ETSI TS 102 165-3 V1.1.1 (2025-12)

TECHNICAL SPECIFICATION

Cyber Security (CYBER);
Methods and Protocols for Security;
Part 3: Vulnerability Assessment extension for TVRA

Reference
DTS/CYBER-00122

Keywords
risk, testing, vulnerabilities

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document defines the application of the Common Criteria Vulnerability Assessment class defined in Common Criteria part 3 [1] alongside the ETSI TVRA method defined in ETSI TS 102 165-1 [2].

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are necessary for the application of the present document.

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

[2] ETSI TS 102 165-1: "Cyber Security (CYBER); Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[3] Common Criteria CCMB-2022-11-006: "Common Methodology for Information Technology, Security Evaluation, Evaluation methodology", November 2022, Revision 1.

[4] Common Criteria CCMB-2022-11-001: "Common Criteria for Information Technology, Security Evaluation, Part 1: Introduction and general model".

[5] Common Criteria CCMB-2022-11-002: "Common Criteria for Information Technology, Security Evaluation, Part 2: Security functional components".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[i.2] Cybersecurity Certification: Candidate EUCC Scheme V1.1.1.

NOTE: The EUCC scheme is a Common Criteria based European candidate cybersecurity certification scheme and issued by the European Union Agency for Cybersecurity (ENISA).

[i.3] S. W. Cadzow: "Security assurance and standards - design for evaluation", The 2nd IEE Secure Mobile Communications Forum: Exploring the Technical Challenges in Secure GSM and WLAN, 2004. (Ref. No. 2004/10660), London, UK, 2004, pp. 8/1-8/6, doi: 10.1049/ic.2004.0664.

[i.4] ETSI's Making Better Standards.

[i.5] ETSI TS 102 165-2: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures".

NOTE: An update is in preparation.

[i.6] Raphaël Hertzog, Jim O"Gorman and Mati Aharoni: "Kali Linux Revealed Mastering the Penetration Testing Distribution", ISBN: 978-0-9976156-0-9.

[i.7] ETSI TS 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.8] ETSI TS 103 993: "Cyber Security (CYBER); ONDS Test Suite Structure and Test Purposes".

[i.9] ETSI ES 202 553: "Methods for Testing and Specification (MTS); TPLan: A notation for expressing Test Purposes".

[i.10] ETSI ES 202 383: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Security Targets".

[i.11] Recommendation ITU-T I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[i.12] ETSI TS 103 996: "Cyber Security (CYBER); ONDS Protection profile - Test cases".

[i.13] ETSI TS 103 962: "CYBER; Optical Network and Device Security; Security provisions in Optical Access Network Devices".

[i.14] ETSI TS 104 102: "Cyber Security (CYBER); Encrypted Traffic Integration (ETI); ZT-Kipling methodology".

[i.15] Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

[i.16] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

[i.17] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166.

[i.18] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

[i.19] ETSI TS 104 158-1: "Securing Artificial Intelligence TC (SAI); AI Common Incident Expression (AICIE); Part 1".

[i.20] ETSI TS 104 170: "Cyber Security (CYBER); Universal Cybersecurity Information Exchange Framework - Repository".

[i.21] NIST Special Publication 800-115: "Technical Guide to Information Security Testing and Assessment".

[i.22] EC Council: "Understanding the Five Phases of the Penetration Testing Process".

[i.23] ETSI TR 103 306 (V1.4.1): "CYBER; Global Cyber Security Ecosystem".

[i.24] Global CVE Allocation System.

[i.25] NIST: "National Vulnerability Database".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

blue team: group acting as a corollary to a red team in order to develop measures to counter physical or digital attacks

high assurance level: assurance that ICT products, ICT services and ICT processes where the corresponding security requirements, including security functionalities, are provided at a level intended to minimize the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with significant skills and resources

NOTE: A contextual definition is given in CSA Article 52.7 [i.1].

red team: group that simulates an adversary in order to attempt physical or digital attacks

substantial assurance level: assurance that the ICT products, ICT services and ICT processes where the corresponding security requirements, including security functionalities, are provided at a level intended to minimize the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources

NOTE: A contextual definition is given in CSA Article 52.6 [i.1].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

(P)ICS	(Protocol) Implementation Conformance Statement
AI	Artificial Intelligence
AICIE	AI Common Incident Expression
API	Application Programming Interface
CC	Common Criteria
CEM	CC Evaluation Methodology
CSA	Cyber Security Act
CSC	Cyber Security Control
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DORA	Digital Operational Resilience Act
EUCC	EU Common Criteria Certification
GCVE	Global CVE Allocation System

NOTE: See https://gcve.eu.

