more comprehensive to address various types of users/consumers.
Type	ed/te
Resolution - Correction / Interpretation	12.4.3, 3rd paragraph, a) and d): a) ensuring that the TOE received by the downstream user corresponds precisely to the evaluated version of the TOE; d) avoiding unwanted knowledge of distribution of the TOE to the downstream user: there can be cases where potential attackers should not know when and how it is delivered; 12.4.4, ALC_DEL.1.1D: **The developer shall document and provide procedures for delivery of the TOE or parts of it to the downstream user.** 12.4.4, ALC_DEL.1.1C: **The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the downstream user.** In addition, the term "downstream user" should be used with the following definition: "any type of user making use of the TOE, e.g. end user, integrator, initializer, personalizer, administrator, supplier".
Status	ma
Remarks	For future revisions of the CC / CEM, the term "downstream user" can be incorporated in the CEM (definition section). However, in that case one has to care for references to the definition section in the CEM because of re-numbering of definitions.

ID	CC2022-P3-R1-0026
Date	2023-12-22
Reference	12.5.1 / 1st paragraph, 12.5.3 / 2nd & 3rd paragraphs, 12.5.4 / ALC_DVS.1.1D & ALC_DVS.1.1C, 12.5.5 / ALC_DVS.2.1D & ALC_DVS.2.1C & ALC_DVS.2.2C
Issue – Problem Description	12.5.1, 1st paragraph: Development security is concerned with the determination and specification of security controls relating to the developer provided environment. 12.5.3, 2nd paragraph: The evaluator should visit the site(s) in order to assess evidence for development security. This may include sites of subcontractors involved in the TOE development and production. Any decision not to visit shall be agreed with the evaluation authority. 12.5.3, 3rd paragraph: Although development security deals with the maintenance of the TOE and hence with aspects becoming relevant after the completion of the evaluation, the Developer environment security (ALC_DVS) requirements specify only that the development security controls be in place at the time of evaluation. Furthermore, Developer environment security (ALC_DVS) does not contain any requirements related to the sponsor's intention to apply the development security controls in the future, after completion of the evaluation. 12.5.4: **ALC_DVS.1.1D** **The developer shall produce and provide development security documentation.** **ALC_DVS.1.1C** **The development security documentation shall describe all the physical, logical, procedural, personnel, and other security controls that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.** 12.5.5: **ALC_DVS.2.1D** The developer shall produce and provide development security documentation. **ALC_DVS.2.1C** The development security documentation shall describe all the physical, logical, procedural, personnel, and other security controls that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

	ALC_DVS.2.2C **The development security documentation shall justify that the security controls provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.** Problem: ALC_DVS is addressing "Developer environment security" but not "Development security".
Type	ed/te
Resolution - Correction / Interpretation	12.5.1, 1st paragraph: Developer environment security is concerned with the determination and specification of security controls relating to the developer provided environment. 12.5.3, 2nd paragraph: The evaluator should visit the site(s) in order to assess evidence for developer environment security. This may include sites of subcontractors involved in the TOE development and production. Any decision not to visit shall be agreed with the evaluation authority. 12.5.3, 3rd paragraph: Although developer environment security deals with the maintenance of the TOE and hence with aspects becoming relevant after the completion of the evaluation, the Developer environment security (ALC_DVS) requirements specify only that the development security controls be in place at the time of evaluation. Furthermore, Developer environment security (ALC_DVS) does not contain any requirements related to the sponsor's intention to apply the development security controls in the future, after completion of the evaluation. 12.5.4: **ALC_DVS.1.1D** **The developer shall produce and provide developer environment security documentation.** **ALC_DVS.1.1C** **The developer environment security documentation shall describe all the physical, logical, procedural, personnel, and other security controls that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.** 12.5.5: **ALC_DVS.2.1D** The developer shall produce and provide developer environment security documentation. **ALC_DVS.2.1C**

	The developer environment security documentation shall describe all the physical, logical, procedural, personnel, and other security controls that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. **ALC_DVS.2.2C** **The developer environment security documentation shall justify that the security controls provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.**
Status	ma
Remarks	-

ID	CC2022-P3-R1-0027
Date	2023-12-22
Reference	12.5.5 / ALC_DVS.2.1C
Issue – Problem Description	**ALC_DVS.1.1C** **The development security documentation shall describe all the physical, logical, procedural, personnel, and other security controls that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.** **ALC_DVS.2.1C** The development security documentation shall describe all the physical, procedural, personnel, and other security controls that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Problem: ALC_DVS.2 is hierarchically higher than ALC_DVS.1, so ALC_DVS.2.1C shall be at least the same requirement than ALC_DVS.1.1C.
Type	ed/te
Resolution - Correction / Interpretation	**ALC_DVS.2.1C** The development security documentation shall describe all the physical, logical, procedural, personnel, and other security controls that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
Status	ma
Remarks	-

ID	CC2022-P3-R1-0028
Date	2023-12-22

Reference	12.7.3 / 2nd paragraph, 1st ~ 3rd bullets
Issue – Problem Description	There are different types of acceptance situations that are dealt with at different locations in the criteria: — acceptance of parts delivered by subcontractors (“integration”) should be treated in this family, — Life-cycle definition (ALC_LCD), — acceptance subsequent to internal transportations in Development security (ALC_DVS), Problem: 1st and 2nd bullets shall be in one bullet. Family names shall be updated in a consistent way as they are defined.
Type	ed/te
Resolution - Correction / Interpretation	There are different types of acceptance situations that are dealt with at different locations in the criteria: — acceptance of parts delivered by subcontractors (“integration”) should be treated in this family, Development Life-cycle definition (ALC_LCD), — acceptance subsequent to internal transportations in Developer environment security (ALC_DVS),
Status	ma
Remarks	-

ID	CC2022-P3-R1-0029
Date	2023-12-22
Reference	12.7.5 / ALC_LCD.2.1C
Issue – Problem Description	**ALC_LCD.1.1C** **The life-cycle definition documentation shall describe the processes used to develop and maintain the TOE.** **ALC_LCD.2.1C** The life-cycle definition documentation shall describe the model used to develop and maintain the TOE **including the details of its arithmetic parameters and/or metrics used to measure the quality of the TOE and/or its development**. Problem: ALC_LCD.2.1C shall include increased content and presentation elements from ALC_LCD.1.1C, and be highlighted accordingly.
Type	ed/te
Resolution - Correction / Interpretation	ALC_LCD.2.1C The life-cycle definition documentation shall describe the processes used to develop and maintain the TOE **including the details of its arithmetic**

	parameters and/or metrics used to measure the quality of the TOE and/or its development.
Status	ma
Remarks	-

ID	CC2022-P3-R1-0030
Date	2023-12-22
Reference	12.8.4 / ALC_TDA.1.3E, 12.8.5 / ALC_TDA.2.3E, 12.8.6 / ALC_TDA.3.3E
Issue – Problem Description	**ALC_TDA.1.3E/2.3E/3.3E** The evaluator shall confirm that the list of unique TOE implementation representation identifiers as recorded during the TOE generation time is consistent with the creation time of the TOE. Problem: ALC_TDA.1.3E/2.3E/3.3E shall address the timestamp of the list considering ALC_TDA.1.3C and ALC_TDA.1-3 from [CEM:2022].
Type	te
Resolution - Correction / Interpretation	**ALC_TDA.1.3E/2.3E/3.3E** The evaluator shall confirm that the timestamp of the list of unique TOE implementation representation identifiers as recorded during the TOE generation time is consistent with the creation time of the TOE.
Status	ma
Remarks	-

ID	CC2022-P3-R1-0031
Date	2023-12-22
Reference	14.1 / Figure 12
Issue – Problem Description	AVA_COMP: Composite product vulnerability assessment Problem: The family name shall be consistent with the 14.4.
Type	ed/te
Resolution - Correction / Interpretation	AVA_COMP: Composite vulnerability assessment
Status	ma
Remarks	-

ID	CC2022-P3-R1-0032
Date	2024-06-07
Reference	10.6.4
Issue – Problem Description	Problem: Missing D-element ADV_SPM.1.7D for provisioning of tools used for formal models, formal properties, proofs and demonstrations. Refer to CEM2022-R1-0071.
Type	te
Resolution - Correction / Interpretation	**ADV_SPM.1.7D** **The developer shall provide all the tools used for the formal model, the formal properties, proofs and demonstrations.**
Status	ma
Remarks	-

Errata / Interpretation for CC:2022 Part 4

This section provides corrections and interpretations to CC:2022 Part 4 ([CC:2022-4]):

None.

Errata / Interpretation for CC:2022 Part 5

This section provides corrections and interpretations to CC:2022 Part 5 ([CC:2022-5]).

ID	CC2022-P5-R1-0001
Date	2023-12-22
Reference	1 / 2nd paragraph / 2nd bullet
Issue – Problem Description	— *composition assurance (CAP)* family of packages that specify sets of security assurance components used for specifying appropriate security assurances to be provided during an evaluation of composed TOEs; Problem: Assurance package name shall be used in a consistent way.
Type	ed/te
Resolution - Correction / Interpretation	— *composed assurance package (CAP)* family of packages that specify sets of security assurance components used for specifying appropriate security assurances to be provided during an evaluation of composed TOEs;
Status	ma
Remarks	-

ID	CC2022-P5-R1-0002
Date	2023-12-22
Reference	4.2.2 / Table 1, 4.4.2.5 / Table 2, 4.4.3.5 / Table 3, 4.4.4.5 / Table 4, 4.4.5.5 / Table 5, 4.4.6.5 / Table 6, 4.4.7.5 / Table 7, 4.4.8.5 / Table 8, 5.3 / Table 9, 5.4.1.5 / Table 10, 5.4.2.5 / Table 11, 5.4.3.5 / Table 12, 6.5 / Table 13, 7.2 / Table 14, 7.4.1.5 / Table 15, 7.4.2.5 / Table 16, 8.2 / Table 17, 8.4.1.5 / Table 18, 8.4.2.5 / Table 19
Issue – Problem Description	ASE: ST evaluation APE: PP evaluation Comment: Class names of ASE and APE shall be consistent with [CC:2022-3].
Type	ed/te
Resolution - Correction / Interpretation	ASE: Security Target (ST) evaluation APE: Protection Profile (PP) evaluation

Status	ma
Remarks	-

ID	CC2022-P5-R1-0003
Date	2023-12-22
Reference	4.4.2.4 / 3rd paragraph, 4th paragraph
Issue – Problem Description	3rd paragraph: **EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.** 4th paragraph: **EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.** Problem: The 3rd paragraph and the 4th paragraph are the same. Considering the previous version of [CC:2022-3], it seems like editorial error.
Type	ed/te
Resolution - Correction / Interpretation	Update 4th paragraph as follows: 4th paragraph: **This EAL provides a meaningful increase in assurance over unevaluated IT.**
Status	ma
Remarks	-

ID	CC2022-P5-R1-0004
Date	2023-12-22
Reference	4.4.2.5 / Table 2
Issue – Problem Description	ASE_REQ.1 Stated security requirements Problem: The component name of ASE_REQ.1 shall be consistent with that of [CC:2022-3].
Type	ed/te
Resolution - Correction / Interpretation	ASE_REQ.1 Direct rationale security requirements
Status	ma
Remarks	-

ID	CC2022-P5-R1-0005
Date	2023-12-22
Reference	4.4.6
Issue – Problem Description	**4.4.6 Evaluation assurance level 5 (EAL5) - Semi-formally verified designed and tested** Problem: EAL package name error.
Type	ed/te
Resolution - Correction / Interpretation	**4.4.6 Evaluation assurance level 5 (EAL5) - Semi-formally designed and tested**
Status	ma
Remarks	-

ID	CC2022-P5-R1-0006
Date	2023-12-22
Reference	4.4.7.4, 4.4.8.4
Issue – Problem Description	In [CC:2022-3], the SAR family ADV_SPM (refer to sections 10.6 and A.5) was completely reworked, and in particular new or updated requirements were defined. This includes a corresponding adaptation of the CEM Work Units in [CEM:2022], section 13.7. However, such update was not entirely transferred to [CC:2022-5], thus showing inconsistencies between CC Part 3 / CEM and CC Part 5. Refer to section 4.4.7.4 with its text entry 'EAL6 provides assurance by a full ST and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, the design of the TOE and the implementation to understand the security behaviour. Assurance is additionally gained through a formal model of select TOE security policies and a semi-formal presentation of the functional specification and TOE design. A modular, layered and simple TSF design is also required.' A similar comment holds for section 4.4.8.4.
Type	ed/te
Resolution - Correction / Interpretation	The text in the objectives section 4.4.7.4 and 4.4.8.4 is of informal character only whereas the requirements on the SPM modelling and related evaluation activities are specified in [CC:2022-3], sections 10.6 and A.5 and in [CEM:2022], section 13.7. Hence, the latter ones are of relevance and have to be applied. Thus for alignment, the present contents of sections 4.4.7.4 and 4.4.8.4 have to be rethought in the sense of the new SPM modelling and related evaluation activities as outlined in [CC:2022-3] and

	[CEM:2022]. Replace the first para in section 4.4.7.4 by: 'EAL6 provides assurance by a full ST and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, a description of the design of the TOE and the implementation to understand the security behaviour. **Assurance is additionally gained through the development of a formal representation of the TSF and its properties, as defined by the SFRs and the security objectives of the ST, further referred to as the formal model and the formal properties, respectively**. A modular, **layered and simple** TSF design is also required.' Replace the first para in section 4.4.8.4 by: 'EAL7 provides assurance by a full ST and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, a description of the design of the TOE and **a structured presentation of** the implementation to understand the security behaviour. Assurance is additionally gained through the development of a formal representation of the TSF and its properties, as defined by the SFRs and the security objectives of the ST, further referred to as the formal model and the formal properties, respectively. A modular, layered and simple TSF design is also required.'
Status	ma
Remarks	-

ID	CC2022-P5-R1-0007
Date	2023-12-22
Reference	5.3 / Table 9, 5.4.1, 5.4.1.1 / 1st paragraph, 5.4.2, 5.4.2.1 / / 1st paragraph, 5.4.3, 5.4.3.1 / 1st paragraph
Issue – Problem Description	**Table 9 — Composition assurance package summary** - 1st low: Assurance components by composition assurance package **5.4.1 Composition assurance package A — Structurally composed** 5.4.1.1, 1st paragraph: The name of the package is composition assurance package A (CAP-A) — structurally composed. **5.4.2 Composition assurance package B — Methodically composed** 5.4.2.1, 1st paragraph: The name of the package is composition assurance package B (CAP-B) — methodically composed.

	5.4.3 Composition assurance package C — Methodically composed, tested and reviewed 5.4.3.1, 1st paragraph: The name of the package is composition assurance package C (CAP-C) — methodically composed, tested and reviewed. Problem: CAP package names shall be used in a consistent way.
Type	ed/te
Resolution - Correction / Interpretation	**Table 9 — Composed assurance package summary** - 1st row: Assurance components by composed assurance package **5.4.1 Composed assurance package A (CAP-A) — Structurally composed** 5.4.1.1, 1st paragraph: The name of the package is composed assurance package A (CAP-A) — structurally composed. **5.4.2 Composed assurance package B (CAP-B) — Methodically composed** 5.4.2.1, 1st paragraph: The name of the package is composed assurance package B (CAP-B) — methodically composed. **5.4.3 Composed assurance package C (CAP-C) — Methodically composed, tested and reviewed** 5.4.3.1, 1st paragraph: The name of the package is composed assurance package C (CAP-C) — methodically composed, tested and reviewed.
Status	ma
Remarks	-

ID	CC2022-P5-R1-0008
Date	2023-12-22
Reference	5.4.1.5 / Table 10
Issue – Problem Description	Problem: Table 10 shows that CAP-A includes ALC_CMS.1 TOE CM coverage, but Table 9 shows that all CAP include ALC_CMS.2 Parts of the TOE CM coverage instead of ALC_CMS.1. Considering composed TOE, ALC_CMS.2 is proper assurance component because it requires the configuration list shall include the parts that

	comprise the TOE.
Type	ed/te
Resolution - Correction / Interpretation	*<Update Table 10 to include ALC_CMS.2 Parts of the TOE CM coverage.>*
Status	ma
Remarks	-

ID	CC2022-P5-R1-0009
Date	2023-12-22
Reference	5.4.2.5 / Table 11, 5.4.3.5 / Table 12
Issue – Problem Description	ASE_OBJ.2 Security objectives for the operational environment ASE_REQ.2 Stated security requirements Problem: Table 11 and Table 12 include ASE_OBJ.2 and ASE_REQ.2, but SAR names are inconsistent with those from [CC:2022-3].
Type	ed/te
Resolution - Correction / Interpretation	ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirements
Status	ma
Remarks	-

ID	CC2022-P5-R1-0010
Date	2023-12-22
Reference	6.5 / Table 13
Issue – Problem Description	ASE_COMP.1 Consistency of Security Target Problem: Assurance component name of ASE_COMP.1 shall be consistent with [CC:2022-3].
Type	ed/te
Resolution - Correction / Interpretation	ASE_COMP.1 Consistency of Security Target (ST)
Status	ma

Remarks	-

ID	CC2022-P5-R1-0011
Date	2023-12-22
Reference	7.4.1
Issue – Problem Description	**7.4.1 Protection profile assurance package — Direct rationale PP** Problem: The package name shall be used in a consistent way. Refer to the Table 14 and 1st paragraph in 7.4.1.1 of [CEM:2022].
Type	ed/te
Resolution - Correction / Interpretation	7.4.1 Protection profile assurance package — **Direct rationale**
Status	ma
Remarks	-

ID	CC2022-P5-R1-0012
Date	2023-12-22
Reference	7.4.1.5, 7.4.2.5, 8.4.1.5, 8.4.2.5
Issue – Problem Description	The titles of the APE- and ASE-components in the referenced sections show the following entries: ‘APE_REQ.1 Stated security requirements’ ‘APE_REQ.2 Security requirements’ ‘ASE_REQ.1 Stated security requirements’ ‘ASE_REQ.2 Stated security requirements’ The titles of these assurance components are inconsistent to their corresponding titles in [CC:2022-3], sections 7.7.3, 7.7.4, 9.7.3, 9.7.4 (and others). Refer as well to CC2022-P3-R1-0006.
Type	ed/te
Resolution - Correction / Interpretation	Correction of the wrong title entries in the referenced sections according to [CC:2022-3] including the correction of the title for APE_REQ.1 in [CC:2022-3] as outlined in CC2022-P3-R1-0006. Section 7.4.1.5: ‘APE_REQ.1 Direct rationale security requirements’ Section 7.4.2.5: ‘APE_REQ.2 Derived security requirements’ Section 8.4.1.5: ‘ASE_REQ.1 Direct rationale security requirements’ Section 8.4.2.5: ‘ASE_REQ.2 Derived security requirements’

	Beyond that any further assurance components and their titles in [CC:2022-5] should be checked for consistency regards [CC:2022-3] and replaced by the ones from [CC:2022-3], where applicable. Relevant are the titles outlined in [CC:2022-3].
Status	ma
Remarks	For future revisions of the CC / CEM, it is recommended to rework the titles of all the APE, ASE and ACE assurance components in a consistent and harmonised manner (in particular, meaningful and uniform use of the entries 'derived', 'stated', 'direct rationale' etc.).

ID	CC2022-P5-R1-0013
Date	2023-12-22
Reference	8.3 / 1st paragraph
Issue – Problem Description	The STA objectives are to support the provision of assurance through evaluation that a protection profile conforms with the requirements given in CC Part 1. Problem: The STA is related to ST evaluation.
Type	ed/te
Resolution - Correction / Interpretation	The STA objectives are to support the provision of assurance through evaluation that a Security Target conforms with the requirements given in CC Part 1.
Status	ma
Remarks	-

Errata / Interpretation for CEM:2022

This section provides corrections and interpretations to CEM:2022 ([CEM:2022]).

