



**Norme
internationale**

ISO/IEC 15408-3

**Sécurité de l'information,
cybersécurité et protection de la
vie privée — Critères d'évaluation
pour la sécurité des technologies de
l'information —**

**Partie 3:
Composants d'assurance de sécurité**

*Information security, cybersecurity and privacy protection —
Evaluation criteria for IT security —*

Part 3: Security assurance components

**Cinquième édition
2026-05**

Sample Document

get full document from standards.iteh.ai

Sample Document

get full document from standards.iteh.ai



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2026

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos	x
Introduction	xi
1 Domaine d'application	1
2 Références normatives	1
3 Termes et définitions	1
4 Vue d'ensemble	5
5 Paradigme d'assurance	5
5.1 Généralités	5
5.2 Approche CC	5
5.3 Approche d'assurance	6
5.3.1 Généralités	6
5.3.2 Signification des vulnérabilités	6
5.3.3 Cause des vulnérabilités	6
5.3.4 Assurance CC	7
5.3.5 Assurance par l'évaluation	7
5.4 Niveau d'assurance de l'évaluation CC	7
6 Composants d'assurance de sécurité	8
6.1 Généralités	8
6.2 Structure de la classe d'assurance	8
6.2.1 Généralités	8
6.2.2 Nom de la classe	8
6.2.3 Introduction de la classe	8
6.2.4 Notes d'application de classe	8
6.2.5 Familles d'assurance	9
6.3 Structure de la famille d'assurance	9
6.3.1 Généralités	9
6.3.2 Nom de la famille	9
6.3.3 Objectifs de la famille	9
6.3.4 Classement des composants	9
6.3.5 Notes d'application familiale	9
6.3.6 Composants d'assurance	10
6.4 Structure du composant d'assurance	10
6.4.1 Généralités	10
6.4.2 Nom du composant	10
6.4.3 Objectifs des composants	10
6.4.4 Notes d'application des composants	10
6.4.5 Dépendances des composants	11
6.4.6 Éléments d'assurance	11
6.5 Éléments d'assurance	12
6.6 Taxonomie des composants	12
7 Évaluation du profil de protection de classe APE (PP)	12
7.1 Généralités	12
7.2 Introduction du PP (APE_INT)	13
7.2.1 Objectifs	13
7.2.2 Introduction de PP (APE_INT.1)	14
7.3 Revendications de conformité (APE_CCL)	14
7.3.1 Objectifs	14
7.3.2 Revendications de conformité (APE_CCL.1)	14
7.4 Définition du problème de sécurité (APE_SPD)	16
7.4.1 Objectifs	16
7.4.2 Définition du problème de sécurité (APE_SPD.1)	16
7.5 Objectifs de sécurité (APE_OBJ)	16