IA	Information Assurance
ICT	Information Communication Technology
IUT	Instrument Under Test
NVD	National Vulnerability Database
ONDS	Optical Network Device Security
PICS	Protocol Implementation Conformance Statement
PP	Protection Profile
SDO	Standards Development Organisation
SFR	Security Functional Requirement
SP	Special Publication
ST	Security Target
ToE	Target of Evaluation
TP	Test Purpose
TSF	ToE Security Function
TSS	Test Suite Structure
TTCN-3	Testing and Test Control Notation Version 3
TVRA	Threat Vulnerability Risk Analysis
UCYBEX	Universal Cybersecurity Information Exchange Framework
ZT	Zero Trust

4 Overview of AVA_VAN

4.1 Vulnerability analysis and its role in risk assessment

NOTE 1: AVA_VAN is described in clause 14 of CC Part 3 [1] and is not strictly an acronym or abbreviation but can be read as part of the Vulnerability Assessment class and the term AVA_VAN read as a word in its own right.

The approach to risk analysis given in ETSI TS 102 165-1 [2] is to determine the level of risk to each stakeholder from an assessment of the likelihood and impact of an attack by a threat agent against an asset, or collection of assets, within a system. The presumption in ETSI TS 102 165-1 [2] is that all assets have weaknesses that become vulnerabilities if a viable threat can be enacted against them. If no viable threat can be enacted the risk assessment is that there is either no risk or minimal risk and that specific countermeasures to mitigate any threat are unnecessary (as the threat is not viable).

The wording of the AVA_VAN class in Common Criteria part 3 [1] is very slightly different as it refers to an exploitable vulnerability (in ETSI TS 102 165-1 [2] a vulnerability is an exploitable weakness). The developer actions for AVA_VAN are relatively simply worded to indicate the developer shall make the TOE available for testing and that it shall be suitable for testing. There is an increasing scale of the depth of analysis from AVA_VAN.1 requiring a vulnerability survey, through AVA_VAN.3 requiring a focussed analysis, and AVA_VAN.5 requiring an Advanced methodical analysis. At the higher levels it is required to conduct a penetration test to verify the implementation.

The wording of ETSI TS 102 165-1 [2] uses the terms threat and threat-agent in the context "*A threat is enacted by a threat agent, and may lead to an unwanted incident breaking certain pre-defined security objectives*" whereas the Common Criteria Part 1 [4] use of the same terms is "*A threat consists of an adverse action performed by a threat agent on an asset*".

NOTE 2: The way in which terms are used in [1] and [3] differ from their use in [2] because the position of the active party is different, in [1] and [3] the terms are used from the perspective on an evaluator determining if the provisions are implemented satisfactorily and if they are sufficient to address the identified risk, whereas in [2] the perspective is to give guidance or to provide a mandate to a developer in determination of a suitable counter to an identified risk.

NOTE 3: The present document addresses the EUCC programme [i.2], [i.15] for only the 2022 versions of Common Criteria [1], [3], [4], [5] and does not allow for use of earlier versions as allowed until the end of 2027 by Article 3(20) of the EUCC Implementing Act [i.15].

4.2 Addressing the evaluator expectations in standards

Common Criteria part 3 [1] addresses the actions of an evaluator and for the purposes of the present document is addressed by equating an evaluator to a test environment.

The present document addresses steps in the development cycle, for standards and for products, that when followed will give confidence to the development group that an evaluator will give a PASS verdict. Thus, while the Common Criteria Evaluation Method (CEM) [3] defines in some detail the tasks that an evaluator is expected to complete the present document identifies how a developer should prepare for the evaluation and is therefore complimentary to [3] albeit from a different stance/perspective. This is also addressed by the "design for evaluation" paradigm in [i.3] that has been inherited in ETSI's work programme including ETSI TS 102 165-1 [2] and ETSI TS 102 165-2 [i.5].

EXAMPLE: For AVA_VAN.1.3E in [3] there are 7 work units identified (in addition to work units identified for prior levels of AVA_VAN.1) to be undertaken by the evaluator that combine to provide content for the Evaluation Test Report (ETR). In the present document the role of standards, and standards developers, in allowing the evaluator to perform the relevant tasks is addressed.

4.3 Addressing evaluation in the standards development process

The model for standards development excellence, as outlined in ETSI's Making Better Standards [i.4] requires that standards are developed against the following criteria:

- **Necessary:** it (a standard) should specify only what is required to meet its objectives, and not impose a particular approach to implementation.
- **Unambiguous:** it should be impossible to interpret the normative parts of the standard in more than one way.
- **Complete:** the requirement should contain all the information necessary to understand that requirement, either directly or by reference to other documents. The reader of a standard should not need to make assumptions about the implementation of any requirement.
- **Precise:** the requirement should be worded clearly and exactly, without unnecessary detail that might confuse the reader.
- **Well-structured:** the individual elements of the requirement should all be included in an appropriate and easy-to-read manner.
- **Consistent:** there should be no contradiction between different requirements within the standard, nor with other related standards.
- **Testable:** there should be clear and obvious means of demonstrating that an implementation complies with the requirement.