ID	CEM2022-R1-0001
Date	2023-12-22
Reference	4
Issue – Problem Description	Problem: “CC” and “CEM” is missing from the abbreviated terms list.
Type	ed
Resolution - Correction / Interpretation	CC Common Criteria CEM Common Evaluation Methodology
Status	ma
Remarks	Note that this errata is only applicable to CEM but not to ISO/IEC 18045 unlike other errata applicable to both CEM and ISO/IEC 18045. However, if possible, both documents should be considered to introduce abbreviated terms of “CC” and “CEM” for content level consistency.

ID	CEM2022-R1-0002
Date	2023-12-22
Reference	9.2.2 / 2nd paragraph
Issue – Problem Description	Since the assurance requirements apply to the entire TOE, all evaluation evidence pertaining to all parts of the TOE is to be made available to the evaluator. The scope and required content of such evaluation evidence is independent of the level of control that the developer has over each of the parts of the TOE. For example, if design is required, then the TOE design (ADV_TDS) requirements will apply to all subsystems that are part of the TSF. In addition, assurance requirements that call for procedures to be in place, e.g. CM capabilities (ALC_CMC) and Delivery (ALC_DEL) will also apply to the entire TOE (including any part produced by another developer). Problem: The statement is true for a single-assurance evaluation but not sufficient for a multi-assurance evaluation.
Type	te
Resolution -	*<Add additional statements for a multi-assurance evaluation.>*

Correction / Interpretation	In case of single-assurance evaluation: Since the assurance requirements apply to the entire TOE, all evaluation evidence pertaining to all parts of the TOE is to be made available to the evaluator. The scope and required content of such evaluation evidence is independent of the level of control that the developer has over each of the parts of the TOE. For example, if design is required, then the TOE design (ADV_TDS) requirements will apply to all subsystems that are part of the TSF. In addition, assurance requirements that call for procedures to be in place, e.g. CM capabilities (ALC_CMC) and Delivery (ALC_DEL) will also apply to the entire TOE (including any part produced by another developer). For multi-assurance evaluation: According to CC Part 1, section 11.3.2.1, a multi-assurance PP-Configuration or the conformant multi-assurance ST respectively describes the organization of the TSF in terms of the sub-TSFs that are defined in its components and defines for each sub-TSF a set of SARs that is consistent with the corresponding component. The multi-assurance evaluation paradigm consists in applying different assurance requirements to different parts of the TSF (sub-TSFs), i.e. each sub-TSF is associated with its own set of security assurance requirements (SARs) in a multi-assurance PP-Configuration/ST. Concerning evaluation aspects in the multi-assurance case, for each component of a multi-assurance PP-Configuration/ST the assurance requirements related to that component have to be applied according to the single-assurance evaluation approach as outlined above. As far as applicable, e.g. for vulnerability analysis or testing, beyond that as well the entire TOE consisting of all those components has to be taken into account.
Status	ma
Remarks	-

ID	CEM2022-R1-0003
Date	2023-12-22
Reference	9.4.1 / 1st paragraph
Issue – Problem Description	The objective of this subclause is to describe the Observation Report (OR) and the Evaluation Technical Report (ETR). Schemes may require additional evaluator reports such as reports on individual units of work, or may require additional information to be contained in the OR and the ETR. This document does not preclude the addition of information into these reports as this International Standard specifies only the minimum information content. Problem: “this International Standard” shall be replace with “this document”.
Type	ed
Resolution -	The objective of this subclause is to describe the Observation Report (OR)

Correction / Interpretation	and the Evaluation Technical Report (ETR). Schemes may require additional evaluator reports such as reports on individual units of work, or may require additional information to be contained in the OR and the ETR. This document does not preclude the addition of information into these reports as this document specifies only the minimum information content.
Status	ma
Remarks	Note that this comment is only applicable to CEM but not to ISO/IEC 18025 unlike other comments applicable to both CEM and ISO/IEC 18025.

ID	CEM2022-R1-0004
Date	2023-12-22
Reference	9.4.5.3.1 / Figure 5
Issue – Problem Description	Problem: Figure 5 has no item for "PP-Configuration overview" which is described in 9.4.5.3.3.
Type	te
Resolution - Correction / Interpretation	*<Update Figure 5 to include "PP-Configuration overview".>*
Status	ma
Remarks	-

ID	CEM2022-R1-0005
Date	2023-12-22
Reference	9.4.5.3.2 / 6th paragraph
Issue – Problem Description	PP configuration control identifiers (e.g. name, date and version number) are required to identify what is being evaluated in order for the evaluation authority to verify that the verdicts have been assigned correctly by the evaluator. Problem: 9.4.5.3.2 is addressing PP-Configuration instead of PP.
Type	ed/te
Resolution - Correction / Interpretation	PP-Configuration configuration control identifiers (e.g. name, date and version number) are required to identify what is being evaluated in order for the evaluation authority to verify that the verdicts have been assigned correctly by the evaluator.
Status	ma

Remarks	-

ID	CEM2022-R1-0006
Date	2023-12-22
Reference	9.4.5.2.2, 9.4.5.3.2, 9.4.5.4.2
Issue – Problem Description	9.4.5.2.2 General 9.4.5.3.2 General 9.4.5.4.2 General Problem: Considering Figure 4, 5 and 6 respectively, the title of 9.4.5.2.2, 9.4.5.3.2 and 9.4.5.4.2 shall be “Introduction”.
Type	ed
Resolution - Correction / Interpretation	9.4.5.2.2 Introduction 9.4.5.3.2 Introduction 9.4.5.4.2 Introduction
Status	ma
Remarks	-

ID	CEM2022-R1-0007
Date	2023-12-22
Reference	9.4.5.4.6 / 1st paragraph
Issue – Problem Description	The evaluator shall report the conclusions of the evaluation, which will relate to whether the TOE has satisfied its associated ST, in particular the overall verdict as defined in CC Part 1, Evaluation and evaluation results, and determined by application of the verdict assignment described in 9.1.5. Problem: Clause reference is missing.
Type	ed/te
Resolution - Correction / Interpretation	The evaluator shall report the conclusions of the evaluation, which will relate to whether the TOE has satisfied its associated ST, in particular the overall verdict as defined in CC Part 1, clause 13, Evaluation and evaluation results, and determined by application of the verdict assignment described in 9.1.5.
Status	ma
Remarks	-

ID	CEM2022-R1-0008
Date	2023-12-22
Reference	10.3.1.3.6 / 2nd paragraph
Issue – Problem Description	While some TOEs may run stand-alone, other TOEs (notably software TOEs) need additional hardware, software or firmware to operate. In this subclause of the PP, the PP author lists all hardware, software, and/or firmware that will be available for the TOE to run on. Problem: Replacing "section(refer to CEM V3.1 R5, paragraph #156)" with "subclasue" here is inappropriate. Here, the work unit is addressing a part of the PP including contents regarding APE_INT.1.5C but not a specific clause/subclause of the PP document.
Type	ed
Resolution - Correction / Interpretation	While some TOEs may run stand-alone, other TOEs (notably software TOEs) need additional hardware, software or firmware to operate. In this section of the PP, the PP author lists all hardware, software, and/or firmware that will be available for the TOE to run on.
Status	ma
Remarks	-

ID	CEM2022-R1-0009
Date	2023-12-22
Reference	10.4.1.2 / 1st paragraph
Issue – Problem Description	The evaluation evidence for this sub-activity is: a) the PP; b) the package(s) that the PP claims conformance to. Problem: Input for APE_CCL.1 sub-activity shall be reviewed in terms of all work units belonging to itself. Considering APE_CCL.1-12 ~ 15, the following shall be listed as a part of input: - the PP(s) that the PP claims conformance to.
Type	te
Resolution - Correction / Interpretation	The evaluation evidence for this sub-activity is: a) the PP; b) the PP(s) that the PP claims conformance to; c) the package(s) that the PP claims conformance to.
Status	ma

Remarks	-

ID	CEM2022-R1-0010
Date	2023-12-22
Reference	10.4.1.3.3 ~10.4.1.3.6 / APE_CCL.1-2 ~APE_CCL.1-5
Issue – Problem Description	**10.4.1.3.3 Work unit APE_CCL.1-2** The evaluator shall check that the CC conformance claim states a claim of either CC Part 2 conformant or CC Part 2 extended for the PP. **10.4.1.3.4 Work unit APE_CCL.1-3** The evaluator shall check that the CC conformance claim states a claim of either CC Part 3 conformant or CC Part 3 extended for the PP. **10.4.1.3.5 Work unit APE_CCL.1-4** The evaluator shall examine the CC conformance claim for CC Part 2 to determine that it is consistent with the extended components definition. If the CC conformance claim contains CC Part 2 conformant, the evaluator determines that the extended components definition does not define functional components. If the CC conformance claim contains CC Part 2 extended, the evaluator determines that the extended components definition defines at least one extended functional component. **10.4.1.3.6 Work unit APE_CCL.1-5** The evaluator shall examine the CC conformance claim for CC Part 3 to determine that it is consistent with the extended components definition. If the CC conformance claim contains CC Part 3 conformant, the evaluator determines that the extended components definition does not define assurance components. If the CC conformance claim contains CC Part 3 extended, the evaluator determines that the extended components definition defines at least one extended assurance component. Problem: Relevant section of the PP is the “conformance claim” section.
Type	ed/te
Resolution - Correction / Interpretation	**10.4.1.3.3 Work unit APE_CCL.1-2** The evaluator shall check that the conformance claim states a claim of either CC Part 2 conformant or CC Part 2 extended for the PP. **10.4.1.3.4 Work unit APE_CCL.1-3**

	The evaluator shall check that the conformance claim states a claim of either CC Part 3 conformant or CC Part 3 extended for the PP. **10.4.1.3.5 Work unit APE_CCL.1-4** The evaluator shall examine the conformance claim for CC Part 2 to determine that it is consistent with the extended components definition. If the conformance claim contains CC Part 2 conformant, the evaluator determines that the extended components definition does not define functional components. If the conformance claim contains CC Part 2 extended, the evaluator determines that the extended components definition defines at least one extended functional component. **10.4.1.3.6 Work unit APE_CCL.1-5** The evaluator shall examine the conformance claim for CC Part 3 to determine that it is consistent with the extended components definition. If the conformance claim contains CC Part 3 conformant, the evaluator determines that the extended components definition does not define assurance components. If the conformance claim contains CC Part 3 extended, the evaluator determines that the extended components definition defines at least one extended assurance component
Status	ma
Remarks	-

ID	CEM2022-R1-0011
Date	2023-12-22
Reference	10.4.1.3.8, 10.4.1.3.9, 11.3.1.3.6, 11.3.1.3.8, 12.4.1.3.12, 12.4.1.3.13
Issue – Problem Description	10.4.1.3.8, 3rd paragraph, a): a) A functional package identification, giving a unique name, version, date, sponsor, and the CC edition; 10.4.1.3.9, 1st paragraph, a): a) An assurance package identification, giving a unique name, version, date, sponsor, and the CC edition; 11.3.1.3.6, 3rd paragraph, a): a) A functional package identification, giving a unique name, version, date, sponsor, and the CC edition; 11.3.1.3.8, 1st paragraph, a):

	a) An assurance package identification, giving a unique name, version, date, sponsor, and the CC edition; 12.4.1.3.12, 3rd paragraph, a): a) A functional package identification, giving a unique name, version, date, sponsor, and the CC edition; 12.4.1.3.13, 1st paragraph, a): a) An assurance package identification, giving a unique name, version, date, sponsor, and the CC edition; Problem: According to [CC:2022-1], Clause 9 “Package”, all packages shall include the package identification giving a unique name, short name, version, date, sponsor, and the relevant parts of the CC.
Type	ed/te
Resolution - Correction / Interpretation	10.4.1.3.8, 3rd paragraph, a): a) A functional package identification, giving a unique name, short name, version, date, sponsor, and the CC edition; 10.4.1.3.9, 1st paragraph, a): a) An assurance package identification, giving a unique name, short name, version, date, sponsor, and the CC edition; 11.3.1.3.6, 3rd paragraph, a): a) A functional package identification, giving a unique name, short name, version, date, sponsor, and the CC edition; 11.3.1.3.8, 1st paragraph, a): a) An assurance package identification, giving a unique name, short name, version, date, sponsor, and the CC edition; 12.4.1.3.12, 3rd paragraph, a): a) A functional package identification, giving a unique name, short name, version, date, sponsor, and the CC edition; 12.4.1.3.13, 1st paragraph, a): a) An assurance package identification, giving a unique name, short name, version, date, sponsor, and the CC edition;
Status	ma
Remarks	-

ID	CEM2022-R1-0012
Date	2023-12-22
Reference	10.4.1.3.8, 11.3.1.3.6, 12.4.1.3.12
Issue – Problem Description	10.4.1.3.8, 3rd paragraph, d), ii: ii. The package includes a security objectives rationale if security objectives for the environment are defined. 11.3.1.3.6, 3rd paragraph, d), ii: ii. the package includes a security objectives rationale if security objectives for the environment are defined.; 12.4.1.3.12, 3rd paragraph, d), ii: ii. the package includes a security objectives rationale if security objectives for the environment are defined.; Problem: Correct name should be used: security objectives for the operational environment.
Type	ed/te
Resolution - Correction / Interpretation	10.4.1.3.8, 3rd paragraph, d), ii: ii. The package includes a security objectives rationale if security objectives for the operational environment are defined. 11.3.1.3.6, 3rd paragraph, d), ii: ii. the package includes a security objectives rationale if security objectives for the operational environment are defined.; 12.4.1.3.12, 3rd paragraph, d), ii: ii. the package includes a security objectives rationale if security objectives for the environment are defined.;
Status	ma
Remarks	-

ID	CEM2022-R1-0013
Date	2023-12-22
Reference	10.4.1.3.9
Issue – Problem Description	Work unit APE_CCL.1-8: ‘The evaluator shall check, for each identified assurance package, that the package definition is complete. If the PP does not claim conformance to an

	assurance package, this work unit is not applicable and therefore considered to be satisfied. If the assurance package is a reference to one of the assurance packages contained in CC Part 5 then this work unit is also considered to be satisfied. The evaluator determines that the package definition is conformant to the requirements from CC Part 1, Clause 9 "Packages" by checking that the assurance package includes: […]' Missing line break after 'definition is complete.'.
Type	ed
Resolution - Correction / Interpretation	Use line break as identified in the problem description.
Status	ma
Remarks	-

ID	CEM2022-R1-0014
Date	2023-12-22
Reference	10.4.1.3.9, 11.3.1.3.8, 12.4.1.3.13
Issue – Problem Description	10.4.1.3.9, 1st paragraph, b): b) An assurance package overview, giving a narrative description of the security functionality; 11.3.1.3.8, 1st paragraph, b): b) An assurance package overview, giving a narrative description of the security functionality; 12.4.1.3.13, 1st paragraph, b): b) An assurance package overview, giving a narrative description of the security functionality; Problem: An assurance package does not provide any security functionality. (cf. [CC:2022-1], Clause 9)
Type	ed/te
Resolution - Correction / Interpretation	10.4.1.3.9, 1st paragraph, b): b) An assurance package overview, giving a narrative description of the purpose; 11.3.1.3.8, 1st paragraph, b): b) An assurance package overview, giving a narrative description of

	the purpose; 12.4.1.3.13, 1st paragraph, b): b) An assurance package overview, giving a narrative description of the purpose;
Status	ma
Remarks	-

ID	CEM2022-R1-0015
Date	2023-12-22
Reference	10.4.1.3.10
Issue – Problem Description	Work unit APE_CCL.1-9: 'The evaluator shall check that, for each identified functional package, the conformance claim states a claim of conformance to that package as one of package-conformant, package-augmented, or package-tailored. If the PP does not claim conformance to a functional package, this work unit is not applicable and therefore considered to be satisfied.' Missing line break after 'or package-tailored.'.
Type	ed
Resolution - Correction / Interpretation	Use line break as as identified in the problem description.
Status	ma
Remarks	-

ID	CEM2022-R1-0016
Date	2023-12-22
Reference	10.4.1.3.11
Issue – Problem Description	Problem: There is no action in case that the PP does not claim conformance to an assurance package. (cf. 10.4.1.3.10)
Type	te
Resolution - Correction / Interpretation	Add the following right after 1st paragraph of 10.4.1.3.11: If the PP does not claim conformance to an assurance package, this work unit is not applicable and therefore considered to be satisfied.
Status	ma

Remarks	-

ID	CEM2022-R1-0017
Date	2023-12-22
Reference	10.4.1.3.11 / 3rd paragraph
Issue – Problem Description	If the package conformance claim contains package-augmented, the evaluator determines that the PP contains all SARs included in the package, and at least one additional SAR or at least one SAR that is hierarchical to a SAR in the package. Problem: Hierarchically higher one is only applicable.
Type	ed/te
Resolution - Correction / Interpretation	If the package conformance claim contains package-augmented, the evaluator determines that the PP contains all SARs included in the package, and at least one additional SAR or at least one SAR that is hierarchically higher than a SAR in the package.
Status	ma
Remarks	-

ID	CEM2022-R1-0018
Date	2023-12-22
Reference	10.4.1.3 / CC Part 3 APE_CCL.1.13C:
Issue – Problem Description	CC Part 3 APE_CCL.1.13C: The conformance statement shall describe the conformance required of any PPs/STs to the PP as exact-PP, strict-PP or demonstrable-PP conformance. Problem: This shall be exactly identical to APE_CCL.1.13C in [CC:2022-3].
Type	ed/te
Resolution - Correction / Interpretation	CC Part 3 APE_CCL.1.13C: The conformance statement shall describe the conformance required of any PPs/STs to the PP as one of exact, strict or demonstrable conformance.
Status	ma
Remarks	-

ID	CEM2022-R1-0019
Date	2023-12-22
Reference	10.4.1.3.17 / APE_CCL.1-16
Issue – Problem Description	The evaluator ***shall check*** that the PP conformance statement states a claim of exact-PP, strict-PP or demonstrable-PP conformance. Problem: Work unit APE_CCL.1-16 shall require evaluator to check the PP conformance claim according to APE_CCL.1.13C.
Type	ed/te
Resolution - Correction / Interpretation	The evaluator shall check that the PP conformance statement states a claim one of exact, strict or demonstrable conformance.
Status	ma
Remarks	-

ID	CEM2022-R1-0020
Date	2023-12-22
Reference	10.7.1.3.6, 11.6.1.3.6, 12.7.1.3.6
Issue – Problem Description	10.7.1.3.6, 3rd paragraph: The evaluator determines that the extended functional component is consistent with CC Part 2, 6.1.3, Component structure. 11.6.1.3.6, 3rd paragraph: The evaluator determines that the extended functional component is consistent with CC Part 2, 6.1.3, Component structure. 12.7.1.3.6, 3rd paragraph: The evaluator determines that the extended functional component is consistent with CC Part 2, 6.1.4, Component structure. Problem: Reference is not correct.
Type	ed/te
Resolution - Correction / Interpretation	10.7.1.3.6, 3rd paragraph: The evaluator determines that the extended functional component is consistent with CC Part 2, 7.1.4, Component structure.