7.5.1	Objectifs	16
7.5.2	Classement des composants.....	16
7.5.3	Objectifs de sécurité pour l'environnement opérationnel (APE_OBJ.1).....	16
7.5.4	Objectifs de sécurité (APE_OBJ.2).....	17
7.6	Définition des composants étendus (APE_ECD).....	18
7.6.1	Objectifs	18
7.6.2	Définitions des composants étendus (APE_ECD.1).....	18
7.7	Exigences de sécurité (APE_REQ).....	19
7.7.1	Objectifs	19
7.7.2	Classement des composants.....	19
7.7.3	Exigences de sécurité avec argumentaire direct (APE_REQ.1).....	19
7.7.4	Exigences de sécurité dérivées (APE_REQ.2).....	20
8	Classe ACE Évaluation de la configuration du profil de protection	21
8.1	Généralités.....	21
8.2	Introduction du module de PP (APE_INT).....	23
8.2.1	Objectifs	23
8.2.2	Introduction du module de PP (ACE_INT.1).....	23
8.3	Revendications de conformité du module de PP (ACE_CCL).....	23
8.3.1	Objectifs	23
8.3.2	Revendications de conformité de Module de PP (ACE_CCL.1).....	24
8.4	Définition de problème de sécurité de Module de PP (ACE_SPD).....	25
8.4.1	Objectifs	25
8.4.2	Définition de problème de sécurité de Module de PP (ACE_SPD.1).....	25
8.5	Objectifs de sécurité de Module de PP (ACE_OBJ).....	26
8.5.1	Objectifs	26
8.5.2	Classement des composants.....	26
8.5.3	Objectifs de sécurité de Module de PP pour l'environnement opérationnel (ACE_OBJ.1).....	26
8.5.4	Objectifs de sécurité de Module de PP (ACE_OBJ.2).....	27
8.6	Définitions des composants étendus du module de PP (ACE_ECD).....	27
8.6.1	Objectifs	27
8.6.2	Définitions des composants étendus du module de PP (ACE_ECD.1).....	27
8.7	Exigences en matière de sécurité d'un module de PP (ACE_REQ).....	28
8.7.1	Objectifs	28
8.7.2	Classement des composants.....	28
8.7.3	Exigences de sécurité avec argumentaire direct du module de PP (ACE_REQ.1).....	28
8.7.4	Exigences de sécurité dérivées de Module de PP (ACE_REQ.2).....	29
8.8	Cohérence du module de PP (ACE_MCO).....	30
8.8.1	Objectifs	30
8.8.2	Cohérence de Module de PP (ACE_MCO.1).....	30
8.9	Cohérence de la configuration de PP (ACE_CCO).....	31
8.9.1	Objectifs	31
8.9.2	Cohérence de configuration de PP (ACE_CCO.1).....	32
9	Évaluation de la cible de sécurité (ST) de classe ASE	34
9.1	Généralités.....	34
9.2	Introduction de la ST (ASE_INT).....	36
9.2.1	Objectifs	36
9.2.2	Introduction de la ST (ASE_INT.1).....	36
9.3	Revendications de conformité (ASE_CCL).....	36
9.3.1	Objectifs	36
9.3.2	Revendications de conformité (ASE_CCL.1).....	37
9.4	Définition du problème de sécurité (ASE_SPD).....	38
9.4.1	Objectifs	38
9.4.2	Définition du problème de sécurité (ASE_SPD.1).....	38
9.5	Objectifs de sécurité (ASE_OBJ).....	39
9.5.1	Objectifs	39
9.5.2	Classement des composants.....	39
9.5.3	Objectifs de sécurité pour l'environnement opérationnel (ASE_OBJ.1).....	39

ISO/IEC 15408-3:2026(fr)