The mapping for evaluation is addressed specifically in the testable criterion. The convention in ETSI for testing of deterministic standards is that formal conformance tests are developed (a flow of the documents is given in Figure 1). In the test environment considered above (and shown in Figure 1) there is an assumption that the test verdict is either PASS or FAIL. In some cases a verdict of INDETERMINATE can be given.

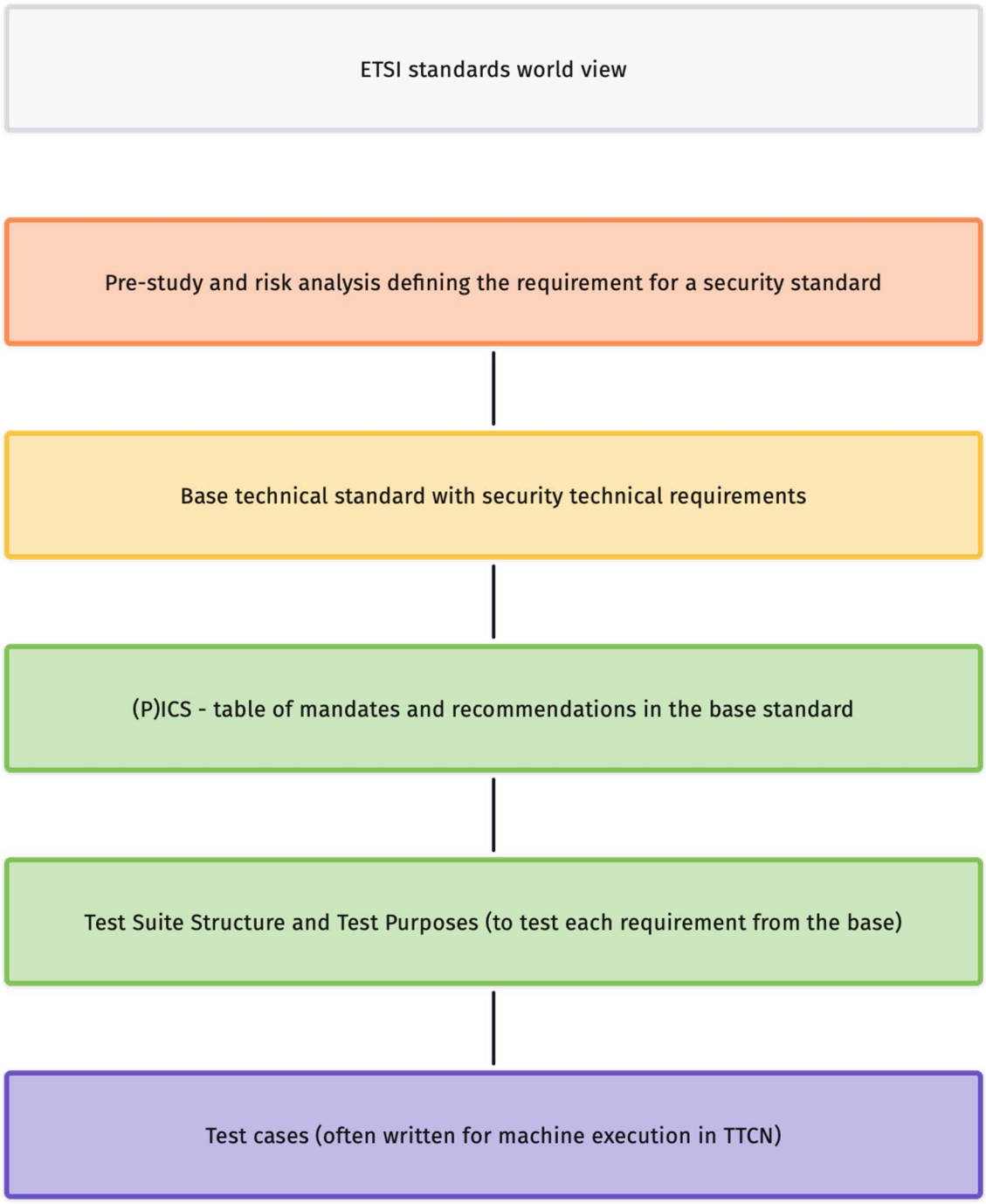

Figure 1: Standards document flow from requirement to testing

Where there is a degree of uncertainty from closed-box testing that the requirement being tested passes or fails it may be appropriate to allow expert evaluation to make a deeper examination of the equipment or implementation in order to assign a pass or fail verdict. The general requirement is that even if the security offered by an equipment or implementation has some uncertainty that the test or evaluation environment is deterministic.

NOTE: A test verdict of INDETERMINATE is often accompanied by advice on why a test verdict of PASS or FAIL could not be assigned. As an INDETERMNATE verdict signifies that the test outcome cannot be definitively determined the test report should identify why, such as missing information, unexpected behaviour, or limitations of the testing environment.