	11.6.1.3.6, 3rd paragraph: The evaluator determines that the extended functional component is consistent with CC Part 2, 7.1.4, Component structure. 12.7.1.3.6, 3rd paragraph: The evaluator determines that the extended functional component is consistent with CC Part 2, 7.1.4, Component structure.
Status	ma
Remarks	-

ID	CEM2022-R1-0021
Date	2023-12-22
Reference	10.7.1.3.6, 11.6.1.3.6, 12.7.1.3.6
Issue – Problem Description	10.7.1.3.6, 5th paragraph: If the extended functional component is hierarchical to an existing functional component, the evaluator determines that the extended functional component is consistent with CC Part 2, 6.2.1, Component changes highlighting. 11.6.1.3.6, 5th paragraph: If the extended functional component is hierarchical to an existing functional component, the evaluator determines that the extended functional component is consistent with CC Part 2, 6.2.1, Component changes highlighting. 12.7.1.3.6, 5th paragraph: If the extended functional component is hierarchical to an existing functional component, the evaluator determines that the extended functional component is consistent with CC Part 2, 6.2.2, Component changes highlighting. Problem: Reference is not correct. The “7.2.1 Component changes highlighting” section from CC Part 2 V3.1 R5 was removed. Instead, new [CC:2022-2] has a NOTE in the Introduction.
Type	ed/te
Resolution - Correction / Interpretation	10.7.1.3.6, 5th paragraph: If the extended functional component is hierarchical to an existing functional component, the evaluator determines that the extended functional component is consistent with CC Part 2, Introduction, NOTE. 11.6.1.3.6, 5th paragraph:

	If the extended functional component is hierarchical to an existing functional component, the evaluator determines that the extended functional component is consistent with CC Part 2, Introduction, NOTE. 12.7.1.3.6, 5th paragraph: If the extended functional component is hierarchical to an existing functional component, the evaluator determines that the extended functional component is consistent with CC Part 2, Introduction, NOTE.
Status	ma
Remarks	-

ID	CEM2022-R1-0022
Date	2023-12-22
Reference	10.7.1.3.7, 11.6.1.3.7, 12.7.1.3.7
Issue – Problem Description	10.7.1.3.7, 3rd paragraph: The evaluator determines that all new functional families are defined consistent with CC Part 2, 6.1.2, Family structure. 11.6.1.3.7, 3rd paragraph: The evaluator determines that all new functional families are defined consistent with CC Part 2, 6.1.2, Family structure. 12.7.1.3.7, 3rd paragraph: The evaluator determines that all new functional families are defined consistent with CC Part 2, 6.1.3, Family structure. Problem: Reference is not correct.
Type	ed/te
Resolution - Correction / Interpretation	10.7.1.3.7, 3rd paragraph: The evaluator determines that all new functional families are defined consistent with CC Part 2, 7.1.3, Family structure. 11.6.1.3.7, 3rd paragraph: The evaluator determines that all new functional families are defined consistent with CC Part 2, 7.1.3, Family structure. 12.7.1.3.7, 3rd paragraph: The evaluator determines that all new functional families are defined consistent with CC Part 2, 7.1.3, Family structure.

Status	ma
Remarks	-

ID	CEM2022-R1-0023
Date	2023-12-22
Reference	10.7.1.3.8, 11.6.1.3.8, 12.7.1.3.8
Issue – Problem Description	10.7.1.3.8, 3rd paragraph: The evaluator determines that all new functional classes are defined consistent with CC Part 2, 6.1.1, Class structure. 11.6.1.3.8, 3rd paragraph: The evaluator determines that all new functional classes are defined consistent with CC Part 2, 6.1.1, Class structure 12.7.1.3.8, 3rd paragraph: The evaluator determines that all new functional classes are defined consistent with CC Part 2, 6.1.2, Class structure. Problem: Reference is not correct.
Type	ed/te
Resolution - Correction / Interpretation	10.7.1.3.8, 3rd paragraph: The evaluator determines that all new functional classes are defined consistent with CC Part 2, 7.1.2, Class structure. 11.6.1.3.8, 3rd paragraph: The evaluator determines that all new functional classes are defined consistent with CC Part 2, 7.1.2, Class structure 12.7.1.3.8, 3rd paragraph: The evaluator determines that all new functional classes are defined consistent with CC Part 2, 7.1.2, Class structure.
Status	ma
Remarks	-

ID	CEM2022-R1-0024
Date	2023-12-22

Reference	10.7.1.3.9, 11.6.1.3.9, 12.7.1.3.9
Issue – Problem Description	10.7.1.3.9, 3rd paragraph: The evaluator determines that the extended assurance component definition is consistent with CC Part 3, 6.1.3, Assurance component structure. 10.7.1.3.9, 5th paragraph: If the extended assurance component is hierarchical to an existing assurance component, the evaluator determines that the extended assurance component is consistent with CC Part 3, 6.1.3, Assurance component structure. 11.6.1.3.9, 3rd paragraph: The evaluator determines that the extended assurance component definition is consistent with CC Part 3, 6.1.3, Assurance component structure. 11.6.1.3.9, 5th paragraph: If the extended assurance component is hierarchical to an existing assurance component, the evaluator determines that the extended assurance component is consistent with CC Part 3, 6.1.3, Assurance component structure. 12.7.1.3.9, 3rd paragraph: The evaluator determines that the extended assurance component definition is consistent with CC Part 3, 6.2, Assurance component structure. 12.7.1.3.9, 5th paragraph: If the extended assurance component is hierarchical to an existing assurance component, the evaluator determines that the extended assurance component is consistent with CC Part 3, 6.1.2, Assurance component structure. Problem: Reference is not correct.
Type	ed/te
Resolution - Correction / Interpretation	10.7.1.3.9, 3rd paragraph: The evaluator determines that the extended assurance component definition is consistent with CC Part 3, 6.4, Assurance component structure. 10.7.1.3.9, 5th paragraph: If the extended assurance component is hierarchical to an existing assurance component, the evaluator determines that the extended assurance component is consistent with CC Part 3, 6.4, Assurance component structure.

	11.6.1.3.9, 3rd paragraph: The evaluator determines that the extended assurance component definition is consistent with CC Part 3, 6.4, Assurance component structure. 11.6.1.3.9, 5th paragraph: If the extended assurance component is hierarchical to an existing assurance component, the evaluator determines that the extended assurance component is consistent with CC Part 3, 6.4, Assurance component structure. 12.7.1.3.9, 3rd paragraph: The evaluator determines that the extended assurance component definition is consistent with CC Part 3, 6.4, Assurance component structure. 12.7.1.3.9, 5th paragraph: If the extended assurance component is hierarchical to an existing assurance component, the evaluator determines that the extended assurance component is consistent with CC Part 3, 6.4, Assurance component structure.
Status	ma
Remarks	-

ID	CEM2022-R1-0025
Date	2023-12-22
Reference	10.7.1.3.11, 11.6.1.3.11, 12.7.1.3.11
Issue – Problem Description	10.7.1.3.11, 3rd paragraph: The evaluator determines that all new assurance families are defined consistent with CC Part 3, 6.1.2, Assurance family structure. 11.6.1.3.11, 3rd paragraph: The evaluator determines that all new assurance families are defined consistent with CC Part 3, 6.1.2, Assurance family structure. 12.7.1.3.11, 3rd paragraph: The evaluator determines that all new assurance families are defined consistent with CC Part 3, 6.1.2, Assurance family structure. Problem: Reference is not correct.
Type	ed/te

Resolution - Correction / Interpretation	10.7.1.3.11, 3rd paragraph: The evaluator determines that all new assurance families are defined consistent with CC Part 3, 6.3, Assurance family structure. 11.6.1.3.11, 3rd paragraph: The evaluator determines that all new assurance families are defined consistent with CC Part 3, 6.3 Assurance family structure. 12.7.1.3.11, 3rd paragraph: The evaluator determines that all new assurance families are defined consistent with CC Part 3, 6.3, Assurance family structure.
Status	ma
Remarks	-

ID	CEM2022-R1-0026
Date	2023-12-22
Reference	10.7.1.3.12, 11.6.1.3.12, 12.7.1.3.12
Issue – Problem Description	10.7.1.3.12, 3rd paragraph: The evaluator determines that all new assurance classes are defined consistent with CC Part 3, 6.1.1, Assurance class structure. 11.6.1.3.12, 3rd paragraph: The evaluator determines that all new assurance classes are defined consistent with CC Part 3, 6.1.1, Assurance class structure. 12.7.1.3.12, 3rd paragraph: The evaluator determines that all new assurance classes are defined consistent with CC Part 3, 6.1.1, Assurance class structure. Problem: Reference is not correct.
Type	ed/te
Resolution - Correction / Interpretation	10.7.1.3.12, 3rd paragraph: The evaluator determines that all new assurance classes are defined consistent with CC Part 3, 6.2, Assurance class structure. 11.6.1.3.12, 3rd paragraph: The evaluator determines that all new assurance classes are defined consistent with CC Part 3, 6.2, Assurance class structure.

	12.7.1.3.12, 3rd paragraph: The evaluator determines that all new assurance classes are defined consistent with CC Part 3, 6.2, Assurance class structure.
Status	ma
Remarks	-

ID	CEM2022-R1-0027
Date	2023-12-22
Reference	10.7.1.3.13 / 1st paragraph
Issue – Problem Description	The evaluator ***shall examine*** the extended components definition to determine that each element in each extended component is measurable and states objective evaluation requirements, such that conformance or nonconformance can be demonstrated. Problem: The auxiliary verb "can" should be replaced with "may" to be consistent description with the related Content and presentation element APE_ECD.1.5C. - APE_ECD.1.5C: The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements may be demonstrated.
Type	ed/te
Resolution - Correction / Interpretation	The evaluator ***shall examine*** the extended components definition to determine that each element in each extended component is measurable and states objective evaluation requirements, such that conformance or nonconformance may be demonstrated.
Status	ma
Remarks	-

ID	CEM2022-R1-0028
Date	2023-12-22
Reference	10.8.1.3.2, 10.8.1.3.3
Issue – Problem Description	10.8.1.3.2, 2nd paragraph: The evaluator determines that each SFR is identified by one of the following means: a) ... b) ... c) by reference to a PP that the PP claims to be conformant with

	including any optional requirements defined in the PP; d) by reference to a security requirements package that the PP claims to be conformant with; e) .... 10.8.1.3.3, 2nd paragraph: The evaluator determines that each SAR is identified by one of the following means: a) ... b) ... c) by reference to a PP that the PP claims to be conformant with; d) by reference to a security requirements package that the PP claims to be conformant with; e) .... Problem: Each SFR/SAR is identified by reference to "an individual component" in a PP or a security requirements package, not by reference to a PP or a security requirements package itself. (Cf. APE_REQ.2-1.)
Type	ed/te
Resolution - Correction / Interpretation	10.8.1.3.2, 2nd paragraph: The evaluator determines that each SFR is identified by one of the following means: a) ... b) ... c) by reference to an individual component in a PP that the PP claims to be conformant with including any optional requirements defined in the PP; d) by reference to an individual component in a security requirements package that the PP claims to be conformant with; e) .... 10.8.1.3.3, 2nd paragraph: The evaluator determines that each SAR is identified by one of the following means: a) ... b) ... c) by reference to an individual component in a PP that the PP claims to be conformant with; d) by reference to an individual component in a security requirements package that the PP claims to be conformant with; e) ....

Status	ma
Remarks	-

ID	CEM2022-R1-0029
Date	2023-12-22
Reference	10.8.1.3.12, 11.7.1.3.12
Issue – Problem Description	10.8.1.3.12, 1st paragraph & 11.7.1.3.12, 1st paragraph: The evaluator ***shall examine*** the security requirements rationale to determine that for each threat it demonstrates that the SFRs are suitable to meet that threat. Problem: According to the definition of [CEM:2022], 3.12, here the verb "justify" shall be used.
Type	te
Resolution - Correction / Interpretation	10.8.1.3.12, 1st paragraph & 11.7.1.3.12, 1st paragraph: The evaluator ***shall examine*** the security requirements rationale to determine that for each threat it justifies that the SFRs are suitable to meet that threat.
Status	ma
Remarks	-

ID	CEM2022-R1-0030
Date	2023-12-22
Reference	10.8.1.3.12, 11.7.1.3.12
Issue – Problem Description	10.8.1.3.12, 2nd paragraph: If no SFRs trace back to a threat, the evaluator action related to this work unit is assigned a fail verdict. 11.7.1.3.12, 2nd paragraph: If no SFRs trace back to a threat, the evaluator action related to this work unit is assigned a fail verdict. Problem: In a direct rationale PP, there are no security objectives for the TOE. So, threats are countered by either security objectives for the operational environment and/or SFRs (Refer to APE_OBJ.1-2). For this reason, the

	statement above is not true. Here, the evaluation sub-activity for APE_REQ.1 only addresses the rationale between SFRs and threats and it is not sufficient to address all threats, therefore the work unit APE_REQ.1-11 shall address the rationale in combination with APE_OBJ.1-2.
Type	te
Resolution - Correction / Interpretation	10.8.1.3.12, 2nd paragraph: If no SFRs trace back to a threat and the evaluator determines that also no security objectives for the operational environment trace back to that threat in APE_OBJ.1-2, the evaluator action related to this work unit is assigned a fail verdict. 11.7.1.3.12, 2nd paragraph: If no SFRs trace back to a threat and the evaluator determines that also no security objectives for the operational environment trace back to that threat in ACE_OBJ.1-2, the evaluator action related to this work unit is assigned a fail verdict.
Status	ma
Remarks	-

ID	CEM2022-R1-0031
Date	2023-12-22
Reference	10.8.1.3.13, 11.7.1.3.13
Issue – Problem Description	10.8.1.3.13, 2nd paragraph: If no SFRs or security objectives for the operational environment trace back to the OSP, the evaluator action related to this work unit is assigned a fail verdict. 11.7.1.3.13, 2nd paragraph: If no SFRs or security objectives for the operational environment trace back to the OSP, the evaluator action related to this work unit is assigned a fail verdict. Problem: Cf. CEM2022-R1-0029. In a direct rationale PP, there are no security objectives for the TOE. So, OSPs are enforced by either security objectives for the operational environment and/or SFRs (Refer to APE_OBJ.1-2). For this reason, the statement above is true. But the evaluation sub-activity for APE_REQ.1 only addresses the rationale between SFRs and OSPs. The rationale between security objectives for the

	operational environments and OSPs is addressed in APE_OBJ.1. Therefore the work unit APE_REQ.1-12 shall address the rationale in combination with APE_OBJ.1-2.
Type	te
Resolution - Correction / Interpretation	10.8.1.3.13, 2nd paragraph: If no SFRs trace back to the OSP and the evaluator determines that also no security objectives for the operational environment trace back to that OSP in APE_OBJ.1-2, the evaluator action related to this work unit is assigned a fail verdict. 11.7.1.3.13, 2nd paragraph: If no SFRs trace back to the OSP and the evaluator determines that also no security objectives for the operational environment trace back to that OSP in ACE_OBJ.1-2, the evaluator action related to this work unit is assigned a fail verdict.
Status	ma
Remarks	-

ID	CEM2022-R1-0032
Date	2023-12-22
Reference	10.8.1.3.13, 11.7.1.3.13
Issue – Problem Description	10.8.1.3.13, 3rd paragraph: The evaluator determines that the justification for an OSP demonstrates that the security objectives are sufficient: if all SFRs that trace back to that OSP are achieved then, in the context of any applicable assumptions, the OSP is enforced. 11.7.1.3.13, 3rd paragraph: The evaluator determines that the justification for an OSP demonstrates that the security objectives are sufficient: if all SFRs that trace back to that OSP are achieved then, in the context of any applicable assumptions, the OSP is enforced. Problem: The work unit APE_REQ.1-11 covers the security requirements rationale not the security objectives rationale.
Type	te
Resolution - Correction / Interpretation	10.8.1.3.13, 3rd paragraph: The evaluator determines that the justification for an OSP demonstrates that the SFRs are sufficient: if all SFRs that trace back to that OSP are achieved

	then, in the context of any applicable assumptions, the OSP is enforced. 11.7.1.3.13, 3rd paragraph: The evaluator determines that the justification for an OSP demonstrates that the SFRs are sufficient: if all SFRs that trace back to that OSP are achieved then, in the context of any applicable assumptions, the OSP is enforced.
Status	ma
Remarks	-

ID	CEM2022-R1-0033
Date	2023-12-22
Reference	10.8.2.3.3 / last paragraph
Issue – Problem Description	Note that if optional requirements are defined by the PP, there may be associated threats that are covered by this work unit. Problem: APE_REQ.2-2 is intended to check that the statement of security requirements describes the SARs. The last paragraph is not related to the work unit.
Type	te
Resolution - Correction / Interpretation	*<Remove the last paragraph>*
Status	ma
Remarks	-

ID	CEM2022-R1-0034
Date	2023-12-22
Reference	10.8.2.3.11 / 2nd paragraph
Issue – Problem Description	Optional requirements may require Threats/OSPs to be specified, and security objectives associated with these SPD elements are also covered by this work unit. Problem: APE_REQ.2-10 is intended to check the security requirements rationale in terms of SFRs and security objectives. The 2nd paragraph might be misleading in view of the contents and intent of the work unit.

Type	te
Resolution - Correction / Interpretation	In CC Part 1, section 7.3.2.6, A. the following is described for optional requirements (of any type): "NOTE Optional requirements can be written in response to SPD-elements that exist in the package, PP or PP-Module, or SPD-elements that are specifically associated with the requirement. Such associations are identified in the package, PP or PP-Module. A Direct Rationale package, PP, PP-Module or ST do not define security objectives for optional requirements that have associated SPD elements, while a regular package, PP, PP-Module or ST includes security objectives for the associated SFRs and SPD elements." Update of the cited text as follows: Security objectives associated with optional requirements also have to be considered for the security requirements rationale and related activities in this work unit.
Status	ma
Remarks	-

ID	CEM2022-R1-0035
Date	2023-12-22
Reference	11.2.1.3 / Application notes
Issue – Problem Description	11.2.1.3 Application notes All actions of APE_INT.1.1E hold. Problem: Compared to previous version of CEM, [CEM:2022] introduces all work units necessary for ACE_INT.1.1E. So, application notes above is not necessary here.
Type	te
Resolution - Correction / Interpretation	*<Remove application notes>* Deletion of section 11.2.1.3. Re-numbering of subsequent sections: Replace section numbers 11.2.1.4 by 11.2.1.3 and 11.2.1.4.* by 11.2.1.3.*.
Status	ma
Remarks	-

ID	CEM2022-R1-0036
Date	2023-12-22

Reference	11.3.1.3.1 / ACE_CCL.1-1
Issue – Problem Description	The evaluator shall check that the conformance claim identifies the version of the CC to which the PP-Module claims conformance. The evaluator determines that the CC conformance claim identifies the version of the CC that was used to develop this PP-Module. This should include the version number of the CC and, unless the English version of the CC was used, the language of the version of the CC that was used. Problem: The work unit shall be consistent with Content and presentation elements (i.e., ACE_CCL.1.1C) (Cf. APE_CCL.1-1)
Type	ed/te
Resolution - Correction / Interpretation	The evaluator shall check that the conformance claim identifies the edition of the CC to which the PP-Module claims conformance. The evaluator determines that the CC conformance claim identifies the edition of the CC that was used to develop this PP-Module. This should include the edition number of the CC and, unless the English edition of the CC was used, the language of the edition of the CC that was used.
Status	ma
Remarks	-

ID	CEM2022-R1-0037
Date	2023-12-22
Reference	11.3.1.3.5 / 2nd paragraph, 3rd paragraph
Issue – Problem Description	If the CC conformance claim contains CC Part 2 and/or CC Part 3 conformant, the evaluator determines that the extended components definition does not define functional/assurance components. If the CC conformance claim contains CC Part 2 and/or CC Part 3 extended, the evaluator determines that the extended components definition defines at least one extended functional/assurance component. Problem: Relevant section of the PP-Module is the “conformance claim” section.
Type	ed/te
Resolution - Correction / Interpretation	If the conformance claim contains CC Part 2 and/or CC Part 3 conformant, the evaluator determines that the extended components definition does not define functional/assurance components. If the conformance claim contains CC Part 2 and/or CC Part 3 extended, the evaluator determines that the extended components definition defines at

	least one extended functional/assurance component.
Status	ma
Remarks	-

ID	CEM2022-R1-0038
Date	2023-12-22
Reference	11.3.1.3.7 / 1st paragraph
Issue – Problem Description	The evaluator shall check that, for each identified package, the conformance claim states a claim of either package-conformant, package-augmented or package-tailored. Problem: The work unit ACE_CCL.1-7 is addressing functional packages. (Cf. ACE_CCL.1-8 for assurance packages)
Type	ed/te
Resolution - Correction / Interpretation	The evaluator shall check that, for each identified functional package, the conformance claim states a claim of either package-conformant, package-augmented or package-tailored.
Status	ma
Remarks	-