9.5.4	Objectifs de sécurité (ASE_OBJ.2)	40
9.6	Définitions des composants étendus (ASE_ECD)	40
9.6.1	Objectifs	40
9.6.2	Définition étendue des composants (ASE_ECD.1)	40
9.7	Exigences de sécurité (ASE_REQ)	41
9.7.1	Objectifs	41
9.7.2	Classement des composants	41
9.7.3	Exigences de sécurité avec argumentaire direct (ASE_REQ.1)	41
9.7.4	Exigences de sécurité dérivées (ASE_REQ.2)	42
9.8	Spécification récapitulative de la TOE (ASE_TSS)	43
9.8.1	Objectifs	43
9.8.2	Classement des composants	44
9.8.3	Spécification de résumé de la TOE (ASE_TSS.1)	44
9.8.4	Spécification de résumé de la TOE avec résumé de la conception architecturale (ASE_TSS.2)	44
9.9	Cohérence de la cible de sécurité d'un produit composite (ASE_COMP)	45
9.9.1	Objectifs	45
9.9.2	Classement des composants	45
9.9.3	Notes d'application	45
9.9.4	Cohérence de la cible de sécurité (ST) (ASE_COMP.1)	46
10	Développement de la classe ADV	47
10.1	Généralités	47
10.2	Architecture de sécurité (ADV_ARC)	53
10.2.1	Objectifs	53
10.2.2	Classement des composants	53
10.2.3	Notes d'application	53
10.2.4	Description de l'architecture de sécurité (ADV_ARC.1)	54
10.3	Spécifications fonctionnelles (ADV_FSP)	55
10.3.1	Objectifs	55
10.3.2	Classement des composants	55
10.3.3	Notes d'application	55
10.3.4	Spécification fonctionnelle de base (ADV_FSP.1)	58
10.3.5	Spécification fonctionnelle de sécurité (ADV_FSP.2)	59
10.3.6	Spécification fonctionnelle avec résumé complet (ADV_FSP.3)	59
10.3.7	Spécification fonctionnelle complète (ADV_FSP.4)	60
10.3.8	Spécification fonctionnelle semi-formelle complète avec informations d'erreurs supplémentaires (ADV_FSP.5)	61
10.3.9	Spécification fonctionnelle semi-formelle complète avec spécification formelle supplémentaire (ADV_FSP.6)	62
10.4	Représentation de l'implémentation (ADV_IMP)	62
10.4.1	Objectifs	62
10.4.2	Classement des composants	63
10.4.3	Notes d'application	63
10.4.4	Représentation de l'implémentation de la TSF (ADV_IMP.1)	64
10.4.5	Mappage complet de la représentation d'implémentation de la TSF (ADV_IMP.2)	64
10.5	Éléments internes de la TSF (ADV_INT)	65
10.5.1	Objectifs	65
10.5.2	Classement des composants	65
10.5.3	Notes d'application	65
10.5.4	Sous-ensemble bien structuré de la TSF interne (ADV_INT.1)	66
10.5.5	Internes bien structurés (ADV_INT.2)	67
10.5.6	Internes de complexité minimale (ADV_INT.3)	68
10.6	Modélisation de TSF formelle (ADV_SPM)	68
10.6.1	Objectifs	68
10.6.2	Classement des composants	69
10.6.3	Notes d'application	69
10.6.4	Modèle TSF formel (ADV_SPM.1)	69
10.7	Conception de la TOE (ADV_TDS)	70

10.7.1	Objectifs	70
10.7.2	Classement des composants	71
10.7.3	Notes d'application	71
10.7.4	Conception de base (ADV_TDS.1)	72
10.7.5	Conception architecturale (ADV_TDS.2)	73
10.7.6	Conception modulaire de base (ADV_TDS.3)	74
10.7.7	Conception modulaire semi-formelle (ADV_TDS.4)	75
10.7.8	Conception modulaire semi-formelle complète (ADV_TDS.5)	75
10.7.9	Conception modulaire semi-formelle complète avec présentation formelle de la conception de haut niveau (ADV_TDS.6)	76
10.8	Conformité de conception composite (ADV_COMP)	77
10.8.1	Objectifs	77
10.8.2	Classement des composants	77
10.8.3	Notes d'application	77
10.8.4	Conformité de la conception aux recommandations de l'utilisateur relatives aux composants de base, RTE pour l'évaluation mixte et rapport de l'autorité d'évaluation des composants de base (ADV_COMP.1)	78
11	Classe AGD Lignes directrices	79
11.1	Généralités	79
11.2	Guide opérationnel de l'utilisateur (AGD_OPE)	80
11.2.1	Objectifs	80
11.2.2	Classement des composants	80
11.2.3	Notes d'application	80
11.2.4	Recommandations opérationnelles de l'utilisateur (AGD_OPE.1)	81
11.3	Guide préparatoire (AGD_PRE)	82
11.3.1	Objectifs	82
11.3.2	Classement des composants	82
11.3.3	Notes d'application	82
11.3.4	Procédures préparatoires (AGD_PRE.1)	83
12	Support du cycle de vie de la classe ALC	83
12.1	Généralités	83
12.2	Capacités CM (ALC_CMC)	85
12.2.1	Objectifs	85
12.2.2	Classement des composants	86
12.2.3	Notes d'application	86
12.2.4	Étiquetage de la TOE (ALC_CMC.1)	86
12.2.5	Utilisation du système CM (ALC_CMC.2)	87
12.2.6	Contrôles d'autorisation (ALC_CMC.3)	88
12.2.7	Support de production, procédures d'acceptation et automatisation (ALC_CMC.4)	89
12.2.8	Support avancé (ALC_CMC.5)	90
12.3	Périmètre de la CM (ALC_CMS)	92
12.3.1	Objectifs	92
12.3.2	Classement des composants	92
12.3.3	Notes d'application	93
12.3.4	Couverture de la CM de la TOE (ALC_CMS.1)	93
12.3.5	Parties de la couverture de la CM de la TOE (ALC_CMS.2)	93
12.3.6	Couverture de CM de représentation de mise en œuvre (ALC_CMS.3)	94
12.3.7	Couverture de CM de suivi des problèmes (ALC_CMS.4)	95
12.3.8	Outils de développement Couverture CM (ALC_CMS.5)	96
12.4	Livraison (ALC_DEL)	97
12.4.1	Objectifs	97
12.4.2	Classement des composants	97
12.4.3	Notes d'application	97
12.4.4	Procédures de livraison (ALC_DEL.1)	98
12.5	Sécurité de l'environnement du développeur (ALC_DVS)	98
12.5.1	Objectifs	98
12.5.2	Classement des composants	98
12.5.3	Notes d'application	98