EXAMPLE: A test to determine if an element is "secure" is mostly non-deterministic as the context of both the attacker and the placement of the element is critical to make a determination. The evaluation process as per [3] takes account of the context in making the determination.

5 Provisions for content and provision of evidence

5.1 Expected evidence defined in CEM

The AVA_VAN class in CEM [3] requires the evidence outlined in Table 1. Whilst [3] identifies the evidence requirements the present document identifies the role of ETSI standards that may be used in providing that evidence.

Table 1: Evidence requirements against AVA_VAN from CEM [3]

AVA_VAN class	Attack potential	Evidence requirement in CEM [3]
AVA_VAN.1.3E	Basic	a) the ST; b) the guidance documentation; c) the TOE suitable for testing; d) information publicly available to support the identification of potential vulnerabilities.
AVA_VAN.2.4E	Basic	a) the ST; b) the functional specification; c) the TOE design; d) the security architecture description; e) the guidance documentation; f) the TOE suitable for testing; g) information publicly available to support the identification of possible potential vulnerabilities.
AVA_VAN.3.4E	Enhanced-Basic	a) the ST; b) the functional specification; c) the TOE design; d) the security architecture description; e) the implementation subset selected; f) the guidance documentation; g) the TOE suitable for testing; h) information publicly available to support the identification of possible potential vulnerabilities; i) the results of the testing of the basic design.
AVA_VAN.4.4E	Moderate	a) the ST; b) the functional specification; c) the TOE design; d) the security architecture description; e) the implementation representation; f) the guidance documentation; g) the TOE suitable for testing; h) information publicly available to support the identification of possible potential vulnerabilities; i) the results of the testing of the basic design.
AVA_VAN.5.4E	High	a) the ST; b) the functional specification; c) the TOE design; d) the security architecture description; e) the implementation representation; f) the guidance documentation; g) the TOE suitable for testing; h) information publicly available to support the identification of possible potential vulnerabilities; i) the results of the testing of the basic design.

5.2 Support to CEM evidence requirements from SDOs/ETSI

5.2.1 The ST

The Security Target (ST) may be defined by reference to a standard, particularly if the standard is a Protection Profile (PP). In such a case the ST can claim to be conformant to the PP.

NOTE: ETSI ES 202 383 [i.10], whilst referring to a prior version of Common Criteria, makes recommendations for the preparation of an ST with the following disclaimer "*CC evaluation involves the preparation of a Security Target (ST) that specifies the security requirements for an identified Target Of Evaluation (TOE) and describes the functional and assurance security measures offered by that TOE to meet the stated requirements. As an ST is directly related to the final TOE and is therefore prepared by the TOE developer there is no impact on the standardization process*".

In preparing the ST the guidance offered in clause 5.3 of ETSI ES 202 383 [i.10] should be taken into account.

Where the ST is developed to conform to a standard the standards suite that have been adopted shall be cited by the ST developer.

5.2.2 The functional specification

As stated in CEM [3] a functional specification provides a description of the purpose and method-of-use of interfaces to the TSF. The ToE Security Function (TSF) may be described by a technical standard. Commonly many standards will identify the pre-conditions, stimuli, and post-conditions for invocation of a TSF.

Where the standard is defined as a PP identifying SFRs it is reasonable to expect that the TSFs are similarly defined in a standard.

NOTE: In the 3-stage development approach defined by Recommendation ITU-T I.130 [i.11] a mapping of the PP containing abstract SFRs to stage 2 can be made, with the more detailed functionality at stage 3 being the domain of TSFs.

EXAMPLE: In ETSI TS 103 996 [i.12] it is identified that the TOE includes FIA_API.1 Authentication proof of identity, with the specific text "The TSF shall provide an [assignment: ***authentication mechanism***] to prove the identity of [assignment: ***entity***] by including the following properties [assignment: ***list of properties***] to an external entity". Where the TOE is being externally accessed then the identity of the accessing entity could be proven by digitally signing a document where the public key for verification is known, or accessible, to the TOE. In which case the entire protocol of the authentication using digital signature may be defined in a standard and that standard identified. In the particular case of ETSI TS 103 996 [i.12] this is contained in ETSI TS 103 962 [i.13] which makes further reference to specific frameworks for authentication given in ETSI TS 102 165-2 [i.5].

5.2.3 The TOE design

Where a standard, or suite of standards, is used as the basis of the design of TSFs the relevant standards should be cited in the evidence. Where standards are profiled, or where the TSFs in the TOE are derived from a chain of documents, e.g. a PP, or a stage 1 or stage 2 definition per Recommendation ITU-T I.130 [i.11], these should also be cited in the evidence.

The TOE is intended to be a secure system and the evidence should be clear in the design documentation. Where a TVRA exercise [2], or a ZT-Kipling exercise [i.14] has been carried out, and which identifies the form of threat that the system has been designed to be resilient against, this should also include evidence of resilience against known threats and vulnerabilities.