ID	CEM2022-R1-0039
Date	2023-12-22
Reference	11.3.1.3.12 / 1st paragraph / a)
Issue – Problem Description	a) if any derived Evaluation Methods and Evaluation Activities are required by other items used with the PP-Module (e.g. a base PP), or required by other items to which the PP-Module claims conformance (e.g. packages), then these are all identified in the PP-Module under evaluation, along with any derived Evaluation Methods and Evaluation Activities that the PP-Module itself requires; Problem: Improper example.
Type	ed/te
Resolution - Correction / Interpretation	a) if any derived Evaluation Methods and Evaluation Activities are required by other items used with the PP-Module (e.g. a PP-Module base), or required by other items to which the PP-Module claims conformance

	(e.g. packages), then these are all identified in the PP-Module under evaluation, along with any derived Evaluation Methods and Evaluation Activities that the PP-Module itself requires;
Status	ma
Remarks	-

ID	CEM2022-R1-0040
Date	2023-12-22
Reference	11.4.1.1, 11.4.1.3.2
Issue – Problem Description	11.4.1.1, 1st paragraph: The objective of this sub-activity is to determine that the security problem intended to be addressed by the PP-Module and its operational environment is clearly defined. 11.4.1.3.2, 3rd paragraph: The evaluator determines that the security problem definition describes the threats that must be countered by the PP-Module and/or its operational environment. Problem: SPD is always defined in terms of the TOE and its operational environment. (Refer to the [CC:2022-3], 8.4.1 and 8.4.2.)
Type	ed/te
Resolution - Correction / Interpretation	11.4.1.1, 1st paragraph: The objective of this sub-activity is to determine that the security problem intended to be addressed by the TOE and its operational environment is clearly defined. 11.4.1.3.2, 3rd paragraph: The evaluator determines that the security problem definition describes the threats that must be countered by the TOE and/or its operational environment.
Status	ma
Remarks	-

ID	CEM2022-R1-0041
Date	2023-12-22

Reference	11.5.1
Issue – Problem Description	Problem: Subclauses “Objectives” and “Input” are missing.
Type	te
Resolution - Correction / Interpretation	11.5.1.1 Objectives The objective of this sub-activity is to determine whether the security objectives for the operational environment are clearly defined. 11.5.1.2 Input The evaluation evidence for this sub-activity is: a) the PP-Module. Subsequent section numbers have to be shifted accordingly: 11.5.1.1 → 11.5.1.3 11.5.1.2 → 11.5.1.4 11.5.1.2.x → 11.5.1.4.x
Status	ma
Remarks	-

ID	CEM2022-R1-0042
Date	2023-12-22
Reference	11.5.1.2.4
Issue – Problem Description	**11.5.1.2.4 Work unit APE_OBJ.1-3** Problem: Reference to the work unit is incorrect.
Type	ed/te
Resolution - Correction / Interpretation	**11.5.1.2.4 Work unit ACE_OBJ.1-3**
Status	ma
Remarks	-

ID	CEM2022-R1-0043
Date	2023-12-22

Reference	11.5.2.3.5 / Below CC Part 3 ACE_OBJ.2.5C
Issue – Problem Description	Problem: A subclause title for work unit ACE_OBJ.2-5 is missing.
Type	ed/te
Resolution - Correction / Interpretation	**11.5.2.3.6 Work unit ACE_OBJ.2-5** Subsequent section number has to be shifted accordingly: 11.5.2.3.6 → 11.5.2.3.7
Status	ma
Remarks	-

ID	CEM2022-R1-0044
Date	2023-12-22
Reference	below 11.6.1.3.12 / CC Part 3 ACE_ECD.1.5C
Issue – Problem Description	CC Part 3 ACE_ECD.1.5C: *The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.* Problem: This shall be exactly identical to ACE_ECD.1.5C in [CC:2022-3].
Type	ed/te
Resolution - Correction / Interpretation	CC Part 3 ACE_ECD.1.5C: *The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements may be demonstrated.*
Status	ma
Remarks	-

ID	CEM2022-R1-0045
Date	2023-12-22
Reference	11.7.1.3.2, 11.7.1.3.3
Issue – Problem Description	11.7.1.3.2, 2nd paragraph: The evaluator determines that each SFR is identified by one of the following means: a) ...

	b) ... c) by reference to a security requirements package that the PP-Module claims to be conformant with; d) .... 11.7.1.3.3, 2nd paragraph: The evaluator determines that each SAR is identified by one of the following means: a) ... b) ... c) by reference to a security requirements package that the PP-Module claims to be conformant with; d) .... Problem: Each SFR/SAR is identified by reference to "an individual component" in a PP or a security requirements package, not by reference to a PP or a security requirements package itself. (Cf. ACE_REQ.2-1.)
Type	ed/te
Resolution - Correction / Interpretation	11.7.1.3.2, 2nd paragraph: The evaluator determines that each SFR is identified by one of the following means: a) ... b) ... c) by reference to an individual component in a security requirements package that the PP-Module claims to be conformant with; d) .... 11.7.1.3.3, 2nd paragraph: The evaluator determines that each SAR is identified by one of the following means: a) ... b) ... c) by reference to an individual component in a security requirements package that the PP-Module claims to be conformant with; d) ....
Status	ma
Remarks	-

ID	CEM2022-R1-0046
Date	2023-12-22
Reference	11.7.2.3.3 / last paragraph
Issue – Problem Description	Note that if optional requirements are defined by the PP-Module, there may be associated threats that are covered by this work unit. Problem: ACE_REQ.2-2 is intended to check that the statement of security requirements describes the SARs. The last paragraph is not related to the work unit.
Type	te
Resolution - Correction / Interpretation	*<Remove the last paragraph>*
Status	ma
Remarks	-

ID	CEM2022-R1-0047
Date	2023-12-22
Reference	11.7.2.3.11 / 2nd paragraph
Issue – Problem Description	Optional requirements may require Threats/OSPs to be specified, and security objectives associated with these SPD elements are also covered by this work unit. Problem: ACE_REQ.2-10 is intended to check the security requirements rationale in terms of SFRs and security objectives. The 2nd paragraph might be misleading in view of the contents and intent of the work unit.
Type	te
Resolution - Correction / Interpretation	In CC Part 1, section 7.3.2.6, A. the following is described for optional requirements (of any type): "NOTE Optional requirements can be written in response to SPD-elements that exist in the package, PP or PP-Module, or SPD-elements that are specifically associated with the requirement. Such associations are identified in the package, PP or PP-Module. A Direct Rationale package, PP, PP-Module or ST do not define security objectives for optional requirements that have associated SPD elements, while a regular package, PP, PP-Module or ST includes security objectives for the associated SFRs and SPD elements." Update of the cited text as follows: Security objectives associated with optional requirements also have to be considered for the security requirements rationale and related activities in

	this work unit.
Status	ma
Remarks	-

ID	CEM2022-R1-0048
Date	2023-12-22
Reference	11.8.1.3.4 / 2nd paragraph / a) & b)
Issue – Problem Description	a) the statements of threats, assumptions and OSPs in the PP-Module do not contradict those drawn from any functional packages to which it claims conformance; b) the statement of assumptions in the PP-Module addresses aspects out of scope of any functional packages to which it claims conformance, in which case, the addition of elements is allowed. Problem: The work unit ACE_MCO.1-3 is addressing the PP-Module base. (Cf. ACE_MCO.1-4 is addressing functional packages.)
Type	te
Resolution - Correction / Interpretation	a) the statements of threats, assumptions and OSPs in the PP-Module do not contradict those drawn from its PP-Module base(s); b) the statement of assumptions in the PP-Module addresses aspects out of scope of its PP-Module base(s), in which case, the addition of elements is allowed.
Status	ma
Remarks	-

ID	CEM2022-R1-0049
Date	2023-12-22
Reference	11.8.1.3.5 / 2nd paragraph / a) & b)
Issue – Problem Description	a) the statements of threats, assumptions and OSPs in the PP-Module do not contradict those from the PP-Module Base; b) the statement of assumptions in the PP-Module addresses aspects out of scope of the PP-Module Base, in which case, the addition of elements is allowed. Problem: The work unit ACE_MCO.1-4 is addressing functional packages.

	(Cf. ACE_MCO.1-3 is addressing the PP-Module Base.)
Type	te
Resolution - Correction / Interpretation	a) the statements of threats, assumptions and OSPs in the PP-Module do not contradict those from any functional packages to which it claims conformance; b) the statement of assumptions in the PP-Module addresses aspects out of scope of any functional packages to which it claims conformance, in which case, the addition of elements is allowed.
Status	ma
Remarks	-

ID	CEM2022-R1-0050
Date	2023-12-22
Reference	11.8.1.3.6, 11.8.1.3.7, 11.8.1.3.8
Issue – Problem Description	**11.8.1.3.6 Work unit ACE_MCO.1-5** For all the assets that are shared between the PP-Module and a base PP or PP-Module, the evaluator shall determine that all the differences in the security problem definitions are justified. For instance, the asset resides in different locations or at different times or is subject to different operational environment conditions. In particular, the evaluator examines the consistency rationale to determine that: a) the statements of security objectives for the TOE and the security objectives for the operational environment the PP-Module do not contradict those drawn from any functional packages to which it claims conformance; b) the statement of security objectives for the operational environment in the PP-Module addresses aspects out of scope of any functional packages to which it claims conformance, in which case, the addition of elements is allowed. **11.8.1.3.7 Work unit ACE_MCO.1-6** The evaluator shall examine the PP-Module consistency rationale to determine that it demonstrates that the statement of security objectives of the PP-Module is consistent with the statement of security objectives of its PP-Module Base. **11.8.1.3.8 Work unit ACE_MCO.1-7** The evaluator shall examine the PP-Module consistency rationale to determine that it demonstrates that the statement of security objectives of the PP-Module is consistent with the statement of security objectives of any functional package for which conformance is being claimed. Where the PP-Module and its PP-Module Base use the Direct Rationale

	approach then this work unit is trivially satisfied for the TOE objectives (because these are not included under the Direct Rationale approach). If any of the PP-Module or its PP-Module Base use the Direct Rationale approach then the PP-Module and all elements of its PP-Module Base must use the Direct Rationale approach, otherwise the evaluator action related to this work unit is assigned a fail verdict. In particular, the evaluator examines the consistency rationale to determine that: a) the statements of the security objectives for the TOE and the security objectives for the operational environment in the PP-Module do not contradict those from the PP-Module Base; b) the statement of the security objectives for the operational environment in the PP-Module addresses aspects out of scope of the PP-Module Base, in which case, the addition of elements is allowed. Problem: For the 1st paragraph of 11.8.1.3.6, "a base PP or PP-Module" shall be replaced with "its PP-Module Base(s) or any functional packages to which it claims conformance". The 2nd paragraph of 11.8.1.3.6 is addressing a part of actions related to ACE_MCO.1-6. So, the paragraph shall be moved below the 1st paragraph of 11.8.1.3.7. Also, For bullets a) and b), "any functional packages to which it claims conformance" shall be replaced with "its PP-Module Base(s)". For the 1st paragraph of 11.8.1.3.7, "its PP-Module Base" shall be replaced with "its PP-Module Base(s)". The 2nd paragraph of 11.8.1.3.8 is addressing Direct rationale PP-Module and its PP-Module Base(s). So, the paragraph shall be moved below the 1st paragraph of 11.8.3.7. For the 3rd paragraph of 11.8.1.3.8, "the PP-Module Base" shall be replaced with "any functional packages to which is claims conformance". All in all, the issue and its resolution only address re-ordering of already contained contents for WUs as currently text sections are mixed up and erroneously appointed to the three impacted WUs (more or less only editorial issue).
Type	ed/te
Resolution - Correction / Interpretation	**11.8.1.3.6 Work unit ACE_MCO.1-5** For all the assets that are shared between the PP-Module and its PP-Module Base(s) or any functional packages to which it claims conformance, the evaluator shall determine that all the differences in the security problem definitions are justified. For instance, the asset resides in different locations or at different times or is subject to different operational environment conditions. **11.8.1.3.7 Work unit ACE_MCO.1-6** The evaluator shall examine the PP-Module consistency rationale to determine that it demonstrates that the statement of security objectives of the PP-Module is consistent with the statement of security objectives of its

	PP-Module Base(s). Where the PP-Module and its PP-Module Base use the Direct Rationale approach then this work unit is trivially satisfied for the TOE objectives (because these are not included under the Direct Rationale approach). If any of the PP-Module or its PP-Module Base use the Direct Rationale approach then the PP-Module and all elements of its PP-Module Base must use the Direct Rationale approach, otherwise the evaluator action related to this work unit is assigned a fail verdict. In particular, the evaluator examines the consistency rationale to determine that: a) the statements of security objectives for the TOE and the security objectives for the operational environment in the PP-Module do not contradict those drawn from its PP-Module Base(s); b) the statement of security objectives for the operational environment in the PP-Module addresses aspects out of scope of its PP-Module Base(s), in which case, the addition of elements is allowed. **11.8.1.3.8 Work unit ACE_MCO.1-7** The evaluator shall examine the PP-Module consistency rationale to determine that it demonstrates that the statement of security objectives of the PP-Module is consistent with the statement of security objectives of any functional package for which conformance is being claimed. In particular, the evaluator examines the consistency rationale to determine that: a) the statements of the security objectives for the TOE and the security objectives for the operational environment in the PP-Module do not contradict those from any functional packages to which is claims conformance; b) the statement of the security objectives for the operational environment in the PP-Module addresses aspects out of scope of any functional packages to which is claims conformance, in which case, the addition of elements is allowed.
Status	ma
Remarks	-

ID	CEM2022-R1-0051
Date	2023-12-22
Reference	11.8.1.3.9, 11.8.1.3.10
Issue – Problem Description	11.8.1.3.9, 1st paragraph: The evaluator shall examine the consistency rationale to determine that the statement of security requirements of the PP-Module is consistent with the statement of security requirements of its PP-Module Base, i.e. the SFRs of the PP-Module either complete or refine the SFRs of the PP-Module Base

	and no contradiction arises from the whole set of SFRs of the PP-Module and the PP-Module Base. 11.8.1.3.10, 1st paragraph: The evaluator shall examine the consistency rationale to determine that the statement of security requirements of the PP-Module is consistent with the statement of security requirements of any functional package for which conformance is being claimed, i.e. the SFRs of the PP-Module either complete or refine the SFRs of the claimed functional packages and no contradiction arises from the whole set of SFRs of the PP-Module and those of the functional packages for which conformance is claimed. Problem: The work unit shall be consistent with the related Content and presentation elements in terms of the scope of action.
Type	ed/te
Resolution - Correction / Interpretation	11.8.1.3.9, 1st paragraph: The evaluator shall examine the consistency rationale to determine that the statement of security functional requirements of the PP-Module is consistent with the statement of security functional requirements of its PP-Module Base, i.e. the SFRs of the PP-Module either complete or refine the SFRs of the PP-Module Base and no contradiction arises from the whole set of SFRs of the PP-Module and the PP-Module Base. 11.8.1.3.10, 1st paragraph: The evaluator shall examine the consistency rationale to determine that the statement of security functional requirements of the PP-Module is consistent with the statement of security functional requirements of any functional package for which conformance is being claimed, i.e. the SFRs of the PP-Module either complete or refine the SFRs of the claimed functional packages and no contradiction arises from the whole set of SFRs of the PP-Module and those of the functional packages for which conformance is claimed.
Status	ma
Remarks	-

ID	CEM2022-R1-0052
Date	2023-12-22
Reference	11.9.1.3.19
Issue – Problem Description	11.9.1.3.19, 1st paragraph, a): a) If any derived Evaluation Methods and Evaluation Activities are required by other items included in the PP-Configuration (e.g. a base PP or

	PP-Module), or required by other items to which the PP-Configuration claims conformance (e.g. packages), then these are all identified in the PP-Configuration under evaluation, along with any derived Evaluation Methods and Evaluation Activities that the PP-Configuration itself chooses to require; 11.9.1.3.19, last paragraph: Where exact conformance is required then the PP-Configuration is not permitted to define its own requirements for derived Evaluation Methods and Evaluation Activities: it can only use those required by the other items (e.g. a base PP or PP-Module) in the PP-Configuration. Problem: Improper example.
Type	ed/te
Resolution - Correction / Interpretation	11.9.1.3.19, 1st paragraph, a): a) If any derived Evaluation Methods and Evaluation Activities are required by other items included in the PP-Configuration (e.g. a PP-Module Base or PP-Module), or required by other items to which the PP-Configuration claims conformance (e.g. packages), then these are all identified in the PP-Configuration under evaluation, along with any derived Evaluation Methods and Evaluation Activities that the PP-Configuration itself chooses to require; 11.9.1.3.19, last paragraph: Where exact conformance is required then the PP-Configuration is not permitted to define its own requirements for derived Evaluation Methods and Evaluation Activities: it can only use those required by the other items (e.g. a PP-Module Base or PP-Module) in the PP-Configuration.
Status	ma
Remarks	-

ID	CEM2022-R1-0053
Date	2023-12-22
Reference	12.4.1.3.13 / last paragraph
Issue – Problem Description	A security requirements rationale that provides the rationale for selecting the assurance components/ requirements included in the package. Problem: The paragraph shall be bullet f) of the previous paragraph.
Type	ed
Resolution - Correction /	a) … b) …

Interpretation	c) … d) … e) … f) A security requirements rationale that provides the rationale for selecting the assurance components/requirements included in the package.
Status	ma
Remarks	-

ID	CEM2022-R1-0054
Date	2023-12-22
Reference	12.4.1.3.14
Issue – Problem Description	Problem: The work unit ASE_CCL.1-13 addresses the identification of packages in the ST conformance claim. So, this work unit is more applicable for ASE_CCL.1.5C instead of ASE_CCL.1.6C.
Type	te
Resolution - Correction / Interpretation	*<Move 12.4.1.3.14 under ASE_CCL.1.5C>*
Status	ma
Remarks	-

ID	CEM2022-R1-0055
Date	2023-12-22
Reference	12.4.1.3.18 / paragraph just before the last paragraph / 1st and 3rd bullets
Issue – Problem Description	• all TOEs that would meet the security problem definition in the ST also meet the security problem definition in the PP/PP-Configuration. This can also be shown indirectly by demonstrating that every event, which realises a threat defined in the PP or violates an OSP defined in the PP/PP-Configuration, would also realise a threat stated in the ST or violate an OSP defined in the ST. Note that fulfilling an OSP stated in the ST may avert a threat stated in the PP/PP-Configuration or that averting a threat stated in the ST may fulfil an OSP stated in the PP/PP-Configuration, so threats and OSPs can substitute each other; • besides a set of assumptions in the ST needed to demonstrate conformance to the SPD of the PP/PP-Configuration, an ST may specify further assumptions, but only if these additional assumptions are independent of and do not affect the security problem definition as defined in the PP/PP-Configuration. More detailed, there are no

	assumptions in the ST that exclude threats to the TOE that need to be countered by the TOE according to the PP. Similarly, there are no assumptions in the ST that realise aspects of an OSP stated in the PP/PP-Configuration, which are meant to be fulfilled by the TOE according to the PP/PP-Configuration. Problem: PP-Configuration shall be addressed together with PP.
Type	te
Resolution - Correction / Interpretation	• all TOEs that would meet the security problem definition in the ST also meet the security problem definition in the PP/PP-Configuration. This can also be shown indirectly by demonstrating that every event, which realises a threat defined in the PP/PP-Configuration or violates an OSP defined in the PP/PP-Configuration, would also realise a threat stated in the ST or violate an OSP defined in the ST. Note that fulfilling an OSP stated in the ST may avert a threat stated in the PP/PP-Configuration or that averting a threat stated in the ST may fulfil an OSP stated in the PP/PP-Configuration, so threats and OSPs can substitute each other; • besides a set of assumptions in the ST needed to demonstrate conformance to the SPD of the PP/PP-Configuration, an ST may specify further assumptions, but only if these additional assumptions are independent of and do not affect the security problem definition as defined in the PP/PP-Configuration. More detailed, there are no assumptions in the ST that exclude threats to the TOE that need to be countered by the TOE according to the PP/PP-Configuration. Similarly, there are no assumptions in the ST that realise aspects of an OSP stated in the PP/PP-Configuration, which are meant to be fulfilled by the TOE according to the PP/PP-Configuration.
Status	ma
Remarks	-