12.5.4	Identification des contrôles de sécurité (ALC_DVS.1)	99
12.5.5	Caractère suffisant des mesures de sécurité (ALC_DVS.2)	99
12.6	Correction des failles (ALC_FLR)	100
12.6.1	Objectifs	100
12.6.2	Classement des composants	100
12.6.3	Notes d'application	100
12.6.4	Correction des failles de base (ALC_FLR.1)	100
12.6.5	Procédures de signalement des failles (ALC_FLR.2)	101
12.6.6	Correction systématique des failles (ALC_FLR.3)	102
12.7	Définition du cycle de vie de développement (ALC_LCD)	103
12.7.1	Objectifs	103
12.7.2	Classement des composants	104
12.7.3	Notes d'application	104
12.7.4	Processus du cycle de vie définis par le développeur (ALC_LCD.1)	104
12.7.5	Modèle mesurable du cycle de vie (ALC_LCD.2)	105
12.8	Artéfacts de développement de la TOE (ALC_TDA)	105
12.8.1	Objectifs	105
12.8.2	Classement des composants	106
12.8.3	Notes d'application	106
12.8.4	Identification unique de la représentation de l'implémentation (ALC_TDA.1)	106
12.8.5	Correspondant au domaine d'application de CMS de la représentation de l'implémentation (ALC_TDA.2)	108
12.8.6	Regénérer la TOE avec des outils de développement bien définis (ALC_TDA.3)	110
12.9	Outils et techniques (ALC_TAT)	112
12.9.1	Objectifs	112
12.9.2	Classement des composants	112
12.9.3	Notes d'application	112
12.9.4	Outils de développement bien définis (ALC_TAT.1)	113
12.9.5	Conformité aux normes de mise en œuvre (ALC_TAT.2)	113
12.9.6	Conformité aux normes de mise en œuvre — toutes les parties (ALC_TAT.3)	114
12.10	Intégration des pièces de composition et de la vérification de cohérence des procédures de livraison (ALC_COMP)	115
12.10.1	Objectifs	115
12.10.2	Classement des composants	115
12.10.3	Notes d'application	115
12.10.4	Intégration du composant dépendant dans le composant de base associé et contrôle de cohérence pour les procédures de livraison et d'acceptation (ALC_COMP.1)	115
13	Classe ATE Essais	116
13.1	Généralités	116
13.2	Couverture (ATE_COV)	118
13.2.1	Objectifs	118
13.2.2	Classement des composants	118
13.2.3	Preuve de couverture (ATE_COV.1)	118
13.2.4	Analyse de la couverture (ATE_COV.2)	118
13.2.5	Analyse rigoureuse de la couverture (ATE_COV.3)	119
13.3	Profondeur (ATE_DPT)	120
13.3.1	Objectifs	120
13.3.2	Classement des composants	120
13.3.3	Notes d'application	120
13.3.4	Tests: conception de base (ATE_DPT.1)	121
13.3.5	Tests: modules d'application de sécurité (ATE_DPT.2)	121
13.3.6	Essais: conception modulaire (ATE_DPT.3)	122
13.3.7	Tests: représentation d'implémentation (ATE_DPT.4)	123
13.4	Essais fonctionnels (ATE_FUN)	124
13.4.1	Objectifs	124
13.4.2	Classement des composants	124
13.4.3	Notes d'application	124