5.2.4 The security architecture description

Any security component, e.g. an authentication service, may be described in detail by a standard and the overall security architecture of a component or system may also be defined by a standard. For example, ETSI TS 102 165-2 [i.5] identifies a number of functional components and their dependencies, and a standard may build on this framework to refine the operation for the identified ST and thus be used as a reference architecture for the ST (in such cases as suggested in clause 5.2.2 above the models from ETSI TS 102 165-2 [i.5] can be identified as TSFs).

NOTE: Whilst it is suggested above the models from ETSI TS 102 165-2 [i.5] can be identified as TSFs that is not their primary function, rather they serve as exemplars for more detailed refinement in specific applications.

5.2.5 The implementation representation

5.2.5.1 Overview of the role of standards in representing the implementation

Not specific to standardization but in cases where the implementation conforms to any standard that standard should be cited in the evidence.

NOTE: The citing of standards should not only address those from an SDO, for example if the development organization has particular standards for development, quality control and so on, these should also be cited as evidence of the rigour of the process leading to the implementation.

5.2.5.2 Role of security controls (as defined in ETSI TS 103 305-1)

In addition to the determination of risk given in ETSI TS 102 165-1 [2], and the adoption of common frameworks as given in ETSI TS 102 165-2 [i.5] in order to counter identified threats and mitigate the risk they represent, and the approach to vulnerability analysis and penetration testing outlined in the present document, there are a set of security controls that apply, in part, to the organization using and deploying ICT equipment in a secure manner.

Whilst a summary of the applicability of such controls is given in ETSI TS 103 305-1 [i.7] it is stressed that any ICT product is vulnerable if weaknesses exist in the supply chain or the development organizations. In addition, to support the rationale for the existence of any asset in a system the ZT-Kipling criteria defined in ETSI TS 104 102 [i.14] should be applied.

NOTE: The purpose of applying the ZT-Kipling method from ETSI TS 104 102 [i.14] is to build evidence that any asset in the system has a known and justified role. Thus, by application of the asset inventory using CSC-1 [i.7] and by validating the purpose of each asset using the ZT-Kipling criteria the developer should have confidence that they can demonstrate to an evaluator that they understand the system. Extending this understanding further by application of the TVRA method from ETSI TS 102 165-1 [2] should demonstrate to the evaluator that a thorough approach to secure system design has been applied by the developer.

Table 2: Mapping of CSCs to AVA_VAN expectations

Control from ETSI TS 103 305-1 [i.7]	Rationale in addressing AVA_VAN
Control 1: Inventory and Control of Enterprise Assets (as defined in ETSI TS 103 305-1 [i.7] an enterprise asset is one with the potential to store or process data, and is identified as hardware)	A complete inventory of assets in the system is essential to give assurance to the evaluator that the developer has understood the scope of each element of the system and how they interact. Thus, for the present document no real distinction is made between the form of asset (hardware or software). The application of the ZT-Kipling criteria from ETSI TS 104 102 [i.14] gives a detailed justification of the presence and role of any asset.
Control 2: Inventory and Control of Software Assets (as defined in ETSI TS 103 305-1 [i.7] a software asset is a discrete package of data and instructions used to direct a computer to complete a specific task, including operating systems and applications)	
Control 3: Data Protection	In applying this control from the perspective of the present document the primary function is to identify data as system assets and to establish and document the role of each data asset and how its role is protected.
Control 4: Secure Configuration of Enterprise Assets and Software	The bulk of the remaining controls reflect good organizational processes and as cited in the note of clause 5.2.5.1 may be used in the overall documentary evidence of the process in which systems are developed.
Control 5: Account Management	
Control 6: Access Control Management	
Control 7: Continuous Vulnerability Management	
Control 8: Audit Log Management	
Control 9: Email and Web Browser Protections	
Control 10: Malware Defences	
Control 11: Data Recovery	
Control 12: Network Infrastructure Management	
Control 13: Network Monitoring and Defence	
Control 14: Security Awareness and Skills Training	
Control 15: Service Provider Management	
Control 16: Application Software Security	
Control 17: Incidence Response Management	
Control 18: Penetration Testing	See Annex A of the present document.

5.2.6 The guidance documentation

The details of guidance documentation are addressed in [1] in the class AGD. The intent is to ensure that all relevant aspects for the secure handling of the TOE are described, including the possibility of unintended incorrect configuration or handling of the TOE. Whilst some of the details will be implementation specific there are many aspects that will be guided by standards and processes that may be used to supplement the data.

EXAMPLE: A system may be designed with the ability for a user to choose a password but if that password is weak it can be circumvented. The guidance should identify how to create and use a strong password, and the system itself should prohibit weak ones. Making the guidance clear, and ensuring the system operation and the guidance are aligned, is critical to a successful evaluation of a secure system.