ID	CEM2022-R1-0056
Date	2023-12-22
Reference	12.4.1.3.20
Issue – Problem Description	12.4.1.3.20, 5th paragraph: If exact conformance is required by the PP/PP-Configuration to which conformance is being claimed, no conformance claim rationale is required. Instead, the evaluator determines that the statement of security requirements in the PP to which conformance is being claimed is exactly reproduced in the ST, with the following allowances: 12.4.1.3.20, 7th paragraph: If strict conformance is required by the PP to which conformance is being claimed, no conformance claim rationale is required. Instead, the evaluator

	determines whether the statement of security requirements in the ST is a superset of, or identical to, the statement of security requirements in the PP to which conformance is being claimed (for strict conformance). Problem: PP-Configuration shall be addressed together with PP.
Type	te
Resolution - Correction / Interpretation	12.4.1.3.20, 5th paragraph: If exact conformance is required by the PP/PP-Configuration to which conformance is being claimed, no conformance claim rationale is required. Instead, the evaluator determines that the statement of security requirements in the PP/PP-Configuration to which conformance is being claimed is exactly reproduced in the ST, with the following allowances: 12.4.1.3.20, 7th paragraph: If strict conformance is required by the PP/PP-Configuration to which conformance is being claimed, no conformance claim rationale is required. Instead, the evaluator determines whether the statement of security requirements in the ST is a superset of, or identical to, the statement of security requirements in the PP/PP-Configuration to which conformance is being claimed (for strict conformance).
Status	ma
Remarks	-

ID	CEM2022-R1-0057
Date	2023-12-22
Reference	12.8.1.3.2, 12.8.1.3.3
Issue – Problem Description	12.8.1.3.2, 2nd paragraph: The evaluator determines that each SFR is identified by one of the following means: a) ... b) ... c) by reference to a PP that the ST claims to be conformant with including any optional requirements defined in the PP; d) by reference to a security requirements package that the ST claims to be conformant with; e) .... 12.8.1.3.3, 2nd paragraph: The evaluator determines that each SAR is identified by one of the following means: a) ...

	b) ... c) by reference to a PP that the ST claims to be conformant with; d) by reference to a security requirements package that the ST claims to be conformant with; e) .... Problem: Each SFR/SAR is identified by reference to "an individual component" in a PP or a security requirements package, not by reference to a PP or a security requirements package itself. (Cf. ASE_REQ.2-1.)
Type	ed/te
Resolution - Correction / Interpretation	12.8.1.3.2, 2nd paragraph: The evaluator determines that each SFR is identified by one of the following means: a) ... b) ... c) by reference to an individual component in a PP that the ST claims to be conformant with including any optional requirements defined in the PP; d) by reference to an individual component in a security requirements package that the ST claims to be conformant with; e) .... 12.8.1.3.3, 2nd paragraph: The evaluator determines that each SAR is identified by one of the following means: a) ... b) ... c) by reference to an individual component in a PP that the ST claims to be conformant with; d) by reference to an individual component in a security requirements package that the ST claims to be conformant with; e) ....
Status	ma
Remarks	-

ID	CEM2022-R1-0058
Date	2023-12-22
Reference	12.8.1.3.3, 12.8.2.3.3
Issue –	12.8.1.3.3, last paragraph:

Problem Description	Note that if optional requirements are defined by the PP, there may be associated threats that are covered by this work unit. 12.8.2.3.3, last paragraph: Note that if optional requirements are defined by the PP, there may be associated threats that are covered by this work unit. Problem: ASE_REQ.1-2 and ASE_REQ.2-2 are intended to check that the statement of security requirements describes the SARs. The last paragraph is not related to the work unit.
Type	te
Resolution - Correction / Interpretation	*<Remove the last paragraph>*
Status	ma
Remarks	-

ID	CEM2022-R1-0059
Date	2023-12-22
Reference	between 12.8.1.3.15 and 12.8.1.3.16
Issue – Problem Description	Problem: The change proposal CC2022-P3-R1-0015 from [CC:2022-3] shall be addressed here. ASE_REQ.1.8C and ASE_REQ.1.9C require to demonstrate the security requirements rationale in terms of threats and OSPs. But there is no explicit element to require to trace each SFR back to them. (cf. APE_REQ.1.6C and ACE_REQ.1.6C) When a new Content and presentation element is defined here, then related work unit shall be added too. (cf. APE_REQ.1-10, APE_REQ.1-11 and APE_REQ.1-12)
Type	te
Resolution - Correction / Interpretation	*<Separate the existing work unit properly, and add new work unit referencing APE_ REQ.1-10, APE_REQ.1-11 and APE_REQ.1-12>* In alignment to APE_REQ.1.6C/APE_REQ.1-10, APE_REQ.1.7C/APE_REQ.1-11 and APE_REQ.1.8C/APE_REQ.1-12 and corresponding to similar work units for ACE_REQ.1; refer as well to CEM2022-R1-0060, CEM2022-R1-0061, CEM2022-R1-0030, CEM2022-R1-0031 (for all refer to corrected / improved versions according to this document), CEM2022-R1-0032:

	12.8.1.3.15 Work unit ASE_REQ.1-14 […] CC Part 3 ASE_REQ.1.8C: *The security requirements rationale shall trace each SFR back to the threats countered by that SFR and the OSPs enforced by that SFR.* *The security requirements rationale shall demonstrate that the SFRs (in conjunction with the security objectives for the environment) counter all threats for the TOE.* **12.8.1.3.16 Work unit ASE_REQ.1-15** The evaluator ***shall check*** that the security requirements rationale traces each SFR back to the threats countered by that SFR and OSPs enforced by that SFR. The evaluator ***shall examine*** the security requirements rationale to determine that for each threat it demonstrates that the SFRs are suitable to meet that threat. The evaluator determines that each SFR is traced back to at least one threat or OSP for the TOE. Failure to trace implies that either the security requirements rationale is incomplete, the security objectives for the operational environment are incomplete, or the SFR has no useful purpose. There is no prescribed location where this tracing element of the rationale must be placed: for example, the relevant parts may be located under each threat and OSP in order to help make the security argument clearer and easier to read. If no SFRs trace back to a threat and the evaluator determines that also no security objectives for the operational environment trace back to that threat in ASE_OBJ.1-2, the evaluator action related to this work unit is assigned a fail verdict. The evaluator determines that the justification for a threat shows whether the threat is removed, diminished or mitigated. The evaluator determines that the justification for a threat demonstrates that the SFRs are sufficient: if all SFRs that trace back to the threat are achieved then, in the context of any applicable OSPs and assumptions, the threat is removed, sufficiently diminished, or the effects of the threat are sufficiently mitigated. Note that simply listing in the security requirements rationale the SFRs associated with each threat may be part of a justification, but does not constitute a justification by itself. A descriptive justification is required, although in simple cases this justification may be as minimal as “SFR X directly counters Threat Y”. The evaluator also determines that each SFR that traces back to a threat is necessary: when the SFR is implemented it actually contributes to the removal, diminishing or mitigation of that threat. CC Part 3 ASE_REQ.1.9C: *The security requirements rationale shall demonstrate that the SFRs (in conjunction with the security objectives for the environment) enforce all OSPs.*

	12.8.1.3.17 Work unit ASE_REQ.1-16 The evaluator ***shall examine*** the security requirements rationale to determine that for each OSP it justifies that the SFRs are suitable to enforce that OSP. If no SFRs trace back to the OSP and the evaluator determines that also no security objectives for the operational environment trace back to that OSP in ASE_OBJ.1-2, the evaluator action related to this work unit is assigned a fail verdict. The evaluator determines that the justification for an OSP demonstrates that the SFRs are sufficient: if all SFRs that trace back to that OSP are achieved then, in the context of any applicable assumptions, the OSP is enforced. The evaluator also determines that each SFR that traces back to an OSP is necessary: when the SFR is implemented it actually contributes to the enforcement of the OSP. Note that simply listing in the security requirements rationale the SFRs associated with each OSP may be part of a justification, but does not constitute a justification by itself. A descriptive justification is required, although in simple cases this justification may be as minimal as "SFR X directly enforces OSP Y". CC Part 3 ASE_REQ.1.10C: *The security requirements rationale shall explain why the SARs were chosen*.
Status	ma
Remarks	-

ID	CEM2022-R1-0060
Date	2023-12-22
Reference	12.8.1.3.16 / 2nd paragraph
Issue – Problem Description	If no SFRs trace back to a threat, the evaluator action related to this work unit is assigned a fail verdict as it implies that either the security requirements rationale is incomplete, the security objectives for the TOE are incomplete, or some SFRs have no useful purpose. Problem: In a direct rationale ST, there are no security objectives for the TOE. So, threats are countered by either security objectives for the operational environment and/or SFRs (Refer to ASE_OBJ.1-2). For this reason, the statement above is not true. Here, the evaluation sub-activity for ASE_REQ.1 only addresses the rationale between SFRs and threats and it is not sufficient to address all threats, therefore the work unit ASE_REQ.1-15 shall address the rationale in combination with ASE_OBJ.1-2.

Type	te
Resolution - Correction / Interpretation	If no SFRs trace back to a threat and the evaluator determines that also no security objectives for the operational environment trace back to that threat in ASE_OBJ.1-2, the evaluator action related to this work unit is assigned a fail verdict.
Status	ma
Remarks	-

ID	CEM2022-R1-0061
Date	2023-12-22
Reference	12.8.1.3.17 / 2nd paragraph
Issue – Problem Description	If no SFRs or security objectives for the operational environment trace back to the OSP, the evaluator action related to this work unit is assigned a fail verdict. Problem: Cf. CEM2022-R1-0060. In a direct rationale ST, there are no security objectives for the TOE. So, OSPs are enforced by either security objectives for the operational environment and/or SFRs (Refer to ASE_OBJ.1-2). For this reason, the statement above is true. But the evaluation sub-activity for ASE_REQ.1 only addresses the rationale between SFRs and OSPs. The rationale between security objectives for the operational environments and OSPs is addressed in ASE_OBJ.1. Therefore the work unit ASE_REQ.1-16 shall address the rationale in combination with ASE_OBJ.1-2.
Type	te
Resolution - Correction / Interpretation	If no SFRs trace back to the OSP and the evaluator determines that also no security objectives for the operational environment trace back to that OSP in ASE_OBJ.1-2, the evaluator action related to this work unit is assigned a fail verdict.
Status	ma
Remarks	-

ID	CEM2022-R1-0062
Date	2023-12-22
Reference	between 12.8.2.3.16 and 12.8.2.3.17
Issue – Problem	The errata CC2022-P3-R1-0016 from [CC:2022-3] shall be addressed here. ASE_REQ.2.8C requires to demonstrate the security requirements rationale

Description	in terms of security objectives for the TOE. But there is no explicit element to require to trace each SFR back to them. (cf. APE_REQ.2.6C and ACE_REQ.2.6C) When a new Content and presentation element is defined here, then related work unit shall be added too. (cf. APE_REQ.2-10 and APE_REQ.2-11)
Type	te
Resolution - Correction / Interpretation	*<Add new work unit referencing APE_ REQ.2-10, and APE_REQ.2-11>* In alignment to APE_REQ.2.6C/APE_REQ.2-10 and APE_REQ.2-11 and corresponding to similar work units for ACE_REQ.2; refer as well to CEM2022-R1-0029 and CEM2022-R1-0032: **12.8.2.3.16 Work unit ASE_REQ.2-15** […] CC Part 3 ASE_REQ.2.8C: *The security requirements rationale shall trace each SFR back to the security objectives for the TOE.* *The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.* **12.8.2.3.17 Work unit ASE_REQ.2-16** The evaluator ***shall check*** that the security requirements rationale traces each SFR back to the security objectives for the TOE. The evaluator ***shall examine*** the security requirements rationale to determine that for each security objective for the TOE it justifies that the SFRs are suitable to meet that security objective for the TOE. Optional requirements may require Threats/OSPs to be specified, and security objectives associated with these SPD elements are also covered by this work unit. The evaluator determines that each SFR is traced back to at least one security objective for the TOE. Failure to trace implies that either the security requirements rationale is incomplete, the security objectives for the TOE are incomplete, or the SFR has no useful purpose. If no SFRs trace back to the security objective for the TOE, the evaluator action related to this work unit is assigned a fail verdict. The evaluator determines that the justification for a security objective for the TOE demonstrates that the SFRs are sufficient: if all SFRs that trace back to the objective are satisfied, the security objective for the TOE is achieved. The evaluator also determines that each SFR that traces back to a security objective for the TOE is necessary: when the SFR is satisfied, it actually contributes to achieving the security objective. Note that the tracings from SFRs to security objectives for the TOE provided in the security requirements rationale may be a part of the

	justification, but do not constitute a justification by themselves. CC Part 3 ASE_REQ.2.9C: *The security requirements rationale shall explain why the SARs were chosen*.
Status	ma
Remarks	-

ID	CEM2022-R1-0063
Date	2023-12-22
Reference	12.10.2.3.2, 12.10.2.3.3, 12.10.1 / Table 1
Issue – Problem Description	12.10.2.3.2, last paragraph: The result of this work unit shall be integrated to the result of ASE_REQ.1.1E / ASE_REQ.1-16 (or the equivalent higher components if a higher assurance level is selected) and ASE_REQ.2.1E / ASE_REQ.2-13. 12.10.2.3.3, last paragraph: The result of this work unit shall be integrated to the result of ASE_REQ.1.1E / ASE_REQ.1-16 (or the equivalent higher components if a higher assurance level is selected) and ASE_REQ.2.1E / ASE_REQ.2-13. Problem: References to the related work units shall be updated according to the scope of ASE_COMP.1-1 and ASE_COMP.1-2. (Considering JIL COMP for CC V3.1 R5, they shall be associated with ASE_REQ.1-18 and ASE_REQ.2-18.)
Type	te
Resolution - Correction / Interpretation	12.10.2.3.2, last paragraph: The result of this work unit shall be integrated to the result of ASE_REQ.1.1E / ASE_REQ.1-18 (or the equivalent higher components if a higher assurance level is selected) and ASE_REQ.2.1E / ASE_REQ.2-18. 12.10.2.3.3, last paragraph: The result of this work unit shall be integrated to the result of ASE_REQ.1.1E / ASE_REQ.1-18 (or the equivalent higher components if a higher assurance level is selected) and ASE_REQ.2.1E / ASE_REQ.2-18. Table 1: The “Evaluation work unit” column of Table 1 – ASE_COMP shall be updated accordingly.
Status	ma
Remarks	-

ID	CEM2022-R1-0064
Date	2023-12-22
Reference	12.10.2.3.4 / last paragraph, 12.10.1 / Table 1
Issue – Problem Description	The result of this work unit shall be integrated to the result of ASE_REQ.2.1E / ASE_REQ.2-12. Problem: References to the related work units shall be updated according to the scope of ASE_COMP.1-3. (Considering JIL COMP for CC V3.1 R5, they shall be associated with ASE_REQ.2-17.)
Type	te
Resolution - Correction / Interpretation	12.10.2.3.4, last paragraph: The result of this work unit shall be integrated to the result of ASE_REQ.2.1E / ASE_REQ.2-17. Table 1: The "Evaluation work unit" column of Table 1 – ASE_COMP shall be updated accordingly.
Status	ma
Remarks	-

ID	CEM2022-R1-0065
Date	2023-12-22
Reference	12.10.2.3.5 / 1st paragraph ~ 3rd paragraph
Issue – Problem Description	The evaluator shall examine the statement of compatibility to determine that all performed operations on the relevant TOE security functional requirements of the base component are appropriate for the composite product Security Target. This work unit relates to Step 3 of the Application Notes above. The relevant TOE security functional requirements of the base component comprise at least the elements of the group RP_SFR-SERV (cf. the work unit ASE_COMP.1-1), but also the RP_SFR-MECH may be presented as relevant TOE security functional requirements. The non-relevant TOE security functional requirements belong to IP_SFR. In order to perform this work unit the evaluator compares single parameters of the relevant SFRs of the base component with those of the composite evaluation. For example, the evaluator compares the properties of the respective components FCS_COP.1/RSA and determines that the composite-ST requires a key length of 2048 bit and the base-ST enforces the RSA-function with a key length of 1024 and 2048 bit, i.e. this parameter

	of the base component is appropriate for the composite-ST. Note, that the composite product-SFRs need not necessarily be the same as the base component-SFRs, e.g. a trusted channel (FTP_ITC.1) in the composite product can be built using an RSA implementation (FCS_COP.1/RSA) of the base component. Problem: The work unit is intended to check the compatibility between base-ST and composite-ST, so the highlighted “base component” shall be replaced with “base component Security Target” or “base-ST”, and the highlighted “composite product” with “composite-ST”.
Type	ed/te
Resolution - Correction / Interpretation	The evaluator shall examine the statement of compatibility to determine that all performed operations on the relevant TOE security functional requirements of the base component Security Target are appropriate for the composite product Security Target. This work unit relates to Step 3 of the Application Notes above. The relevant TOE security functional requirements of the base-ST comprise at least the elements of the group RP_SFR-SERV (cf. the work unit ASE_COMP.1-1), but also the RP_SFR-MECH may be presented as relevant TOE security functional requirements. The non-relevant TOE security functional requirements belong to IP_SFR. In order to perform this work unit the evaluator compares single parameters of the relevant SFRs of the base-ST with those of the composite evaluation. For example, the evaluator compares the properties of the respective components FCS_COP.1/RSA and determines that the composite-ST requires a key length of 2048 bit and the base-ST enforces the RSA-function with a key length of 1024 and 2048 bit, i.e. this parameter of the base-ST is appropriate for the composite-ST. Note, that the composite product-SFRs need not necessarily be the same as the base component-SFRs, e.g. a trusted channel (FTP_ITC.1) in the composite-ST can be built using an RSA implementation (FCS_COP.1/RSA) of the base-ST.
Status	ma
Remarks	-

ID	CEM2022-R1-0066
Date	2023-12-22
Reference	12.10.2.3.5 / last paragraph, 12.10.1 / Table 1
Issue – Problem Description	The result of this work unit shall be integrated to the result of ASE_REQ.2.1E / ASE_REQ.2-4. Problem: References to the related work units shall be updated according to the scope of ASE_COMP.1-4. (Considering JIL COMP for CC V3.1 R5, they shall be associated with

	ASE_REQ.2-10.)
Type	te
Resolution - Correction / Interpretation	12.10.2.3.5 last paragraph: The result of this work unit shall be integrated to the result of ASE_REQ.2.1E / ASE_REQ.2-10. Table 1: The "Evaluation work unit" column of Table 1 – ASE_COMP shall be updated accordingly.
Status	ma
Remarks	-

ID	CEM2022-R1-0067
Date	2023-12-22
Reference	12.10.2.3.6 / 1st paragraph
Issue – Problem Description	The evaluator shall examine the statement of compatibility to determine that the relevant TOE security objectives of the base component are not contradictory to those of the composite product Security Target. Problem: The work unit is intended to check the compatibility between base-ST and composite-ST, so the highlighted "base component" shall be replaced with "base component Security Target" or "base-ST".
Type	ed/te
Resolution - Correction / Interpretation	The evaluator shall examine the statement of compatibility to determine that the relevant TOE security objectives of the base component Security Target are not contradictory to those of the composite product Security Target.
Status	ma
Remarks	-

ID	CEM2022-R1-0068
Date	2023-12-22
Reference	12.10.2.3.7 / 1st paragraph
Issue – Problem Description	The evaluator shall examine the statement of compatibility to determine that the significant security objectives for the operational environment of the base component are not contradictory to those of the composite product Security Target.