13.4.4	Essais fonctionnels (ATE_FUN.1)	124
13.4.5	Essai fonctionnel ordonné (ATE_FUN.2)	125
13.5	Essais indépendants (ATE_IND)	126
13.5.1	Objectifs	126
13.5.2	Classement des composants	126
13.5.3	Notes d'application	126
13.5.4	Essais indépendants — conformité (ATE_IND.1)	127
13.5.5	Essais indépendants — échantillon (ATE_IND.2)	128
13.5.6	Essais indépendants — terminés (ATE_IND.3)	129
13.6	Essais fonctionnels composites (ATE_COMP)	130
13.6.1	Objectifs	130
13.6.2	Classement des composants	130
13.6.3	Notes d'application	130
13.6.4	Essais fonctionnels des produits composites (ATE_COMP.1)	131
14	Classe AVA Évaluation de la vulnérabilité	131
14.1	Généralités	131
14.2	Notes d'application	132
14.3	Analyse des vulnérabilités (AVA_VAN)	133
14.3.1	Objectifs	133
14.3.2	Classement des composants	133
14.3.3	Enquête de vulnérabilité (AVA_VAN.1)	133
14.3.4	Analyse de vulnérabilité (AVA_VAN.2)	134
14.3.5	Analyse de vulnérabilités ciblée (AVA_VAN.3)	135
14.3.6	Analyse de vulnérabilité méthodique (AVA_VAN.4)	136
14.3.7	Analyse de vulnérabilité méthodique avancée (AVA_VAN.5)	137
14.4	Évaluation de vulnérabilité composite (AVA_COMP)	138
14.4.1	Objectifs	138
14.4.2	Classement des composants	138
14.4.3	Notes d'application	138
14.4.4	Évaluation de la vulnérabilité des produits composites (AVA_COMP.1)	139
15	Composition de la classe ACO	139
15.1	Généralités	139
15.2	Argumentaire relatif à la composition (ACO_COR)	144
15.2.1	Objectifs	144
15.2.2	Classement des composants	144
15.2.3	Justification de la composition (ACO_COR.1)	145
15.3	Preuve de développement (ACO_DEV)	145
15.3.1	Objectifs	145
15.3.2	Classement des composants	145
15.3.3	Notes d'application	145
15.3.4	Description fonctionnelle (ACO_DEV.1)	146
15.3.5	Preuve de base de la conception (ACO_DEV.2)	147
15.3.6	Preuve détaillée de la conception (ACO_DEV.3)	147
15.4	Confiance dans les composants dépendants (ACO_REL)	148
15.4.1	Objectifs	148
15.4.2	Classement des composants	149
15.4.3	Notes d'application	149
15.4.4	Informations de base sur la confiance (ACO_REL.1)	149
15.4.5	Informations de fiabilité (ACO_REL.2)	149
15.5	Test de TOE composée (ACO_CTT)	150
15.5.1	Objectifs	150
15.5.2	Classement des composants	150
15.5.3	Notes d'application	150
15.5.4	Essais d'interface (ACO_CTT.1)	151
15.5.5	Essai d'interface rigide (ACO_CTT.2)	152
15.6	Analyse de vulnérabilité de composition (ACO_VUL)	153
15.6.1	Objectifs	153
15.6.2	Classement des composants	153

ISO/IEC 15408-3:2026(fr)

15.6.3	Notes d'application	153
15.6.4	Revue de vulnérabilité de la composition (ACO_VUL.1)	153
15.6.5	Analyse de la vulnérabilité à la composition (ACO_VUL.2)	154
15.6.6	Analyse de la vulnérabilité de composition de base améliorée (ACO_VUL.3)	155
Annexe A	(informative) Développement (ADV)	156
Annexe B	(informative) Composition (ACO)	178
Bibliographie	187

Sample Document

get full document from standards.iteh.ai

Avant-propos

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC, participent également aux travaux.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives ou www.iec.ch/members_experts/refdocs).