5.2.7 The TOE suitable for testing

Not relevant to standards (if the TOE is built to conform to standards that has already been addressed). See also clause 5.2.3 above.

5.2.8 Information publicly available to support the identification of possible potential vulnerabilities

In general the recommendation for any security work in order to identify the necessary security functionality a TVRA should be performed. The guidance given in ETSI TS 102 165-1 [2] therefore applies. In addition where the ST makes use of known software or hardware the developer should have performed a documentary analysis of reported vulnerabilities in public databases.

NOTE: The further development of standards in this domain such as AICIE for AI vulnerabilities (see ETSI TS 104 158-1 [i.19]) and UCYBEX for general cybersecurity vulnerabilities in ETSI TS 104 170 [i.20] should be cited and integrated to the system design.

5.2.9 The results of the testing of the basic design

The general principles of good standards design outlined in clause 4.3 above and listed as "***Testable**: there should be clear and obvious means of demonstrating that an implementation complies with the requirement*" should indicate that a test specification exists for each element of the design and for the composition of those elements in the particular configuration required of the design.

6 Determination of attack potential

The AVA_VAN class is mapped to attack potential as follows. Attack potential is defined in ETSI TS 102 165-1 [2] using the weighted summation method, the metrics of which are mapped to Annex B of CEM [3] but as per the note in clause 4.1 above written from the perspective of the analyst and not the evaluator. The mapping of the results of the weighted summation analysis to the attack potential measures described in AVA_VAN given in ETSI TS 102 165-1 [2] are copied below and annotated as appropriate.

Table 3: Mapping of the weighted summation analysis to attack potential

Attack potential values	Attack potential required to exploit attack	Resistant to attacker with attack potential of	AVA_VAN	CSA [i.1] rating
0 to 9	Basic	No rating		CSA-Basic
10 to 13	Enhanced-basic	Basic	AVA_VAN.1 and AVA_VAN.2	CSA-Substantial
14 to 19	Moderate	Enhanced basic	AVA_VAN.3	CSA-High
20 to 24	High	Moderate	AVA_VAN.4	CSA-High
> 24	Beyond High	High	AVA_VAN.5	CSA-High

The developer should be aware that over time attacks are often refined and distributed in a way that increases the likelihood, by either reducing the level of expertise or nature of the equipment required to instantiate the attack. Thus, a system made available at time t0 expected to be resistant to an attack potential High, may over time only be resistant to an attack potential of Basic.

Table 4: Expectation of evaluator tasks in AVA_VAN class

AVA_VAN class	Attack potential	Notes
AVA_VAN.1.3E AVA_VAN.2.4E	Basic	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.
AVA_VAN.3.4E	Enhanced-Basic	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Enhanced-Basic attack potential.
AVA_VAN.4.4E	Moderate	The evaluator shall conduct penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing Moderate attack potential.
AVA_VAN.5.4E	High	The evaluator shall conduct penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing High attack potential.

A designer may determine the risk of the system by conducting an analysis using the methods described in ETSI TS 102 165-1 [2]. In doing so it will be determined by the analyst what level of expertise the system offers protection against, i.e. in developing the analysis to identify necessary countermeasures the analyst will have made a quantitative assessment of both the attacker capability and motivation, and the resistance to attack offered by the security functions defined. In documenting the analysis undertaken the analyst will be expected to have performed some form of intellectual or actual penetration test in order to validate the results.

As shown in Table 4 the evaluator shall conduct penetration testing at a level consistent with the attack potential, therefore the developer should have identified the likelihood of an attacker with the appropriate level of attack potential in conducting their pre-design risk evaluation and, as stated in ETSI TS 102 165-1 [2], updated that analysis as the design is developed. The fully documented TVRA ETSI TS 102 165-1 [2] should be part of the evidence that the selected security functions (SFRs and TSFs) are sufficient to address the identified attack potential.

7 Standards for the conduct of penetration tests

7.1 Preparing for a penetration test

Penetration testing differs from vulnerability testing and vulnerability identification as outlined in clause 4.1. Vulnerability identification as outlined in ETSI TS 102 165-1 [2] identifies the attack surface and from there assesses the risk to assets. The approach outlined in ETSI TS 103 305-1 [i.7] addresses vulnerability testing as a check for the presence of known, insecure enterprise assets, and stops there, although the analysis of ETSI TS 102 165-1 [2] identifies the nature of the threat agent and the means of enabling the threat agent to determine likelihood of an attack. Penetration testing as described in ETSI TS 103 305-1 [i.7] is closer to the form of analysis identified in ETSI TS 102 165-1 [2] by identifying means to exploit weaknesses to see how far an attacker could get, and what business process or data might be impacted through exploitation of that vulnerability.

A particular characteristic of penetration testing identified in ETSI TS 103 305-1 [i.7] is that it requires more human involvement and analysis.