	Problem: The work unit is intended to check the compatibility between base-ST and composite-ST, so the highlighted “base component” shall be replaced with “base component Security Target” or “base-ST”.
Type	ed/te
Resolution - Correction / Interpretation	The evaluator shall examine the statement of compatibility to determine that the significant security objectives for the operational environment of the base component Security Target are not contradictory to those of the composite product Security Target.
Status	ma
Remarks	-

ID	CEM2022-R1-0069
Date	2023-12-22
Reference	13.5.2.4.2 / 3rd paragraph
Issue – Problem Description	If the evaluator has the possibility to actually execute or witness the "built" procedure used to transfer the implementation representation into the actual implementation, and to compare the result to the TOE as delivered, this may provide an easier and at the same time more reliable check for this work unit (and possibly also for the following one). Problem: The paragraph above has been added in ADV_IMP.2-1 in comparison to ADV_IMP.1-1. ADV_IMP.2-1 and ADV_IMP.1-1 are related to the Content and presentation element ADV_IMP.2.1C and ADV_IMP.1.1C respectively, and they are all the same. So, if the paragraph above is necessary for ADV_IMP.2-1, then it shall be necessary for ADV_IMP.1-1.
Type	te
Resolution - Correction / Interpretation	*<Synchronize two work units ADV_IMP.2-1 and ADV_IMP.1-1.>* In alignment of ADV_IMP.1-1 and ADV_IMP.2-1: **13.5.1.4.2 Work unit ADV_IMP.1-1** The evaluator ***shall check*** that the implementation representation defines the TSF to a level of detail such that the TSF can be generated without further design decisions. Source code or hardware diagrams and/or IC hardware design language code or layout data that are used to build the actual hardware are examples of parts of an implementation representation. The evaluator samples the implementation representation to gain confidence that it is at the appropriate level and not, for instance, a pseudo-code level which requires additional design decisions to be made. The evaluator is encouraged to perform a quick check when first looking at the implementation representation to

	assure themselves that the developer has supplied all the required information. However, the evaluator is also encouraged to perform the bulk of this check while working on other work units that call for examining the implementation; this will ensure the sample examined for this work unit is relevant. If the evaluator has the possibility to actually execute or witness the "built" procedure used to transfer the implementation representation into the actual implementation, and to compare the result to the TOE as delivered, this may provide an easier and at the same time more reliable check for this work unit (and possibly also for the following one). **13.5.1.4.2 Work unit ADV_IMP.2-1** The evaluator ***shall check*** that the implementation representation defines the TSF to a level of detail such that the TSF can be generated without further design decisions. Source code or hardware diagrams and/or IC hardware design language code or layout data that are used to build the actual hardware are examples of parts of an implementation representation. The evaluator samples the implementation representation to gain confidence that it is at the appropriate level and not, for instance, a pseudo-code level which requires additional design decisions to be made. The evaluator is encouraged to perform a quick check when first looking at the implementation representation to assure themselves that the developer has supplied all the required information. However, the evaluator is also encouraged to perform the bulk of this check while working on other work units that call for examining the implementation; this will ensure the sample examined for this work unit is relevant. If the evaluator has the possibility to actually execute or witness the "built" procedure used to transfer the implementation representation into the actual implementation, and to compare the result to the TOE as delivered, this may provide an easier and at the same time more reliable check for this work unit (and possibly also for the following one).
Status	ma
Remarks	-

ID	CEM2022-R1-0070
Date	2023-12-22
Reference	13.6.3.5.2 / 3rd paragraph
Issue – Problem Description	The evaluator examines a sample of the TSF to verify the accuracy of the internals description. For example, a sample of the procedural software portions of the TSF is analysed to determine its cohesion and coupling, its adherence to the coding standards, etc. As with all areas where the evaluator performs activities on a subset the evaluator provides a justification of the sample size and scope.

	Problem: ADV_INT.3-4 shall examine entire of the TSF considering ADV_INT.3.2C.
Type	te
Resolution - Correction / Interpretation	The evaluator examines the TSF to verify the accuracy of the internals description. For example, a sample of the procedural software portions of the TSF is analysed to determine its cohesion and coupling, its adherence to the coding standards, etc. As with all areas where the evaluator performs activities on a subset the evaluator provides a justification of the sample size and scope.
Status	ma
Remarks	-

ID	CEM2022-R1-0071
Date	2023-12-22
Reference	13.7.1.2 / 1st paragraph / i)
Issue – Problem Description	i) all the tools used for the formal model, the formal properties, proofs and demonstrations (CC Part 3 ADV_SPM.1.7D). Problem: There is no ADV_IMP.1.7D in CC Part 3.
Type	te
Resolution - Correction / Interpretation	The text entry in i) remains unchanged, and the missing ADV_IMP.1.7D element will be supplemented in CC Part 3 as it seems valuable for clarity to explictly address requirements on the provisioning of tools for formal models, formal properties, proofs and demonstrations. Refer to CC2022-P3-R1-0032.
Status	ma
Remarks	-

ID	CEM2022-R1-0072
Date	2023-12-22
Reference	13.8.1.2.2 / 3rd paragraph
Issue – Problem Description	The TOE (and TSF) may be described in multiple layers of abstraction (i.e. subsystems and modules). Depending upon the complexity of the TOE, its design may be described in terms of subsystems and modules, as described in CC Part 3, Annex A, ADV_TDS: Subsystems and Modules. At this level of assurance, the decomposition only need be at the "subsystem" level.

	Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	The TOE (and TSF) may be described in multiple layers of abstraction (i.e. subsystems and modules). Depending upon the complexity of the TOE, its design may be described in terms of subsystems and modules, as described in CC Part 3, Annex A.4, ADV_TDS: Subsystems and Modules. At this level of assurance, the decomposition only need be at the "subsystem" level.
Status	ma
Remarks	-

ID	CEM2022-R1-0073
Date	2023-12-22
Reference	13.8.2.2.3, 13.8.3.4.4, 13.8.4.4.5, 13.8.5.4.5
Issue – Problem Description	Problem: Evaluator action is missing from ADV_TDS.2-2, ADV_TDS.3-3, ADV_TDS.4-4, and ADV_TDS.5-4. ADV_TDS.1.2C, ADV_TDS.2.2C, ADV_TDS.3.3C, ADV_TDS.4.3C, and ADV_TDS.5.3C are the same Content and presentation elements. ADV_TDS.1-2 has an evaluator action related to multi-assurance case, so the same evaluator action shall be added to ADV_TDS.2-2, ADV_TDS.3-3, ADV_TDS.4-4, and ADV_TDS.5-4 too.
Type	te
Resolution - Correction / Interpretation	*<Add the following paragraph under the ADV_TDS.2-2,* ADV_TDS.3-3, ADV_TDS.4-4, and ADV_TDS.5-4.*>* If TSFs are defined in terms of sub-TSFs for multi assurance the evaluator shall examine that the combination of all sub-TSF is consistent and does not omit relevant information for each sub-TSF considering the relevant decomposition level.
Status	ma
Remarks	-

ID	CEM2022-R1-0074
Date	2023-12-22
Reference	13.8.5.4.13 / 2nd paragraph
Issue – Problem Description	The interfaces of a module are those interfaces used by other modules as a means to invoke the operations provided, and to provide inputs to or receive outputs from the module. The purpose in the specification of these interfaces is to permit the exercise of them during testing. Inter-module

	interfaces that are not SFR-related need not be specified or described, since they are not a factor in testing. Likewise, other internal interfaces that are not a factor in traversing SFR-related paths of execution (such as those internal paths that are fixed). Problem: The main difference between ADV_TDS.4.8C and ADV_TDS.5.7C is that for the latter one a "semiformal description of each module in terms of its purpose, interaction, interfaces, return values from those interfaces, and called interfaces to other modules" is required. The highlighted text in section 13.8.5.4.13, 2nd paragraph origins as a copy from the comparable ADV_TDS.4.8C / ADV_TDS.4-12 and seems at first sight to be inconsistent to the requirements in ADV_TDS.5.7C.
Type	te
Resolution - Correction / Interpretation	**13.8.5.4.13 Work unit ADV_TDS.5-12** […] The interfaces of a module are those interfaces used by other modules as a means to invoke the operations provided, and to provide inputs to or receive outputs from the module. The purpose in the specification of these interfaces is to permit the exercise of them during testing. The focus of this work unit lies on the modules and their SFR-related interfaces by using a semiformal description. Sufficiently detailed information about the modules and their interfaces should be provided so that the evaluator is able to determine that the SFRs are completely and accurately implemented and that the provided module information supports as preparatory work further evaluation activities in ADV_FSP, ADV_ARC, ADV_INT, ATE and AVA. Refer as well to the explanations for work unit ADV_TDS.5-11 in section 13.8.5.4.12. [SFR-related interfaces are all interfaces …]
Status	ma
Remarks	-

ID	CEM2022-R1-0075
Date	2023-12-22
Reference	13.8.5.4.13 / 5th paragraph
Issue – Problem Description	In terms of the assessment of parameters (inputs and outputs) to a module, any use of global data must also be considered. A module "uses" global data if it either reads or writes the data. In order to assure the description of such parameters (if used) is complete, the evaluator uses other information provided about the module in the TOE design (interfaces, algorithmic description, etc.), as well as the description of the particular set of global data assessed in work unit ADV_TDS.5-10. For instance, the evaluator can first determine the processing the module performs by examining its function and interfaces presented (particularly the parameters of the

	interfaces). They can then check to see if the processing appears to "touch" any of the global data areas identified in the TDS design. The evaluator then determines that, for each global data area that appears to be "touched", that global data area is listed as a means of input or output by the module the evaluator is examining. Problem: Referencing error. ADV_TDS.5-10 is intended to examine the mapping between subsystems and modules. Parameters are examined in ADV_TDS.5-12.
Type	ed/te
Resolution - Correction / Interpretation	In terms of the assessment of parameters (inputs and outputs) to a module, any use of global data must also be considered. A module "uses" global data if it either reads or writes the data. In order to assure the description of such parameters (if used) is complete, the evaluator uses other information provided about the module in the TOE design (interfaces, algorithmic description, etc.), as well as the description of the particular set of global data. For instance, the evaluator can first determine the processing the module performs by examining its function and interfaces presented (particularly the parameters of the interfaces). They can then check to see if the processing appears to "touch" any of the global data areas identified in the TDS design. The evaluator then determines that, for each global data area that appears to be "touched", that global data area is listed as a means of input or output by the module the evaluator is examining.
Status	ma
Remarks	-

ID	CEM2022-R1-0076
Date	2023-12-22
Reference	13.8.5.4.14
Issue – Problem Description	Problem: Right after the last paragraph of 13.8.5.4.14, there shall be subclause for Action ADV_TDS.5.2E.
Type	ed
Resolution - Correction / Interpretation	*<Insert the following>* **13.8.5.5 Action ADV_TDS.5.2E**
Status	ma
Remarks	-

ID	CEM2022-R1-0077
Date	2023-12-22
Reference	14.3.1.3.7
Issue – Problem Description	The evaluator ***shall examine*** the operational user guidance to determine that it describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST. The evaluator analyses the security objectives for the operational environment in the ST and determines that for each user role, the relevant security measures are described appropriately in the user guidance. The security measures described in the user guidance should include all relevant external procedural, physical, personnel and connectivity measures. Note that those measures relevant for secure installation of the TOE are examined in Preparative procedures (AGD_PRE). Problem: “security measures” or “measures” shall be replaced with “security controls” or “controls”.
Type	ed/te
Resolution - Correction / Interpretation	The evaluator ***shall examine*** the operational user guidance to determine that it describes, for each user role, the security controls to be followed in order to fulfil the security objectives for the operational environment as described in the ST. The evaluator analyses the security objectives for the operational environment in the ST and determines that for each user role, the relevant security controls are described appropriately in the user guidance. The security controls described in the user guidance should include all relevant external procedural, physical, personnel and connectivity controls. Note that those controls relevant for secure installation of the TOE are examined in Preparative procedures (AGD_PRE).
Status	ma
Remarks	-

ID	CEM2022-R1-0078
Date	2023-12-22
Reference	15.2.4.3.10, 15.2.5.3.16
Issue – Problem Description	15.2.4.3.10, 2nd paragraph, h): h) the description of the change management; 15.2.5.3.16, 2nd paragraph, h) h) the description of the change management;

	Problem: They shall be consistent with ALC_CMC.3-7, 2nd paragraph, bullet g).
Type	ed/te
Resolution - Correction / Interpretation	15.2.4.3.10, 2nd paragraph, h): h) the description of the change management, including the process of verifying that the proposed change is necessary and the consequence would be acceptable; 15.2.5.3.16, 2nd paragraph, h) h) the description of the change management, including the process of verifying that the proposed change is necessary and the consequence would be acceptable;
Status	ma
Remarks	-

ID	CEM2022-R1-0079
Date	2023-12-22
Reference	15.4.1.3.2 / 1st paragraph
Issue – Problem Description	The evaluator ***shall examine*** the delivery documentation to determine that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer. Problem: Check the term “consumer”. In 12.1 of CC Part 3, the term “downstream user” is used regarding ALC_DEL instead of “user” or “consumer”. (cf. errata CC2022-P3-R1-0025 of [CC:2022-3])
Type	ed/te
Resolution - Correction / Interpretation	The evaluator ***shall examine*** the delivery documentation to determine that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the downstream user. Refer as well to CC2022-P3-R1-0025.
Status	ma
Remarks	-

ID	CEM2022-R1-0080

Date	2023-12-22
Reference	15.5
Issue – Problem Description	**15.5 Development security (ALC_DVS)** Problem: Family name shall be consistent with [CC:2022-3]
Type	ed/te
Resolution - Correction / Interpretation	**15.5 Developer environment security (ALC_DVS)**
Status	ma
Remarks	-

ID	CEM2022-R1-0081
Date	2023-12-22
Reference	15.5
Issue – Problem Description	Problem: To reflect the family name, “development security” shall be replaced with “developer environment security” within 15.5. (cf. errata CC2022-P3-R1-0026 of [CC:2022-3]) In addition, to be consistent with Content and presentation element, “security measures” or “measures” shall be replaced with “security controls” or “controls” within 15.5.
Type	ed/te
Resolution - Correction / Interpretation	*<Replace “development security” with “developer environment security”.>* *<Replace “security measures” or “measures” with “security controls” or “controls”.>*
Status	ma
Remarks	-

ID	CEM2022-R1-0082
Date	2023-12-22
Reference	15.5.1.3.2, 15.5.2.3.2
Issue – Problem Description	15.5.1.3.2, 5th paragraph: The development security documentation should identify the locations at which development occurs, and describe the aspects of development performed, along with the security measures applied at each location and

	for transports between different locations. For example, development can occur at multiple facilities within a single building, multiple buildings at the same site, or at multiple sites. Transports of parts of the TOE or the unfinished TOE between different development sites are to be covered by Development security (ALC_DVS), whereas the transport of the finished TOE to the consumer is dealt with in Delivery (ALC_DEL). 15.5.2.3.2, 5th paragraph: The development security documentation should identify the locations at which development occurs, and describe the aspects of development performed, along with the security measures applied at each location and for transports between different locations. For example, development can occur at multiple facilities within a single building, multiple buildings at the same site, or at multiple sites. Transports of parts of the TOE or the unfinished TOE between different development sites are to be covered by the Development security (ALC_DVS), whereas the transport of the finished TOE to the consumer is dealt with in the Delivery (ALC_DEL). Problem: Check the term "consumer". In 12.1 of [CC:2022-3], the term "downstream user" is used regarding ALC_DEL instead of "user" or "consumer". (cf. errata CC2022-P3-R1-0025 of [CC:2022-3] and CEM2022-R1-0079 of [CEM:2022])
Type	ed/te
Resolution - Correction / Interpretation	15.5.1.3.2, 5th paragraph: The development security documentation should identify the locations at which development occurs, and describe the aspects of development performed, along with the security measures applied at each location and for transports between different locations. For example, development can occur at multiple facilities within a single building, multiple buildings at the same site, or at multiple sites. Transports of parts of the TOE or the unfinished TOE between different development sites are to be covered by Development security (ALC_DVS), whereas the transport of the finished TOE to the downstream user is dealt with in Delivery (ALC_DEL). 15.5.2.3.2, 5th paragraph: The development security documentation should identify the locations at which development occurs, and describe the aspects of development performed, along with the security measures applied at each location and for transports between different locations. For example, development can occur at multiple facilities within a single building, multiple buildings at the same site, or at multiple sites. Transports of parts of the TOE or the unfinished TOE between different development sites are to be covered by the Development security (ALC_DVS), whereas the transport of the finished TOE to the downstream user is dealt with in the Delivery (ALC_DEL).

	Refer as well to CC2022-P3-R1-0025.
Status	ma
Remarks	-

ID	CEM2022-R1-0083
Date	2023-12-22
Reference	15.7
Issue – Problem Description	**15.7 Life-cycle definition (ALC_LCD)** Problem: Family name shall be consistent with CC Part 3
Type	ed/te
Resolution - Correction / Interpretation	**15.7 Development Life-cycle definition (ALC_LCD)**
Status	ma
Remarks	-

ID	CEM2022-R1-0084
Date	2023-12-22
Reference	End of 15.7
Issue – Problem Description	Problem: There is no work unit for ALC_LCD.2.2E.
Type	te
Resolution - Correction / Interpretation	*<Add work units for ALC_LCD.2.2E at the end of the 15.7>* **15.7.2.4 Action ALC_LCD.2.2E** **15.7.2.4.1 Work unit ALC_LCD.2-4** The evaluator ***shall examine*** the measurements of the TOE development processes and security relevant properties of the TOE to determine that they support improvements in the development processes and/or the TOE itself. On base of – the life-cycle definition documentation that describes the model used to develop and maintain the TOE including the details of its arithmetic parameters and/or metrics used to measure the quality of the TOE and/or its development (refer to ALC_LCD.2.1C and

	ALC_LCD.2.2C), and – the life-cycle output documentation that provides the results of the measurements of the TOE development using the measurable life-cycle model (refer to ALC_LCD.2.3C) and in continuation of the work units ALC_LCD.2-2 and ALC_LCD.2-3 the evaluator analyses whether improvements in the development processes and/or the TOE itself in practice take place. This work unit requires the evaluator to determine if the documented procedures for quality improvement of the development processes and/or the TOE itself as defined for the TOE's measurable life-cycle model are being followed and the intended improvement (if applicable) is achieved. If the evaluation is conducted in parallel with the development of the TOE it may be possible that quality measurements have not been used in the past. In this case the evaluator should refer to work unit ALC_LCD.2-3 and use the documentation of the planned procedures in order to gain confidence that improvement actions are defined and being continuously followed.
Status	ma
Remarks	-

ID	CEM2022-R1-0085
Date	2023-12-22
Reference	15.8.2.5.2, 15.8.2.8.1, 15.8.2.9.1
Issue – Problem Description	15.8.2.5.2, 1st paragraph: The evaluator shall check the timestamp of the list of TOE implementation representation identifiers as output from the developer action of CC Part 3 ALC_TDA.1.2D that it is consistent with the creation time of the TOE as referenced in the ST. 15.8.2.8.1, 2nd paragraph: It is necessary that the evaluator follows the developer documentation to find a list of identifiers using the TOE as its input and the evaluator checks that this list of identifiers matches the list of TOE implementation representation identifiers as output from the developer action of CC Part 3 ALC_TDA.1.1D. 15.8.2.9.1, 1st paragraph: The evaluator shall check that the TOE implementation representation identifiers in the correspondence as determined in Work unit ALC_TDA.1-1 are capable to identify the element names of implementation representation (as parts of the configuration list) under the configuration scope of ALC_CMS.3. Problem:

	Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	15.8.2.5.2, 1st paragraph: The evaluator shall check the timestamp of the list of TOE implementation representation identifiers as output from the developer action of CC Part 3 ALC_TDA.2.2D that it is consistent with the creation time of the TOE as referenced in the ST. 15.8.2.8.1, 2nd paragraph: It is necessary that the evaluator follows the developer documentation to find a list of identifiers using the TOE as its input and the evaluator checks that this list of identifiers matches the list of TOE implementation representation identifiers as output from the developer action of CC Part 3 ALC_TDA.2.1D. 15.8.2.9.1, 1st paragraph: The evaluator shall check that the TOE implementation representation identifiers in the correspondence as determined in Work unit ALC_TDA.2-1 are capable to identify the element names of implementation representation (as parts of the configuration list) under the configuration scope of ALC_CMS.3.
Status	ma
Remarks	-