L'ISO et l'IEC attirent l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'ISO et l'IEC ne prennent pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, L'ISO et l'IEC n'avaient pas] reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse www.iso.org/brevets et <https://patents.iec.ch>. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié tout ou partie de tels droits de propriété.

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir www.iso.org/iso/avant-propos. Pour l'IEC, voir www.iec.ch/understanding-standards.

Le présent document a été élaboré par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*, en collaboration avec le comité technique CEN/CLC/JTC 13, *Cybersécurité et protection des données*, du Comité européen de normalisation (CEN), conformément à l'Accord de coopération technique entre l'ISO et le CEN (Accord de Vienne).

Cette cinquième édition annule et remplace la quatrième édition (ISO/IEC 15408-3:2022), qui a fait l'objet d'une révision technique.

Les principales modifications sont les suivantes:

- la terminologie a été revue et mise à jour;
- un élément d'action de développeur manquant a été ajouté (ADV_SPM.1.7D).

Une liste de toutes les parties de la série ISO/IEC 15408 se trouve sur les sites Web de l'ISO et de l'IEC.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/members.html et www.iec.ch/national-committees.

Introduction

Les composants d'assurance de sécurité, tels que définis dans le présent document, constituent la base des exigences d'assurance de sécurité exprimées dans un paquet d'assurance de sécurité, un profil de protection (PP), un module de PP, une configuration de PP ou une cible de sécurité (ST).

Ces exigences établissent une façon normalisée d'exprimer les exigences d'assurance des TOE. Le présent document propose un catalogue de l'ensemble des composants, des familles et des classes d'assurance. Il définit également des critères d'évaluation pour les PP, les configurations de PP, les modules de PP et les ST.

Il s'adresse notamment aux consommateurs, aux développeurs, aux groupes de travail techniques, aux évaluateurs de produits TI sécurisés. L'ISO/IEC 15408-1 fournit des informations supplémentaires sur le public cible de la série ISO/IEC 15408 et sur l'utilisation de la série ISO/IEC 15408 par les groupes qui composent le public cible. Les groupes suivants peuvent utiliser le présent document comme suit:

- les consommateurs qui utilisent le présent document lorsqu'ils choisissent des composants pour exprimer des exigences d'assurance afin de satisfaire aux objectifs de sécurité exprimés dans un PP ou une ST, déterminant les niveaux requis d'assurance de sécurité de la TOE;
- les développeurs, qui répondent aux exigences de sécurité des consommateurs réelles ou perçues lors de la construction d'une TOE, font référence au présent document lorsqu'ils interprètent les énoncés des exigences d'assurance et déterminent les approches d'assurance des TOE;
- les évaluateurs qui utilisent les exigences d'assurance définies dans le présent document comme un énoncé obligatoire des critères d'évaluation lors de la détermination de l'assurance des TOE et lors de l'évaluation des PP et des ST.

Dans le présent document, les caractères gras sont utilisés pour mettre en évidence les relations hiérarchiques entre les exigences. Cette convention d'écriture impose les caractères gras à toute nouvelle exigence.

Pour les exigences d'assurance de sécurité, les verbes spéciaux relatifs aux activités d'évaluation obligatoires sont présentés en caractères gras italiques.

Plusieurs organisations gouvernementales ont contribué à l'élaboration de la présente version des critères communs pour la sécurité des technologies de l'information. Par la présente, en tant que cotitulaires des droits d'auteur des critères communs pour la sécurité des technologies de l'information (en abrégé, CC), ces organisations accordent à l'ISO/IEC une licence non exclusive d'utilisation des CC pour poursuivre l'élaboration/la maintenance de la série de normes ISO/IEC 15408. Toutefois, lesdites organisations gouvernementales se réservent le droit d'utiliser, de copier, de diffuser, de traduire ou de modifier les CC comme elles l'entendent. De plus amples informations concernant ces agences sont disponibles à l'adresse <https://commoncriteriaportal.org/cc/copyright/index.cfm>.