As outlined in clause 6, and in AVA_VAN, the evaluator is mandated to conduct penetration testing. There are no ETSI standards for the conduct of penetration testing, however some aspects of penetration testing are addressed in ETSI TS 103 305-1 [i.7] (see clause 7.2 below). There are many industry guides, and some guidance to the evaluator in Common Criteria Part 3 [1] and in CEM [3]. One key document in this regard is NIST SP 800-115 [i.21] but it is also recognized that there are considerable public resources that offer training in a number of forms of penetration testing (see Annex A).

7.2 Application of CSC-18 from ETSI TS 103 305-1

ETSI TS 103 305-1 [i.7] addresses Penetration Testing in Control 18 and this is addressed in more detail below with movement of some elements to mandated actions of the developer in order to be able to meet the expectations of the evaluator.

Table 5: Review of CSC18 from ETSI TS 103 305-1 [i.7] to AVA_VAN

Safeguard	Asset Type	Security Function	Safeguard Title	Safeguard Description
18.1	Documentation	Govern	Establish and Maintain a Penetration Testing Program	Establish and maintain a penetration testing program appropriate to the size, complexity, industry, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
18.2	Network	Detect	Perform Periodic External Penetration Tests	Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing should include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and should be conducted through a qualified party. The testing may be clear box or opaque box.
18.3	Network	Protect	Remediate Penetration Test Findings	Remediate penetration test findings based on the enterprise's documented vulnerability remediation process. This should include determining a timeline and level of effort based on the impact and prioritization of each identified finding.
18.4	Network	Protect	Validate Security Measures	Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.
18.5	Network	Detect	Perform Periodic Internal Penetration Tests	Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.

The content of CSC-18.1 shows the essential requirement to have a penetration testing programme within the organization. The result of having this as an organizational stance is expected that in the development parts of the organization that in addition to the conventional functional, interoperability, and maintenance testing activities that the development groups have enabled penetration testing teams (e.g. red-teaming). In this example Red-teams may be used to address CSC-18.2, and CSC-18.5 with mirror Blue-teams addressing CSC-18.3 and CSC-18-4.

7.3 Formal and semi-formal test definitions applied to vulnerability analysis

As identified in ETSI TS 103 993 [i.8] using the test purpose notation described in ETSI ES 202 553 [i.9] it can be shown how any requirement in the system should be tested. It is strongly recommended that the developer, in the documentation suite (see clauses 5.1 and 5.2 above) includes, either by reference or directly in the package, the relevant test standards, including a TSS&TP.

In preparing a TSS&TP using the TPLan notation of ETSI ES 202 553 [i.9] it should be clear to both the developer and to the evaluator how any security function is to be tested.

EXAMPLE: The Test Purpose copied below from ETSI TS 103 993 [i.8] identifies the objective of the test, the pre-conditions and the behaviour to be verified.

TP Id	ONDS-IA-001
Test Objective	The identity shall always be authenticated on first presentation and periodically thereafter (the latter also is used to verify the operation of periodic re-establishment of a security association (here for authentication)).
Reference	REQ-31, REQ-30, REQ-4, REQ-8 (implicit), REQ-22, REQ-29
Configuration	
PICS Selection	

Initial conditions

```
with {IUT in NotIdentified and NotAuthenticated}
with {IUT 'having relevant algorithms and key formats defined in the security policy}
```

Expected behaviour

```
ensure that {
    when {IUT receives 'Startup' or 'Reauthentication timer expires'}
    then [IUT sends authentication-claim containing 'semantic or canonical identifier'}
    when {IUT receives authentication-verification}
    then {IUT in Authenticated and Identified}
}
```

Annex A (normative): Application of tools for penetration testing

A.1 Overview of penetration testing phases

A system cannot be made immune to attack, but can be made more resilient or resistant to attack. In this case the conventional analysis of identifying what the system is, the attack surface and the boundary of that attack surface, and the purpose of the system and its defences, are all critical to determining where the system is most at risk from exploit.

The developer has to assume that the system will be vulnerable even if all protections are implemented, if only because some of the system will be implemented with errors, or the assumptions made by the designer will be proven to be false.

EXAMPLE 1: A designer may assume that data in memory with strict access control cannot be altered without authorization, i.e. assumes that the only means to read and write data is through the access control system. However, if there is no strict hardware protection of the memory elements there is a potential to modify the memory content electrically. Thus, it may be necessary to specify not just the strict security controls (e.g. access control, authentication) but also the form of memory device used.

EXAMPLE 2: An integer value may be represented as having only 8 bits of range (i.e. 0 to 255), but stored in a 64 bit memory structure on the assumption, by the designer, that only the relevant 8 bits of the field are read and the rest ignored. If however a coding error reads the value as a 16- or 32- or 64-bit value and there is no bounds checking to verify the number is in the correct range the system may end up operating on invalid data. If the value is assigned a meaning "maximum speed" with a view to throttling back the system when the speed is exceeded, and this was encoded as 0C in hex as an 8-bit element but when read as a 32-bit element read 1F 1F 1F 0C then the system, without bounds checking (i.e. it acts on the entire 32 bits and not on the 8 relevant bits), could overstress the machine (allowing it to run to dangerous speed) and cause damage.