ID	CEM2022-R1-0086
Date	2023-12-22
Reference	before 15.8.2.7.1, CC Part 3 ALC_TDA.2.5C
Issue – Problem Description	Problem: Currently, ALC_TDA.2.5C is under ALC_TDA.2.5E but it is related to ALC_TDA.2.7E, so it shall be moved under ALC_TDA.2.7E.
Type	ed/te
Resolution - Correction / Interpretation	*<Move ALC_TDA.2.5C under ALC_TDA.2.7E>* **15.8.2.9.1 General** CC Part 3 ALC_TDA.2.5C: *The list of identifiers of the elements of implementation representation under the configuration scope of ALC_CMS.3 shall match with the list of unique TOE implementation representation identifiers as recorded during the TOE generation time.* Subsequent section numbers have to be shifted accordingly:

	15.8.2.7.2 → 15.8.2.7.1 15.8.2.9.1 → 15.8.2.9.2
Status	ma
Remarks	-

ID	CEM2022-R1-0087
Date	2023-12-22
Reference	before “CC Part 3 ALC_TDA.3.2C”
Issue – Problem Description	Problem: Subclause title “15.8.3.4 Action ALC_TDA.3.2E” is missing.
Type	ed
Resolution - Correction / Interpretation	*<Add following Subclause title>* Incorporate after EXAMPLE text in section 15.8.3.3.2: **15.8.3.4 Action ALC_TDA.3.2E** **15.8.3.4.1 General** CC Part 3 ALC_TDA.3.2C: The TOE implementation representation element names shall be in the same form as used or referenced by the development tool to generate the TOE. **15.8.3.4.2 Work unit ALC_TDA.3-2** The evaluator ***shall examine*** the user manual of the developer's development tool used to generate the TOE to determine that the development tool accepts the TOE implementation representation element names as its input parameters. EXAMPLE If the TOE implementation representation elements are data files residing in a repository such as a hard drive or in the cloud, then the evaluator only need to discover from the development tool user manual that the development tool accepts local or remote file names as its input parameters. Refer as well to CEM2022-R1-0088 (including re-numbering of subsequent section numbers).
Status	ma
Remarks	-

ID	CEM2022-R1-0088

Date	2023-12-22
Reference	before “CC Part 3 ALC_TDA.3.3C”
Issue – Problem Description	Problem: Subclause title “15.8.3.5 Action ALC_TDA.3.3E” is missing.
Type	ed
Resolution - Correction / Interpretation	*<Add following Subclause title>* Incorporate after EXAMPLE text in new section 15.8.3.4.2 according to CEM2022-R1-0087: **15.8.3.5 Action ALC_TDA.3.3E** **15.8.3.5.1 General** CC Part 3 ALC_TDA.3.3C: The timestamp of the list of unique TOE implementation representation identifiers as recorded during the TOE generation time shall be consistent with the creation time of the TOE. **15.8.3.5.2 Work unit ALC_TDA.3-3** The evaluator ***shall check*** the timestamp of the list of TOE implementation representation identifiers as output from the developer action of CC Part 3 ALC_TDA.1.2D that it is consistent with the creation time of the TOE as referenced in the ST. Consistency is confirmed by determining that the timestamp on the list of TOE implementation representation identifiers is earlier than the TOE creation time as referenced in the ST, and consistent with the time interval expected from the developer’s build process (e.g. as described in deliverables for ALC_LCD). Refer as well to CEM2022-R1-0087. Furthermore, corresponding re-numbering of subsequent section numbers: Replace section number 15.8.3.4 by 15.8.3.6. Replace section number 15.8.3.4.* by 15.8.3.6.*. Replace section number 15.8.3.5 by 15.8.3.7. Replace section number 15.8.3.5.* by 15.8.3.7.*. Replace section number 15.8.3.6 by 15.8.3.8. Replace section number 15.8.3.6.* by 15.8.3.8.*. Replace section number 15.8.3.7 by 15.8.3.9. Replace section number 15.8.3.7.* by 15.8.3.9.*. Replace section number 15.8.3.8 by 15.8.3.10. Replace section number 15.8.3.8.* by 15.8.3.10.*.
Status	ma
Remarks	-

ID	CEM2022-R1-0089
Date	2023-12-22
Reference	15.8.3.3.4, 15.8.3.6.2, 15.8.3.7.1
Issue – Problem Description	15.8.3.3.4, 1st paragraph: The evaluator shall check the timestamp of the list of TOE implementation representation identifiers as output from the developer action of CC Part 3 ALC_TDA.1.2D that it is consistent with the creation time of the TOE as referenced in the ST. 15.8.3.6.2, 2nd paragraph: It is necessary that the evaluator follows the developer documentation to find a list of identifiers using the TOE as its input and the evaluator checks that this list of identifiers matches the list of TOE implementation representation identifiers as output from the developer action of CC Part 3 ALC_TDA.1.1D. 15.8.3.7.1, 1st paragraph: The evaluator shall check that the TOE implementation representation identifiers in the correspondence as determined in Work unit ALC_TDA.1-1 are capable to identify the element names of implementation representation (as parts of the configuration list) under the configuration scope of ALC_CMS.3. Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	15.8.3.3.4, 1st paragraph: The evaluator shall check the timestamp of the list of TOE implementation representation identifiers as output from the developer action of CC Part 3 ALC_TDA.3.2D that it is consistent with the creation time of the TOE as referenced in the ST. 15.8.3.6.2, 2nd paragraph: It is necessary that the evaluator follows the developer documentation to find a list of identifiers using the TOE as its input and the evaluator checks that this list of identifiers matches the list of TOE implementation representation identifiers as output from the developer action of CC Part 3 ALC_TDA.3.1D. 15.8.3.7.1, 1st paragraph: The evaluator shall check that the TOE implementation representation identifiers in the correspondence as determined in Work unit ALC_TDA.3-1 are capable to identify the element names of implementation representation (as parts of the configuration list) under the configuration scope of ALC_CMS.3.

Status	ma
Remarks	-

ID	CEM2022-R1-0090
Date	2023-12-22
Reference	before 15.8.3.5.1, CC Part 3 ALC_TDA.3.5C
Issue – Problem Description	Problem: Currently, ALC_TDA.3.5C is under ALC_TDA.3.5E but it is related to ALC_TDA.3.7E, so it shall be moved under ALC_TDA.3.7E.
Type	ed/te
Resolution - Correction / Interpretation	*<Move ALC_TDA.3.5C under ALC_TDA.3.7E>* **15.8.3.7 Action ALC_TDA.3.5E** **15.8.3.7.1 Work unit ALC_TDA.3-5** The evaluator ***shall check*** the integrity of the list of unique TOE implementation representation identifiers as recorded during the TOE generation time and its associated timestamp and (author) origination information by examining the developer documentation describing the maintenance of this integrity characteristic. […] **15.8.3.9 Action ALC_TDA.3.7E** **15.8.3.9.1 General** CC Part 3 ALC_TDA.3.5C: *The list of identifiers of the elements of implementation representation under the configuration scope of ALC_CMS.3 shall match with the list of unique TOE implementation representation identifiers as recorded during the TOE generation time.* **15.8.3.9.2 Work unit ALC_TDA.3-7** The evaluator ***shall check*** that the TOE implementation representation identifiers in the correspondence as determined in Work unit ALC_TDA.1-1 are capable to identify the element names of implementation representation (as parts of the configuration list) under the configuration scope of ALC_CMS.3.
Status	ma
Remarks	-

ID	CEM2022-R1-0091
Date	2023-12-22

Reference	before 15.8.3.6.1, CC Part 3 ALC_TDA.3.6C
Issue – Problem Description	Problem: Currently, ALC_TDA.3.6C is under ALC_TDA.3.6E but it is related to ALC_TDA.3.8E, so it shall be moved under ALC_TDA.3.8E.
Type	ed/te
Resolution - Correction / Interpretation	*<Move ALC_TDA.3.6C under ALC_TDA.3.8E>* **5.8.3.8 Action ALC_TDA.3.6E** **15.8.3.8.1 Work unit ALC_TDA.3-6** The evaluator ***shall examine*** the developer documentation describing the developer's mechanism to trace from the TOE to the list of unique TOE implementation representation identifiers as recorded during the TOE generation time to confirm the developer's ability to trace from the TOE to the list of unique TOE implementation representation identifiers. […] **15.8.3.10 Action ALC_TDA.3.8E** **15.8.3.10.1 General** CC Part 3 ALC_TDA.3.6C: *The developer's explanation of the functional differences, if any, between the regenerated TOE copy and the original TOE shall take into account all visible differences, if any, between the regenerated TOE copy and the original TOE.* **15.8.3.10.2 Work unit ALC_TDA.3-8** The evaluator ***shall check*** that the developer's explanation of the functional differences, if any, between the regenerated TOE copy and the original TOE takes into account all visible differences, if any, between the regenerated TOE copy and the original TOE. […]
Status	ma
Remarks	-

ID	CEM2022-R1-0092
Date	2023-12-22
Reference	16.3.2.3.3, 16.3.2.3.4, 16.3.3.3.3, 16.3.3.3.4, 16.3.3.3.6
Issue – Problem Description	16.3.2.3.3, 2nd paragraph: Guidance on this work unit can be found in: • 15.2.1, Understanding the expected behaviour of the TOE; • 15.2.2, Testing vs. alternate approaches to verify the expected behaviour of functionality.

	16.3.2.3.4, 2nd paragraph: Guidance on this work units, as it pertains to the functional specification, can be found in: • 15.2.3, Verifying the adequacy of tests. 16.3.3.3.3, 2nd paragraph: Guidance on this work unit can be found in: • 15.2.1, Understanding the expected behaviour of the TOE; • 15.2.2, Testing vs. alternate approaches to verify the expected behaviour of functionality. 16.3.3.3.4, 2nd paragraph: Guidance on this work units, as it pertains to the functional specification, can be found in: • 15.2.3 Verifying the adequacy of tests. 16.3.3.3.6, 7th paragraph: Similar considerations as for parameters hold for error messages specified in the functional specification: Each error message, which belongs to a qualitatively distinct error case, needs to be covered by testing. Note, that there may be exceptions, for example error messages for errors, which cannot be provoked during testing. For such error messages other ways of coverage need to be found as discussed in 15.2.2, "Testing vs. alternate approaches to verify the expected behaviour of functionality". Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	16.3.2.3.3, 2nd paragraph: Guidance on this work unit can be found in: • 16.2.1, Understanding the expected behaviour of the TOE; • 16.2.2, Testing vs. alternate approaches to verify the expected behaviour of functionality. 16.3.2.3.4, 2nd paragraph: Guidance on this work units, as it pertains to the functional specification, can be found in: • 16.2.3, Verifying the adequacy of tests. 16.3.3.3.3, 2nd paragraph: Guidance on this work unit can be found in: • 16.2.1, Understanding the expected behaviour of the TOE; • 16.2.2, Testing vs. alternate approaches to verify the expected behaviour of functionality.

	16.3.3.3.4, 2nd paragraph: Guidance on this work units, as it pertains to the functional specification, can be found in: • 16.2.3 Verifying the adequacy of tests. 16.3.3.3.6, 7th paragraph: Similar considerations as for parameters hold for error messages specified in the functional specification: Each error message, which belongs to a qualitatively distinct error case, needs to be covered by testing. Note, that there may be exceptions, for example error messages for errors, which cannot be provoked during testing. For such error messages other ways of coverage need to be found as discussed in 16.2.2, "Testing vs. alternate approaches to verify the expected behaviour of functionality".
Status	ma
Remarks	-

ID	CEM2022-R1-0093
Date	2023-12-22
Reference	16.4.1.3.3, 16.4.1.3.4, 16.4.2.3.3, 16.4.2.3.4, 16.4.2.3.6, 16.4.3.3.3, 16.4.3.3.4, 16.4.3.3.6
Issue – Problem Description	16.4.1.3.3, 2nd paragraph: Guidance on this work unit can be found in: • 15.2.1, Understanding the expected behaviour of the TOE; • 15.2.2, Testing vs. alternate approaches to verify the expected behaviour of functionality. 16.4.1.3.4, 3rd paragraph: Guidance on this work unit can be found in: • 15.2.1, Understanding the expected behaviour of the TOE; • 15.2.2, Testing vs. alternate approaches to verify the expected behaviour of functionality. 16.4.2.3.3, 2nd paragraph: Guidance on this work unit can be found in: • 15.2.1, Understanding the expected behaviour of the TOE; • 15.2.2, Testing vs. alternate approaches to verify the expected behaviour of functionality. 16.4.2.3.4, 3rd paragraph:

	Guidance on this work unit can be found in: • 15.2.1, Understanding the expected behaviour of the TOE; • 15.2.2, Testing vs. alternate approaches to verify the expected behaviour of functionality. 16.4.2.3.6, 3rd paragraph: Guidance on this work unit can be found in: • 15.2.1, Understanding the expected behaviour of the TOE; • 15.2.2, Testing vs. alternate approaches to verify the expected behaviour of functionality. 16.4.3.3.3, 2nd paragraph: Guidance on this work unit can be found in: • 15.2.1, Understanding the expected behaviour of the TOE; • 15.2.2, Testing vs. alternate approaches to verify the expected behaviour of functionality. 16.4.3.3.4, 2nd paragraph: Guidance on this work unit can be found in: • 15.2.1, Understanding the expected behaviour of the TOE; • 15.2.2, Testing vs. alternate approaches to verify the expected behaviour of functionality. 16.4.3.3.6, 2nd paragraph: Guidance on this work unit can be found in: • 15.2.1, Understanding the expected behaviour of the TOE; • 15.2.2, Testing vs. alternate approaches to verify the expected behaviour of functionality. Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	16.4.1.3.3, 2nd paragraph: Guidance on this work unit can be found in: • 16.2.1, Understanding the expected behaviour of the TOE; • 16.2.2, Testing vs. alternate approaches to verify the expected behaviour of functionality. 16.4.1.3.4, 3rd paragraph: Guidance on this work unit can be found in: • 16.2.1, Understanding the expected behaviour of the TOE; • 16.2.2, Testing vs. alternate approaches to verify the expected behaviour of functionality.

	16.4.2.3.3, 2nd paragraph: Guidance on this work unit can be found in: • 16.2.1, Understanding the expected behaviour of the TOE; • 16.2.2, Testing vs. alternate approaches to verify the expected behaviour of functionality. 16.4.2.3.4, 3rd paragraph: Guidance on this work unit can be found in: • 16.2.1, Understanding the expected behaviour of the TOE; • 16.2.2, Testing vs. alternate approaches to verify the expected behaviour of functionality. 16.4.2.3.6, 3rd paragraph: Guidance on this work unit can be found in: • 16.2.1, Understanding the expected behaviour of the TOE; • 16.2.2, Testing vs. alternate approaches to verify the expected behaviour of functionality. 16.4.3.3.3, 2nd paragraph: Guidance on this work unit can be found in: • 16.2.1, Understanding the expected behaviour of the TOE; • 16.2.2, Testing vs. alternate approaches to verify the expected behaviour of functionality. 16.4.3.3.4, 2nd paragraph: Guidance on this work unit can be found in: • 16.2.1, Understanding the expected behaviour of the TOE; • 16.2.2, Testing vs. alternate approaches to verify the expected behaviour of functionality. 16.4.3.3.6, 2nd paragraph: Guidance on this work unit can be found in: • 16.2.1, Understanding the expected behaviour of the TOE; • 16.2.2, Testing vs. alternate approaches to verify the expected behaviour of functionality.
Status	ma
Remarks	-

ID	CEM2022-R1-0094

Date	2023-12-22
Reference	17.2.1.6.6 / 3rd paragraph
Issue – Problem Description	The guidance in B.2 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 Enhanced-Basic. Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	The guidance in B.6 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 Enhanced-Basic.
Status	ma
Remarks	-

ID	CEM2022-R1-0095
Date	2023-12-22
Reference	17.2.2.4, 17.2.3.4, 17.2.4.4, 17.2.5.4, 17.2.2.5, 17.2.3.5, 17.2.4.5, 17.2.5.5
Issue – Problem Description	CC Part 3 AVA_VAN.2.2C, CC Part 3 AVA_VAN.3.2C, CC Part 3 AVA_VAN.4.2C, CC Part 3 AVA_VAN.5.2C CC Part 3 AVA_VAN.2.2E, CC Part 3 AVA_VAN.3.2E, CC Part 3 AVA_VAN.4.2E, CC Part 3 AVA_VAN.5.2E Problem: Though for AVA_VAN.* a new Content and presentation element AVA_VAN.*.2C concerning third party components and IT products in the TOE environment including an adapted Evaluator action element AVA_VAN.*.2E has been introduced in AVA_VAN.* of [CC:2022-3], corresponding work units that address those new / adapted elements are missing.
Type	te
Resolution - Correction / Interpretation	*<Supplement work units AVA_VAN.*-1 related to AVA_VAN.*.1E and AVA_VAN.*-3 related to AVA_VAN.*.2E>* 17.2.2.4.2 Work unit AVA_VAN.2-1 / 17.2.3.4.2 Work unit AVA_VAN.3-1 / 17.2.4.4.2 Work unit AVA_VAN.4-1 / 17.2.5.4.2 Work unit AVA_VAN.5-1:

	The evaluator ***shall examine*** the TOE and the related list of third party components provided by the developer to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST and considers hereby the identified third party components that are part of the TOE or otherwise part of the TOE delivery. […] In particular, the evaluator should examine that the list of third party components provided by the developer includes information about the TOE related third party components and that those are part of the TOE or otherwise part of the TOE delivery. The evaluator should take care of that the ST and the TOE test configuration including its intended test environment fit to that list of third party components. 17.2.2.5.1 Work unit AVA_VAN.2-3 / 17.2.3.5.1 Work unit AVA_VAN.3-3 / 17.2.4.5.1 Work unit AVA_VAN.4-3 / 17.2.5.5.1 Work unit AVA_VAN.5-3: The evaluator ***shall examine*** sources of information publicly available to identify potential vulnerabilities in the TOE under consideration of the components identified in the list of third party components, and specific IT products in the environment that the TOE depends on. The evaluator examines the sources of information publicly available to support the identification of possible potential vulnerabilities in the TOE. This examination includes consideration of the components in the list of third party components, and specific IT products in the environment that the TOE depends on as all those might have an impact on the TOE's security functionality and secure operation. There are many sources of publicly available information which the evaluator should consider using items such as those available on the world wide web, including: […] The search of the information publicly available should be focused on those sources that refer specifically to the product from which the TOE is derived. The extensiveness of this search should consider the following factors: TOE type, evaluator experience in this TOE type, third party components and specific IT products in the environment that the TOE depends on, expected attack potential and the level of ADV evidence available. […]
Status	op
Remarks	For future revisions of the CC / CEM, one could think about a split-up of the updated work unit AVA_VAN.*-1 (see above) into two work units to address AVA_VAN.*.1C and AVA_VAN.*.2C separately. For the current proposal as outlined above the intent was to avoid re-numbering of subsequent work units.