Sample Document

get full document from standards.iteh.ai

Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information —

Partie 3: Composants d'assurance de sécurité

1 Domaine d'application

Le présent document spécifie les exigences d'assurance de sécurité de la série ISO/IEC 15408. Il comprend les éléments d'assurance individuels à partir desquels sont composés les niveaux d'assurance de l'évaluation et les autres paquets contenus dans l'ISO/IEC 15408-5, ainsi que les critères d'évaluation des profils de protection (PP), des configurations de PP, des modules de PP et des cibles de sécurité (ST).

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO/IEC 15408-1:2026, *Sécurité de l'information — Critères d'évaluation pour la sécurité des technologies de l'information — Partie 1: Introduction et modèle général*

ISO/IEC 15408-2:2026, *Sécurité de l'information — Critères d'évaluation pour la sécurité des technologies de l'information — Partie 2: Composants fonctionnels de sécurité*

ISO/IEC 15408-4, *Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information — Partie 4: Cadre prévu pour la spécification des méthodes d'évaluation et des activités connexes*

ISO/IEC 15408-5:2026, *Sécurité de l'information — Critères d'évaluation pour la sécurité des technologies de l'information — Partie 5: Paquets prédéfinis d'exigences de sécurité*

ISO/IEC 18045:2026, *Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation de la sécurité informatique — Méthodologie d'évaluation de la sécurité informatique*

ISO/IEC/IEEE 24765:2017, *Ingénierie des systèmes et du logiciel — Vocabulaire*

3 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de l'ISO/IEC 15408-1, de l'ISO/IEC 15408-2, de l'ISO/IEC 18045 et de l'ISO/IEC IEEE 24765, ainsi que les suivants, s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- ISO Online browsing platform: disponible à l'adresse <https://www.iso.org/obp>
- IEC Electropedia: disponible à l'adresse <https://www.electropedia.org/>

3.1

procédure d'acceptation

procédure suivie pour accepter un ou plusieurs *élément(s) de configuration* (3.4) nouvellement créé(s) ou modifié(s) comme faisant partie de la cible de l'évaluation (TOE), ou pour le déplacer vers l'étape suivante du cycle de vie

Note 1 à l'article: Ces procédures identifient les rôles ou individus responsables de l'acceptation ainsi que les critères à appliquer dans la décision d'acceptation.

Note 2 à l'article: Il existe plusieurs types de situations d'acceptation, dont certaines peuvent se chevaucher:

- l'acceptation d'un élément dans le système de gestion de configuration pour la première fois, en particulier dans le cadre d'un processus d'intégration;
- progression des éléments de configuration vers la phase suivante du cycle de vie à chaque étape de la construction de la TOE.

3.2

action

élément qui spécifie une activité entreprise par un évaluateur ou un développeur

Note 1 à l'article: Ces actions sont soit explicitement déclarées comme actions d'évaluateur, soit implicitement dérivées d'actions de développeur (actions d'évaluateur implicites) dans les composants d'assurance Voir 6.5 pour plus d'informations.

3.3

résultat réel des essais

résultat d'un essai qui peut être différent du résultat attendu des essais si le résultat réel des essais n'est pas égal au résultat attendu des essais

3.4

élément de configuration

élément ou agrégation de matériel, de logiciel ou des deux qui est conçu pour la gestion de configuration et traité comme une entité unique dans le processus de gestion de configuration pendant le *développement* (3.12) de la cible d'évaluation (TOE)

Note 1 à l'article: Il peut s'agir de parties de la TOE ou d'objets liés au développement de la TOE, par exemple des documents d'évaluation ou des outils de développement. Les éléments de gestion de configuration peuvent être stockés directement dans le système de gestion de configuration (p. ex. des fichiers) ou par voie de référence (p. ex. des pièces matérielles) avec leur version.