It is expected that an unbounded penetration test will succeed to break one or more TSFs, or bypass one or more TSFs. The particular application of AVA_VAN provides some boundaries to the penetration testing.

The primary aim of a penetration test is to show exploitation of a system by means of a discovered vulnerability.

One model of penetration testing is the 5-phase model from EC-Council [i.22] that is elaborated for the present document in the succeeding clauses.

NOTE: Many of the tools described in this annex can be readily found online (e.g. kali.org [i.6]).

A.2 Information Gathering

NOTE: This phase is often also referred to as Reconnaissance.

Addressed in large part by ETSI TS 102 165-1 [2]. May exploit security controls given in ETSI TS 103 305-1 [i.7] in order to determine the assets and control of the organization, in addition the analyst may apply the ZT-Kipling method from ETSI TS 104 102 [i.14] to assist in determining the legitimacy of any asset in the system.

See also clause 5.2.5.2 of the present document and the role of each of the cited documents in building evidence of the rigour of the system and its likely attacks.

A.3 Vulnerability Discovery

Vulnerability discovery is addressed in ETSI TS 102 165-1 [2] by systematically identifying how any weakness in an asset, or combination of assets, can be attacked (the definition of vulnerability requiring both a weakness and a means to exploit that weakness).

Many known vulnerabilities have been listed in public repositories, and have been evaluated and rated using the CVE metrics [i.25] or GCVE metrics [i.24]. As a minimum the developer shall be expected to show that any such listed, and publicly known, vulnerabilities have been mitigated and can be declared as having no impact on the system.

EXAMPLE 1: The US based National Vulnerability Database (NVD), is historically a repository of vulnerability management data created and maintained by the U.S. government that analyses software vulnerabilities published in the Common Vulnerabilities and Exposures (CVE) database. The NVD rates the severity of known vulnerabilities using the Common Vulnerability Scoring System (CVSS). A CVSS calculator available online uses a system of metrics very similar to those given in ETSI TS 102 165-1 [2].

EXAMPLE 2: The Global CVE Allocation System (GCVE) [i.24] is a modernized approach to the CVE systems that is more decentralised than prior systems but which, similarly, should be treated as a resource by developers to give assurance that publicly known vulnerabilities have been examined and mitigated.

EXAMPLE 3: A wider listing of similar repositories can be found in ETSI TR 103 306 [i.23].

A.4 Exploitation

This is not addressed in the present document in detail. The role of exploitation is to actually verify the identified penetration actually works. In practice exploitation, and the creation of any application or process to achieve it, should be treated as any other development project.

A.5 Pivoting and Exfiltration

In this case an attacker has made an initial entry to the system and may exploit that to cause further damage (e.g. privilege escalation).

A.6 Reporting

The aim of a report in conventional penetration tests is based on an understanding that a pen-test has been requested by a client and the report identifies the nature of the vulnerabilities that have been identified and exploited. For the purposes of the present document this element of a pen-test is not addressed.

Annex B (informative): Application of VAN in regulation

B.1 EU Cyber security act

The CSA [i.1] identifies the following definitions (see also clause 3.1) for assurance. The main body of the present document maps the expectation of testing in VAN to these levels.

NOTE: The present document does not consider basic assurance level in detail but for completeness it is shown below.

High assurance level: assurance that ICT products, ICT services and ICT processes where the corresponding security requirements, including security functionalities, are provided at a level intended to minimize the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with significant skills and resources.

Substantial assurance level: assurance that the ICT products, ICT services and ICT processes where the corresponding security requirements, including security functionalities, are provided at a level intended to minimize the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources.

Basic assurance level: assurance that the ICT products, ICT services and ICT processes where the corresponding security requirements, including security functionalities, are provided at a level intended to minimize the known basic risks of incidents and cyberattacks.

B.2 EU Cyber Resilience Act

Applies the general expectation of the CSA.

B.3 EU Network and Information Security Directive 2

Applies the general expectation of the CSA.

B.4 Sector specific regulation

B.4.1 DORA

Not specifically addressed but in financial markets stress tests are used as a close equivalent of some forms of penetration testing to determine the resilience of markets to attack (see Regulation (EU) 2022/2554 [i.16]).

B.4.2 Vehicle type regulation

Applies the general expectation of the CSA (see Regulation (EU) 2019/2144 [i.17]).

B.4.3 Medical devices

Applies the general expectation of the CSA (see Regulation (EU) 2017/745 [i.18]).

History

Document history		
V1.1.1	December 2025	Publication