ID	CEM2022-R1-0096

Date	2023-12-22
Reference	17.2.2.7.1 / 3rd paragraph, 6th paragraph
Issue – Problem Description	- 3rd paragraph: The evaluator is reminded that, as for considering the security architecture description in the search for vulnerabilities (as detailed in AVA_VAN.2-4), testing should be performed to confirm the architectural properties. This is likely to require negative tests attempting to disprove the properties of the security architecture. In developing the strategy for penetration testing, the evaluator will ensure that each of the major characteristics of the security architecture description are tested, either in functional testing (as considered in Clause 14) or evaluator penetration testing. - 6th paragraph: Guidance on determining the necessary attack potential to exploit a potential vulnerability can be found in B.2. Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	- 3rd paragraph: The evaluator is reminded that, as for considering the security architecture description in the search for vulnerabilities (as detailed in AVA_VAN.2-4), testing should be performed to confirm the architectural properties. This is likely to require negative tests attempting to disprove the properties of the security architecture. In developing the strategy for penetration testing, the evaluator will ensure that each of the major characteristics of the security architecture description are tested, either in functional testing (as considered in Clause 16) or evaluator penetration testing. - 6th paragraph: Guidance on determining the necessary attack potential to exploit a potential vulnerability can be found in B.6.
Status	ma
Remarks	-

ID	CEM2022-R1-0097
Date	2023-12-22
Reference	17.2.2.7.6, 17.2.2.7.7
Issue – Problem Description	17.2.2.7.6, 3rd paragraph: The guidance in B.2 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 Enhanced-Basic. 17.2.2.7.7, 1st paragraph, e) e) the amount of time, level of expertise, level of knowledge of the TOE, level of opportunity and the equipment required to perform the identified vulnerabilities, and the corresponding values using Tables B.2 and B.3 of B.2. Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	17.2.2.7.6, 3rd paragraph: The guidance in B.6 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 Enhanced-Basic. 17.2.2.7.7, 1st paragraph, e) e) the amount of time, level of expertise, level of knowledge of the TOE, level of opportunity and the equipment required to perform the identified vulnerabilities, and the corresponding values using Tables B.2 and B.3 of B.6.
Status	ma
Remarks	-

ID	CEM2022-R1-0098
Date	2023-12-22
Reference	17.2.3.3 / 2nd paragraph
Issue – Problem Description	The focused approach to the identification of potential vulnerabilities is an analysis of the evidence with the aim of identifying any potential vulnerabilities evident through the contained information. It is an unstructured analysis, as the approach is not predetermined. Further guidance on focused vulnerability analysis can be found in B.1.4.2.2. Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	The focused approach to the identification of potential vulnerabilities is an analysis of the evidence with the aim of identifying any potential vulnerabilities evident through the contained information. It is an unstructured analysis, as the approach is not predetermined. Further

	guidance on focused vulnerability analysis can be found in B.4.2.3.
Status	ma
Remarks	-

ID	CEM2022-R1-0099
Date	2023-12-22
Reference	17.2.3.7.1 / 3rd paragraph, 6th paragraph
Issue – Problem Description	- 3rd paragraph: The evaluator is reminded that, as for considering the security architecture description in the search for vulnerabilities (as detailed in AVA_VAN.3-4), testing should be performed to confirm the architectural properties. If requirements from ATE_DPT are included in the SARs, the developer testing evidence will include testing performed to confirm the correct implementation of any specific mechanisms detailed in the security architecture description. However, the developer testing will not necessarily include testing of all aspects of the architectural properties that protect the TSF, as much of this testing will be negative testing in nature, attempting to disprove the properties. In developing the strategy for penetration testing, the evaluator will ensure that all aspects of the security architecture description are tested, either in functional testing (as considered in Clause 14) or evaluator penetration testing. - 6th paragraph: Guidance on determining the necessary attack potential to exploit a potential vulnerability can be found in B.2. Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	- 3rd paragraph: The evaluator is reminded that, as for considering the security architecture description in the search for vulnerabilities (as detailed in AVA_VAN.3-4), testing should be performed to confirm the architectural properties. If requirements from ATE_DPT are included in the SARs, the developer testing evidence will include testing performed to confirm the correct implementation of any specific mechanisms detailed in the security architecture description. However, the developer testing will not necessarily include testing of all aspects of the architectural properties that protect the TSF, as much of this testing will be negative testing in nature, attempting to disprove the properties. In developing the strategy for penetration testing, the evaluator will ensure that all aspects of the security architecture description are tested, either in functional testing (as considered in Clause 16) or evaluator penetration testing. - 6th paragraph: Guidance on determining the necessary attack potential to exploit a

	potential vulnerability can be found in B.6.
Status	ma
Remarks	-

ID	CEM2022-R1-0100
Date	2023-12-22
Reference	17.2.3.7.6 / 3rd paragraph
Issue – Problem Description	The guidance in B.2 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 Enhanced-Basic. Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	The guidance in B.6 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 Enhanced-Basic.
Status	ma
Remarks	-

ID	CEM2022-R1-0101
Date	2023-12-22
Reference	17.2.3.7.7 / last paragraph
Issue – Problem Description	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities, detailing for each: a) its source (e.g. evaluation methodology activity being undertaken when it was conceived, known to the evaluator, read in a publication); b) the SFR(s) not met; c) a description; d) whether it is exploitable in its operational environment or not (i.e. exploitable or residual). the amount of time, level of expertise, level of knowledge of the TOE, level of opportunity and the equipment required to perform the identified

	vulnerabilities, and the corresponding values using Tables B.2 and B.3 of B.2. Problem: The last paragraph shall be a bullet e) of the previous paragraph. And referencing error.
Type	ed/te
Resolution - Correction / Interpretation	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities, detailing for each: a) its source (e.g. evaluation methodology activity being undertaken when it was conceived, known to the evaluator, read in a publication); b) the SFR(s) not met; c) a description; d) whether it is exploitable in its operational environment or not (i.e. exploitable or residual). e) the amount of time, level of expertise, level of knowledge of the TOE, level of opportunity and the equipment required to perform the identified vulnerabilities, and the corresponding values using Tables B.2 and B.3 of B.6.
Status	ma
Remarks	-

ID	CEM2022-R1-0102
Date	2023-12-22
Reference	17.2.4.6.1 / 2nd paragraph
Issue – Problem Description	Guidance on methodical vulnerability analysis is provided in B.1.4.2.3. Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	Guidance on methodical vulnerability analysis is provided in B.4.2.4.
Status	ma
Remarks	-

ID	CEM2022-R1-0103
Date	2023-12-22
Reference	17.2.4.7.1 / 6th paragraph

Issue – Problem Description	Guidance on determining the necessary attack potential to exploit a potential vulnerability can be found in B.2. Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	Guidance on determining the necessary attack potential to exploit a potential vulnerability can be found in B.6.
Status	ma
Remarks	-

ID	CEM2022-R1-0104
Date	2023-12-22
Reference	17.2.4.7.6 / 3rd paragraph
Issue – Problem Description	The guidance in B.2 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 Enhanced-Basic. Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	The guidance in B.6 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 Enhanced-Basic.
Status	ma
Remarks	-

ID	CEM2022-R1-0105
Date	2023-12-22
Reference	17.2.4.7.7 / last paragraph
Issue – Problem	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities, detailing for each:

Description	a) its source (e.g. evaluation methodology activity being undertaken when it was conceived, known to the evaluator, read in a publication); b) the SFR(s) not met; c) a description; d) whether it is exploitable in its operational environment or not (i.e. exploitable or residual). the amount of time, level of expertise, level of knowledge of the TOE, level of opportunity and the equipment required to perform the identified vulnerabilities, and the corresponding values using Tables B.2 and B.3 of B.2. Problem: The last paragraph shall be a bullet e) of the previous paragraph. And referencing error.
Type	ed/te
Resolution - Correction / Interpretation	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities, detailing for each: a) its source (e.g. evaluation methodology activity being undertaken when it was conceived, known to the evaluator, read in a publication); b) the SFR(s) not met; c) a description; d) whether it is exploitable in its operational environment or not (i.e. exploitable or residual). e) the amount of time, level of expertise, level of knowledge of the TOE, level of opportunity and the equipment required to perform the identified vulnerabilities, and the corresponding values using Tables B.2 and B.3 of B.6.
Status	ma
Remarks	-

ID	CEM2022-R1-0106
Date	2023-12-22
Reference	17.2.5.3 / 1st paragraph
Issue – Problem Description	The methodical analysis approach takes the form of a structured examination of the evidence. This method requires the evaluator to specify the structure and form the analysis will take (i.e. the manner in which the analysis is performed is predetermined, unlike the focused analysis). The method is specified in terms of the information that will be considered and how/why it will be considered. Further guidance on methodical vulnerability analysis can be found in B.2.2.2.3. Problem: Referencing error.

Type	ed/te
Resolution - Correction / Interpretation	The methodical analysis approach takes the form of a structured examination of the evidence. This method requires the evaluator to specify the structure and form the analysis will take (i.e. the manner in which the analysis is performed is predetermined, unlike the focused analysis). The method is specified in terms of the information that will be considered and how/why it will be considered. Further guidance on methodical vulnerability analysis can be found in B.4.2.4.
Status	ma
Remarks	-

ID	CEM2022-R1-0107
Date	2023-12-22
Reference	17.2.5.6.1 / 2nd paragraph
Issue – Problem Description	Guidance on methodical vulnerability analysis is provided in B.2.2.2.3. Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	Guidance on methodical vulnerability analysis is provided in B.4.2.4.
Status	ma
Remarks	-

ID	CEM2022-R1-0108
Date	2023-12-22
Reference	17.2.5.6.1 / last two paragraphs
Issue – Problem Description	Items b) to f) are explained in greater detail in B.2.1.-consideration if the evaluator determines that the potential vulnerability is not applicable in the operational environment. Otherwise, the evaluator records the potential vulnerability for further consideration. A list of potential vulnerabilities applicable to the TOE in its operational environment, which can be used as an input into penetration testing activities, shall be reported in the ETR by the evaluators. Problem: As mentioned in section 17.2.5, 1st paragraph, AVA_VAN.5 work units are copied from those of AVA_VAN.4. The last two paragraphs of section 17.2.5.6.1 cited above are copied incorrectly from AVA_VAN.4-4

	in section 17.2.4.6.1 to AVA_VAN.5-4 in section 17.2.5.6.1. Furthermore, AVA_VAN.5-5 is missing, i.e. a copy from AVA_VAN.4-5 in section 17.2.4.6.2 for AVA_VAN.5-5 is missing.
Type	te
Resolution - Correction / Interpretation	*<Update last two paragraphs of 17.2.5.6.1 as follows.>* Replacement of the last two paragraphs in section 17.2.5.6.1 and supplement of new section 17.2.5.6.2 for work unit AVA_VAN.5-5 according to AVA_VAN.4-5 in section 17.2.4.6.2. More detailed: **17.2.5.6.1 Work unit AVA_VAN.5-4** […] Items b) - f) are explained in greater detail in Annex B. The security architecture description should be considered in light of each of the above generic potential vulnerabilities. Each potential vulnerability should be considered to search for possible ways in which to defeat the TSF protection and undermine the TSF. **17.2.5.6.2 Work unit AVA_VAN.5-5** The evaluator ***shall record*** in the ETR the identified potential vulnerabilities that are candidates for testing and applicable to the TOE in its operational environment. It may be identified that no further consideration of the potential vulnerability is required if for example the evaluator identifies that measures in the operational environment, either IT or non-IT, prevent exploitation of the potential vulnerability in that operational environment. For instance, restricting physical access to the TOE to authorised users only may effectively render a potential vulnerability to tampering unexploitable. The evaluator records any reasons for exclusion of potential vulnerabilities from further consideration if the evaluator determines that the potential vulnerability is not applicable in the operational environment. Otherwise the evaluator records the potential vulnerability for further consideration. A list of potential vulnerabilities applicable to the TOE in its operational environment, which can be used as an input into penetration testing activities, shall be reported in the ETR by the evaluators.
Status	ma
Remarks	-

ID	CEM2022-R1-0109
Date	2023-12-22
Reference	17.2.5.7.1 / 6th paragraph

Issue – Problem Description	Guidance on determining the necessary attack potential to exploit a potential vulnerability can be found in B.4. Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	Guidance on determining the necessary attack potential to exploit a potential vulnerability can be found in B.6.
Status	ma
Remarks	-

ID	CEM2022-R1-0110
Date	2023-12-22
Reference	17.2.5.7.6 / 3rd paragrah
Issue – Problem Description	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. Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	The guidance in B.6 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.
Status	ma
Remarks	-

ID	CEM2022-R1-0111
Date	2023-12-22
Reference	18.3.1.2.4 / 11th paragraph, Table 5

Issue – Problem Description	18.3.1.2.4 11th paragraph: Table 5 provides guidance on how to determine consistency between assurance gained in the base component, the evidence provided for the composed TOE, and the analysis performed by the evaluator in the instances where inconsistencies are identified. **Table 5 - Guidance on how to determine consistency** Problem: Table numbering error. Table 5 -> Table 6.
Type	ed/te
Resolution - Correction / Interpretation	18.3.1.2.4 11th paragraph: Table 6 provides guidance on how to determine consistency between assurance gained in the base component, the evidence provided for the composed TOE, and the analysis performed by the evaluator in the instances where inconsistencies are identified. **Table 6 - Guidance on how to determine consistency**
Status	ma
Remarks	-

ID	CEM2022-R1-0112
Date	2023-12-22
Reference	18.6.1.3.4, 18.6.1.3.5, 18.6.2.3.5, 18.6.2.3.7
Issue – Problem Description	18.6.1.3.4, 3rd paragraph: Guidance on this work unit can be found in: • Subclause 15.2.1. • Subclause 15.2.2. 18.6.1.3.5, 3rd paragraph: Guidance on this work unit can be found in: • Subclause 15.2.1. • Subclause 15.2.2. 18.6.2.3.5, 2nd paragraph: Guidance on this work unit can be found in: • Subclause 15.2.1. • Subclause 15.2.2.

	18.6.2.3.7, 2nd paragraph: Guidance on this work unit can be found in: • Subclause 15.2.1. • Subclause 15.2.2. Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	18.6.1.3.4, 3rd paragraph: Guidance on this work unit can be found in: • Subclause 16.2.1. • Subclause 16.2.2. 18.6.1.3.5, 3rd paragraph: Guidance on this work unit can be found in: • Subclause 16.2.1. • Subclause 16.2.2. 18.6.2.3.5, 2nd paragraph: Guidance on this work unit can be found in: • Subclause 16.2.1. • Subclause 16.2.2. 18.6.2.3.7, 2nd paragraph: Guidance on this work unit can be found in: • Subclause 16.2.1. • Subclause 16.2.2.
Status	ma
Remarks	-

ID	CEM2022-R1-0113
Date	2023-12-22
Reference	A.5.1 / bullet for “access control to development systems;”
Issue – Problem Description	• access control to development systems; • policies for access control and logging.; • policies for project specific assignment and changing of access rights. Problem: “access control to development systems;” shall be a upper level

	item.
Type	ed
Resolution - Correction / Interpretation	access control to development systems: • policies for access control and logging.; • policies for project specific assignment and changing of access rights.
Status	ma
Remarks	-

ID	CEM2022-R1-0114
Date	2023-12-22
Reference	A.5.2 / bullet for “infrastructure”
Issue – Problem Description	• infrastructure Security measures for physical access control to the development site and rationale for the effectiveness of these measures. Problem: Editorial error.
Type	ed
Resolution - Correction / Interpretation	Infrastructure: • Security measures for physical access control to the development site and rationale for the effectiveness of these measures.
Status	ma
Remarks	-

ID	CEM2022-R1-0115
Date	2023-12-22
Reference	Annex B / 2nd paragraph
Issue – Problem Description	This annex consists of two major parts: a) guidance for completing an independent vulnerability analysis. This is summarized in B.1.1 and described in more detail in B.1.2. These subclauses describe how an evaluator should approach the construction of an independent vulnerability analysis. b) how to characterise and use assumed Attack Potential of an attacker. This is described in B.1.5 to B.3. These subclauses provide an example of how an attack potential can be characterised and should be used, and provide examples.

	Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	This annex consists of two major parts: a) guidance for completing an independent vulnerability analysis. This is summarized in B.1 and described in more detail in B.2. These subclauses describe how an evaluator should approach the construction of an independent vulnerability analysis. b) how to characterise and use assumed Attack Potential of an attacker. This is described in B.5 to B.7. These subclauses provide an example of how an attack potential can be characterised and should be used, and provide examples.
Status	ma
Remarks	-

ID	CEM2022-R1-0116
Date	2023-12-22
Reference	B.2 / 3rd paragraph
Issue – Problem Description	However, vulnerability analysis should not be performed as an isolated activity. It is closely linked with ADV and AGD. The evaluator performs these other evaluation activities with a focus on identifying potential vulnerabilities or "areas of concern". Therefore, evaluator familiarity with the generic vulnerability guidance (provided in B.1.3) is required. Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	However, vulnerability analysis should not be performed as an isolated activity. It is closely linked with ADV and AGD. The evaluator performs these other evaluation activities with a focus on identifying potential vulnerabilities or "areas of concern". Therefore, evaluator familiarity with the generic vulnerability guidance (provided in B.3) is required.
Status	ma
Remarks	-

ID	CEM2022-R1-0117
Date	2023-12-22
Reference	B.3.1 / 2nd paragraph / d)
Issue – Problem	d) using a component in an unexpected context or for an unexpected purpose includes using an unrelated TOE interface to bypass the TSF by

Description	using it to achieve a purpose that it was not designed or intended to achieve. Covert channels are an example of this type of attack (see B.1.3.4 for further discussion of covert channels). The use of undocumented interfaces, which may be insecure, also falls into this category. Such interfaces may include undocumented support and help facilities; Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	d) using a component in an unexpected context or for an unexpected purpose includes using an unrelated TOE interface to bypass the TSF by using it to achieve a purpose that it was not designed or intended to achieve. Covert channels are an example of this type of attack (see B.3.4 for further discussion of covert channels). The use of undocumented interfaces, which may be insecure, also falls into this category. Such interfaces may include undocumented support and help facilities;
Status	ma
Remarks	-

ID	CEM2022-R1-0118
Date	2023-12-22
Reference	B.4.2.2 / 1st paragraph
Issue – Problem Description	The unstructured analysis to be performed by the evaluator [for Evaluation of sub-activity (AVA_VAN.2)] permits the evaluator to consider the generic vulnerabilities (as discussed in B.1.3). The evaluator will also apply their experience and knowledge of flaws in similar technology types. Problem: Referencing error.
Type	ed/te
Resolution - Correction / Interpretation	The unstructured analysis to be performed by the evaluator [for Evaluation of sub-activity (AVA_VAN.2)] permits the evaluator to consider the generic vulnerabilities (as discussed in B.3). The evaluator will also apply their experience and knowledge of flaws in similar technology types.
Status	ma
Remarks	-

ID	CEM2022-R1-0119
Date	2024-06-07
Reference	13.3.1.4.4

Issue – Problem Description	Refer to CC2022-P2-R1-0018 and its problem description and resolution concerning the SFR FPT_INI.1 in [CC:2022-2], section 15.4.
Type	te
Resolution - Correction / Interpretation	Section 13.3.1.4.4, last para for work unit ADV_ARC.1-3: The TOE components related to TSF initialisation are considered part of the TSF, and analysed from that perspective. It should be noted that even though these are evaluated as part of the TSF, it is likely that a justification (as allowed by TSF internals (ADV_INT)) can be made that they do not have to meet the internal structuring requirements of ADV_INT.
Status	ma
Remarks	-

ID	CEM2022-R1-0120
Date	2024-06-07
Reference	13.8.5
Issue – Problem Description	Problem: Missing entry for E-element ADV_TDS.5.2E defined in [CC:2022-3], section 10.6.4.
Type	te
Resolution - Correction / Interpretation	Incorporation of new section **13.8.5.5 Action ADV_TDS.5.2E** directly after section 13.8.5.4.14. Subsequent section number 13.8.5.4.15 is changed to 13.8.5.5.1, and 13.8.5.4.15 is switched to 13.8.5.5.2 as the Work Units ADV_TDS.5-14 and ADV_TDS.5-15 belong to ADV_TDS.5.2E.
Status	ma
Remarks	-

References

[CC:2022-1] CCMB-2022-11-001: Common Criteria for Information Technology Security Evaluation, CC:2022, Part 1: Introduction and general model, Revision 1, November 2022

[CC:2022-2] CCMB-2022-11-002: Common Criteria for Information Technology Security Evaluation, CC:2022, Part 2: Security functional components, Revision 1, November 2022

[CC:2022-3] CCMB-2022-11-003: Common Criteria for Information Technology Security Evaluation, CC:2022, Part 3: Security assurance components, Revision 1, November 2022

[CC:2022-4] CCMB-2022-11-004: Common Criteria for Information Technology Security Evaluation, CC:2022, Part 4: Framework for the specification of evaluation methods and activities, Revision 1, November 2022

[CC:2022-5] CCMB-2022-11-005: Common Criteria for Information Technology Security Evaluation, CC:2022, Part 5: Pre-defined packages of security requirements, Revision 1, November 2022

[CEM:2022] CCMB-2022-11-006: Common Methodology for Information Technology Security Evaluation, CEM:2022, Evaluation Methodology, Revision 1, November 2022