3.5

liste de configuration

document énumérant tous les *éléments de configuration* (3.4) pour un produit spécifique ainsi que la version exacte de chaque élément de gestion de configuration pertinent pour une version spécifique du produit complet

Note 1 à l'article: Cette liste permet de distinguer les éléments appartenant à la version évaluée du produit des autres versions de ces éléments appartenant à d'autres versions du produit. La liste de gestion de configuration finale est un document spécifique applicable à une version spécifique d'un produit spécifique. Cette liste peut, prendre la forme d'un document électronique à l'intérieur d'un *outil de gestion de configuration* (3.10). Dans ce cas, elle peut être considérée comme une vue spécifique sur le système ou une partie du système, plutôt que comme une donnée de sortie du système. Cependant, pour une utilisation pratique dans le cadre d'une évaluation, la liste de configuration sera probablement fournie dans le cadre de la documentation d'évaluation. La liste de configuration définit les éléments qui sont soumis aux exigences de gestion de la configuration des ALC_CMC (capacités CM) (12.2).

3.6 gestion de configuration CM

discipline appliquant une orientation et une surveillance techniques et administratives pour identifier et documenter les caractéristiques fonctionnelles et physiques d'*éléments de configuration* (3.4), pour contrôler les changements apportés à ces caractéristiques, pour consigner et déclarer l'état de traitement et d'implémentation et pour vérifier la conformité aux exigences spécifiées

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.779, modifié — La deuxième et troisième définitions ont été supprimées.]

3.7 documentation de la gestion de configuration documentation de CM

documentation comprenant les *listes de configuration* (3.5) et les *plans de gestion de configuration* (3.8)

3.8 plan de gestion de configuration plan de CM

description de la manière dont le *système de gestion de la configuration* (3.9) est utilisé pour la cible de l'évaluation (TOE)

Note 1 à l'article: L'objectif d'éditer un plan de gestion de configuration est de permettre aux membres du personnel de voir clairement ce qu'ils ont à faire. Du point de vue du système de gestion de configuration global, il peut être vu comme un document de sortie (car il peut être produit dans le cadre de l'application du système de gestion de configuration). Du point de vue du projet concret, il s'agit d'un document d'utilisation étant donné que les membres de l'équipe du projet l'utilisent pour comprendre les étapes qu'ils ont à effectuer tout au long du projet. Le plan de gestion de configuration définit l'usage du système pour le produit spécifique; le même système peut être utilisé dans une différente mesure pour d'autres produits. Le plan de gestion de configuration définit et décrit les données de sortie du système de gestion de configuration d'une entreprise qui sont utilisées au cours du *développement* (3.12) de la TOE.

Note 2 à l'article: La structure et le contenu d'un plan de gestion de configuration sont présentés dans l'ISO 10007:2017, Annexe A.

3.9 système de gestion de configuration système CM

ensemble de procédures et d'outils (y compris leur documentation) utilisés par un développeur pour développer et maintenir les configurations de ses produits pendant leur cycle de vie

Note 1 à l'article: Les systèmes de gestion de configuration peuvent avoir des degrés de rigueur et de fonction variables. À des niveaux supérieurs, les systèmes de gestion de configuration peuvent être automatisés, avec une correction des défaillances, des contrôles des modifications et d'autres mécanismes de suivi.

3.10 outil de gestion de configuration

outil opéré manuellement ou automatisé, qui assure l'exécution ou la prise en charge d'un *système de gestion de configuration* (3.9)

EXEMPLE Outils de gestion de la version des parties de la cible d'évaluation (TOE).

3.11 livraison

transmission aux clients de la cible d'évaluation (TOE) finie depuis l'environnement de *production* (3.21)

Note 1 à l'article: Cette phase du cycle de vie du produit peut inclure l'emballage et le stockage sur le site de *développement* (3.12), mais ne comprend pas le transport de la TOE inachevée ou de parties de la TOE entre différents développeurs ou sites de développement différents.